



DS-900WN DS-800WN

Guide de l'administrateur

Paramètres requis selon l'utilisation

Paramètres réseau

Paramètres requis pour la numérisation

Paramètres de sécurité de base

Paramètres de sécurité avancés

Utilisation d'Epson Open Platform

Copyright

Aucune partie de cette publication ne peut être reproduite, stockée dans un système de système de récupération de données, ni transmise, sous quelque forme que ce soit ni par aucun procédé électronique ou mécanique, y compris la photocopie, l'enregistrement ou autrement, sans le consentement écrit préalable de Seiko Epson Corporation. Aucune responsabilité ne sera engagée relative à l'utilisation des informations contenues dans ce manuel. Aucune responsabilité n'est assumée pour les dommages résultant des informations contenues dans ce manuel. L'information contenue dans la présente ne peut être utilisée qu'avec ce produit Epson. Epson décline toute responsabilité de l'utilisation de ces informations appliquées à d'autres produits.

Neither Seiko Epson Corporation et ses filiales ne peuvent être tenus responsables par l'acheteur de ce produit ou des tiers de tout dommage, perte, coût ou dépense encourus par l'acheteur ou des tiers à la suite d'un accident, d'une mauvaise utilisation, d'un abus ou des modifications, réparations ou altérations non autorisées de ce produit, ou (sauf aux États-Unis) le non-respect strict des instructions d'exploitation et de maintenance de Seiko Epson Corporation.

Seiko Epson Corporation et ses filiales ne peuvent être tenus responsables des dommages ou des problèmes découlant de l'utilisation d'options ou de consommables autres que ceux désignés comme des produits Epson authentiques approuvés par Seiko Epson Corporation.

Seiko Epson Corporation ne pourra être tenu pour responsable des dommages résultant des interférences électromagnétiques dues à l'utilisation de câbles d'interface autres que ceux désignés comme produits Epson approuvés par Seiko Epson Corporation.

© 2024 Seiko Epson Corporation

Le contenu de ce manuel et les caractéristiques de ce produit sont modifiables sans préavis.

Marques commerciales

- Microsoft, Windows, Windows Server, Microsoft Edge, SharePoint, and Internet Explorer are trademarks of the Microsoft group of companies.
- Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- Chrome, Chromebook and Android are trademarks of Google LLC.
- Wi-Fi®, Wi-Fi Direct®, and Wi-Fi Protected Access® are registered trademarks of Wi-Fi Alliance®. Wi-Fi Protected Setup™, WPA2™, WPA3™ are trademarks of Wi-Fi Alliance®.
- The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- The Mopria™ word mark and the Mopria™ Logo are registered and/or unregistered trademarks of Mopria Alliance, Inc. in the United States and other countries. Unauthorized use is strictly prohibited.
- Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- Remarque générale : toutes les autres marques commerciales sont la propriété de leurs détenteurs respectifs et ne sont utilisées qu'à titre de références.

Table des matières

Copyright

Marques commerciales

Introduction

| | |
|--|---|
| Le contenu de ce document. | 8 |
| Utilisation de ce guide. | 8 |
| Marques et symboles. | 8 |
| Descriptions utilisées dans ce manuel. | 8 |
| Références du système d'exploitation. | 8 |

Remarques concernant le mot de passe administrateur

| | |
|--|----|
| Remarques concernant le mot de passe administrateur. | 11 |
| Mot de passe administrateur initial. | 11 |
| Opérations qui nécessitent le mot de passe administrateur. | 11 |
| Modification du mot de passe administrateur. | 11 |
| Réinitialisation du mot de passe administrateur. | 12 |

Paramètres requis selon l'utilisation

| | |
|--|----|
| Paramètres requis selon l'utilisation. | 14 |
|--|----|

Paramètres réseau

| | |
|---|----|
| Connecter le scanner au réseau. | 17 |
| Avant de configurer une connexion réseau. | 17 |
| Connexion au réseau depuis le panneau de commande. | 19 |
| Ajout ou remplacement d'ordinateurs ou périphériques. | 24 |
| Connexion à un scanner déjà présent sur le réseau. | 24 |
| Connexion directe d'un périphérique intelligent et le scanner (Wi-Fi Direct). | 25 |
| Réinitialisation de la connexion réseau. | 27 |
| Vérification de l'état de la connexion réseau. | 29 |
| Vérification de l'état de la connexion réseau depuis le panneau de commande. | 30 |
| Caractéristiques réseau. | 31 |
| Caractéristiques du Wi-Fi. | 31 |
| Caractéristiques Ethernet. | 32 |

| | |
|---|----|
| Fonctionnalités réseau et prise en charge | |
| IPv4/IPv6. | 33 |
| Protocole de sécurité. | 33 |
| Utilisation du port pour le scanner. | 33 |
| Résolution des problèmes. | 35 |
| Impossible de se connecter à un réseau. | 35 |

Logiciel pour la configuration du scanner

| | |
|--|----|
| Application de configuration des opérations du scanner (Web Config). | 39 |
| Comment exécuter Web Config dans un navigateur Web. | 39 |
| Epson Device Admin. | 40 |
| Modèle de configuration. | 41 |

Paramètres requis pour la numérisation

| | |
|--|----|
| Enregistrer un serveur de messagerie. | 46 |
| Vérifier la connexion à un serveur de messagerie. | 47 |
| Créer un dossier réseau. | 49 |
| Mise à disposition des contacts. | 56 |
| Comparaison des outils de configuration des contacts. | 57 |
| Enregistrement d'une destination dans les contacts à l'aide de Web Config. | 57 |
| Enregistrement des destinations en tant que groupe à l'aide de Web Config. | 59 |
| Sauvegarde et importation de contacts. | 60 |
| Exportation et enregistrement de contacts en volume à l'aide d'un outil. | 61 |
| Coopération entre le serveur LDAP et les utilisateurs. | 63 |
| Configuration de AirPrint. | 66 |
| Problèmes lors de la préparation de la numérisation du réseau. | 67 |
| Conseils pour résoudre les problèmes. | 67 |
| Accès impossible à Web Config. | 67 |

Personnalisation de l'affichage du panneau de commande

| | |
|--|----|
| Enregistrement de Prédéfinis. | 70 |
| Options des menus de Prédéfinis. | 71 |

| | |
|--|----|
| Modifier l'écran d'accueil du panneau de commande. | 72 |
| Modification de Mise en page de l'écran d'accueil. | 72 |
| Ajouter icône. | 73 |
| Supprimer icône. | 74 |
| Déplacer icône. | 75 |

Paramètres de sécurité de base

| | |
|---|----|
| Présentation des fonctions de sécurité du produit. | 77 |
| Réglages de l'administrateur. | 77 |
| Configurer le mot de passe administrateur. | 77 |
| Utilisation de Verrouiller le réglage pour le panneau de commande. | 79 |
| Connexion en tant qu'administrateur depuis le panneau de commande. | 82 |
| Limitation des fonctionnalités disponibles (Contrôle d'accès). | 83 |
| Création du compte utilisateur. | 83 |
| Activation du Contrôle d'accès. | 84 |
| Connexion à un scanner sur lequel Contrôle d'accès est activé. | 85 |
| Désactivation de l'interface externe. | 85 |
| Activation de la vérification du programme au démarrage. | 86 |
| Désactiver la numérisation via le réseau depuis votre ordinateur. | 86 |
| Activation ou désactivation de la numérisation avec WSD. | 86 |
| Contrôler un scanner à distance. | 87 |
| Vérification des informations pour un scanner à distance. | 87 |
| Réception de notifications par courrier électronique en cas d'événements. | 87 |
| Utilisation de Web Config pour contrôler l'alimentation du scanner. | 89 |
| Restauration des paramètres par défaut. | 89 |
| Informations Epson Remote Services. | 89 |
| Résolution des problèmes. | 89 |
| Mot de passe administrateur oublié. | 89 |

Paramètres de sécurité avancés

| | |
|---|----|
| Paramètres de sécurité et prévention du danger. | 92 |
| Paramètres de la fonction de sécurité. | 93 |
| Contrôle à l'aide des protocoles. | 93 |
| Contrôle des protocoles. | 93 |
| Protocoles que vous pouvez activer ou désactiver. | 93 |

| | |
|---|-----|
| Éléments de configuration du protocole. | 94 |
| Utilisation d'un certificat numérique. | 96 |
| À propos de la certification numérique. | 96 |
| Configuration d'un Certificat signé CA. | 97 |
| Mise à jour d'un certificat à signature automatique. | 100 |
| Configuration d'un Certificat CA. | 101 |
| Communication SSL/TLS avec le scanner. | 101 |
| Configuration des paramètres SSL/TLS de base. | 102 |
| Configuration d'un certificat de serveur pour le scanner. | 102 |
| Communication chiffrée par filtrage IPsec/IP. | 103 |
| À propos d'IPsec/filtrage IP. | 103 |
| Configuration de la politique par défaut. | 103 |
| Configuration de la politique de groupe. | 107 |
| Exemples de configuration de IPsec/filtrage IP. | 113 |
| Configuration d'un certificat pour IPsec/filtrage IP. | 114 |
| Connexion du scanner à un réseau IEEE802.1X. | 115 |
| Configuration d'un réseau IEEE 802.1X. | 115 |
| Configuration d'un certificat pour IEEE 802.1X | 116 |
| Résolution des problèmes pour la sécurité avancée | 117 |
| Restauration des paramètres de sécurité. | 117 |
| Problèmes lors de l'utilisation des fonctionnalités de sécurité réseau. | 117 |
| Problèmes lors de l'utilisation d'un certificat numérique. | 119 |

Utilisation d'Epson Open Platform

| | |
|---|-----|
| Présentation d'Epson Open Platform. | 125 |
| Configuration de Epson Open Platform. | 125 |
| Validation d'Epson Open Platform. | 125 |

Montage d'un dispositif d'authentification

| | |
|--|-----|
| Connexion du périphérique d'authentification. | 128 |
| Vérification de l'utilisation du périphérique d'authentification. | 128 |
| Vérification de la reconnaissance de la carte d'authentification. | 128 |
| Résolution des problèmes rencontrés avec le dispositif d'authentification. | 129 |
| Impossible de lire la carte d'authentification. | 129 |

Entretien

| | |
|--|-----|
| Nettoyage de l'extérieur du scanner. | 131 |
| Nettoyage de l'intérieur du scanner. | 131 |

| | |
|--|-----|
| Remplacement du jeu de rouleaux. | 135 |
| Codes de jeu de rouleaux. | 141 |
| Réinitialiser le nombre de numérisations après avoir remplacé les rouleaux. | 141 |
| Économie d'énergie. | 142 |
| Transport du scanner. | 142 |
| Sauvegarde des paramètres. | 143 |
| Exporter les paramètres. | 143 |
| Importer les paramètres. | 144 |
| Rest param défaut. | 144 |
| Mise à jour des applications et du micrologiciel. . . | 145 |
| Mise à jour du micrologiciel du scanner à l'aide du panneau de commande. | 146 |
| Mettre à jour le micrologiciel à l'aide de Web Config. | 146 |
| Mise à jour du micrologiciel sans connexion à Internet. | 147 |

Introduction

| | |
|------------------------------------|---|
| Le contenu de ce document. | 8 |
| Utilisation de ce guide. | 8 |

Le contenu de ce document

Ce document fournit les informations suivantes pour les administrateurs du scanner.

- Paramètres réseau
- Préparation de la fonction de numérisation
- Activer et gérer les paramètres de sécurité
- Effectuer la maintenance quotidienne

Pour les méthodes standard d'utilisation du scanner, voir le *Guide d'utilisation*.

Utilisation de ce guide

Marques et symboles



Attention:

Vous devez suivre attentivement les instructions pour éviter les blessures.



Important:

Vous devez respecter les instructions pour éviter d'endommager votre équipement.

Remarque:

Fournit des informations complémentaires et de référence.

Informations connexes

- ➔ Lien vers les sections connexes.

Descriptions utilisées dans ce manuel

- Les captures d'écran des applications proviennent de Windows 10 ou de macOS High Sierra. Le contenu affiché sur les écrans varie en fonction du modèle et de la situation.
- Les illustrations de ce manuel sont utilisées uniquement à titre indicatif. Bien qu'elles puissent varier légèrement du produit réel, les méthodes de fonctionnement sont les mêmes.

Références du système d'exploitation

Windows

Dans ce manuel, les termes comme « Windows 11 », « Windows 10 », « Windows 8.1 », « Windows 8 », « Windows 7 », « Windows Server 2022 », « Windows Server 2019 », « Windows Server 2016 », « Windows Server 2012 R2 », « Windows Server 2012 », « Windows Server 2008 R2 » et « Windows Server 2008 » font référence aux systèmes d'exploitation suivants. De plus, « Windows » est utilisé pour faire référence à toutes les versions.

- Système d'exploitation Microsoft® Windows® 11
- Système d'exploitation Microsoft® Windows® 10
- Système d'exploitation Microsoft® Windows® 8.1
- Système d'exploitation Microsoft® Windows® 8
- Système d'exploitation Microsoft® Windows® 7
- Système d'exploitation Microsoft® Windows Server® 2022
- Système d'exploitation Microsoft® Windows Server® 2019
- Système d'exploitation Microsoft® Windows Server® 2016
- Système d'exploitation Microsoft® Windows Server® 2012 R2
- Système d'exploitation Microsoft® Windows Server® 2012
- Système d'exploitation Microsoft® Windows Server® 2008 R2
- Système d'exploitation Microsoft® Windows Server® 2008

Mac OS

Dans ce manuel, « Mac OS » désigne Mac OS X 10.9 ou version ultérieure ainsi que macOS 11 ou version ultérieure.

Remarques concernant le mot de passe administrateur

| | |
|--|----|
| Remarques concernant le mot de passe administrateur. | 11 |
| Mot de passe administrateur initial. | 11 |
| Opérations qui nécessitent le mot de passe administrateur. | 11 |
| Modification du mot de passe administrateur. | 11 |
| Réinitialisation du mot de passe administrateur. | 12 |

Remarques concernant le mot de passe administrateur

Cet appareil vous permet de définir un mot de passe administrateur pour empêcher tout intervenant non autorisé d'accéder ou de modifier ses paramètres intrinsèques ou les paramètres réseau en mémoire lorsqu'il est connecté à un réseau.

Si vous définissez un mot de passe administrateur, vous devrez saisir ce mot de passe pour pouvoir modifier les paramètres dans des logiciels de configurations tels que Web Config.

Le mot de passe administrateur initial est défini au niveau du scanner, mais vous pouvez le modifier à votre guise.

Mot de passe administrateur initial

Le mot de passe administrateur initial dépend de la présence ou non d'une étiquette collée sur le produit. Si une étiquette « PASSWORD » se trouve à l'arrière, saisissez le nombre à 8 chiffres indiqué dessus. Si aucune étiquette « PASSWORD » n'est présente, saisissez le numéro de série situé à l'arrière du produit en guise de mot de passe administrateur initial.

Nous vous recommandons de ne pas conserver le mot de passe administrateur initial.

Remarque:

Aucun nom d'utilisateur par défaut n'est défini.

Opérations qui nécessitent le mot de passe administrateur

Si vous êtes invité à saisir le mot de passe administrateur lors des opérations suivantes, saisissez celui qui est défini au niveau du produit.

- Lors d'une connexion aux paramètres avancés de Web Config
- Lors de la navigation dans un menu du panneau de commande verrouillé par l'administrateur
- Lors de la modification des paramètres de l'appareil dans l'application
- Lors de la mise à jour du micrologiciel de l'appareil
- Lors de la modification ou réinitialisation du mot de passe administrateur

Modification du mot de passe administrateur

Vous pouvez le modifier depuis le panneau de commande du produit ou dans Web Config.

Lorsque vous modifiez le mot de passe, celui-ci doit contenir entre 8 et 20 caractères ou symboles alphanumériques d'un seul octet.

Réinitialisation du mot de passe administrateur

Vous pouvez réinitialiser le mot de passe administrateur à sa valeur initiale depuis le panneau de commande du produit ou depuis Web Config.

Si vous avez oublié le mot de passe et que vous ne pouvez pas réinitialiser sa valeur par défaut, vous devrez faire réparer le produit. Contactez votre revendeur local.

Paramètres requis selon l'utilisation

Paramètres requis selon l'utilisation. 14

Paramètres requis selon l'utilisation

Consultez ce qui suit pour effectuer les réglages nécessaires selon l'utilisation.

Connecter le scanner au réseau

| Utilisation | Paramètres requis |
|--|--|
| Je souhaite connecter le scanner au réseau. | Configurez votre scanner pour une numérisation via le réseau. « Connecter le scanner au réseau » à la page 17 |
| Je souhaite connecter le scanner à un nouvel ordinateur. | Définissez les paramètres réseau pour votre scanner sur le nouvel ordinateur. « Ajout ou remplacement d'ordinateurs ou périphériques » à la page 24 |

Paramètres pour la numérisation

| Utilisation | Paramètres requis |
|--|--|
| Je souhaite envoyer des images numérisées par e-mail. (Numér. vers email) | 1. Configurez le serveur de messagerie que vous souhaitez lier. « Enregistrer un serveur de messagerie » à la page 46 2. Enregistrez l'adresse e-mail du destinataire dans Contacts (en option). En enregistrant l'adresse e-mail, vous n'avez pas à la saisir à chaque fois que vous souhaitez effectuer un envoi : il vous suffit de la sélectionner depuis vos Contacts. « Mise à disposition des contacts » à la page 56 |
| Je souhaite enregistrer les images numérisées vers un dossier sur le réseau. (Numér. vers dossier réseau/FTP) | 1. Créez un dossier sur le réseau où vous souhaitez sauvegarder les images. « Créer un dossier réseau » à la page 49 2. Enregistrez le chemin vers le dossier dans Contacts (en option). En enregistrant le chemin du dossier, vous n'avez pas à le saisir à chaque fois que vous souhaitez effectuer un envoi : il vous suffit de le sélectionner depuis vos Contacts. « Mise à disposition des contacts » à la page 56 |
| Je souhaite enregistrer les images numérisées vers un service de cloud. (Numér. vers Cloud) | Configuration Epson Connect. Pour plus de détails sur la configuration, reportez-vous au site Web du portail Epson Connect. Lors de la configuration, vous avez besoin d'un compte utilisateur pour le service de stockage en ligne que vous souhaitez connecter. https://www.epsonconnect.com/ http://www.epsonconnect.eu (Europe uniquement) |

Personnalisation de l'affichage du panneau de commande

| Utilisation | Paramètres requis |
|--|---|
| Je souhaite modifier les éléments qui s'affichent sur le panneau de commande du scanner. | Définissez Prédéfinis ou Modifier Accueil . Vous pouvez enregistrer vos paramètres de numérisation préférés sur le panneau de commande et modifier les éléments qui s'affichent. « Personnalisation de l'affichage du panneau de commande » à la page 69 |

Définition des fonctions de sécurité de base

| Utilisation | Paramètres requis |
|---|--|
| Je souhaite que personne d'autre que l'administrateur ne puisse modifier les paramètres du scanner. | Définissez un mot de passe de l'administrateur pour le scanner. « Réglages de l'administrateur » à la page 77 |
| Je souhaite désactiver l'utilisation de scanners avec des connexions USB. | Désactiver l'interface externe. « Désactivation de l'interface externe » à la page 85 |

Définition des fonctions de sécurité avancées

| Utilisation | Paramètres requis |
|--|---|
| Je souhaite contrôler les protocoles à utiliser. | Activez ou désactivez les protocoles. « Contrôle à l'aide des protocoles » à la page 93 |
| Je souhaite chiffrer le chemin de communication. | 1. Configurez votre certificat numérique. « Utilisation d'un certificat numérique » à la page 96 2. Configurez la communication SSL/TLS. « Communication SSL/TLS avec le scanner » à la page 101 |
| Je souhaite utiliser la communication chiffrée (IPsec). Je souhaite être capable d'utiliser le logiciel uniquement depuis un ordinateur spécifique (filtre IP). | Configurer des politiques pour filtrer le trafic. « Communication chiffrée par filtrage IPsec/IP » à la page 103 |
| Je souhaite utiliser un scanner dans un réseau IEEE802.1X. | Configuration IEEE802.1X pour le scanner. « Connexion du scanner à un réseau IEEE802.1X » à la page 115 |

Synchronisation du scanner avec un système d'authentification

Obtenez une clé produit depuis le site Web dédié et activez Epson Open Platform sur votre scanner.

[« Utilisation d'Epson Open Platform » à la page 124](#)

Utilisation d'une option d'authentification (Epson Print Admin/Epson Print Admin Serverless)

Vous avez besoin d'une clé de licence pour utiliser cette option.

Veillez contacter votre revendeur pour en savoir plus.

Remarque:

Vous ne pouvez pas utiliser Epson Print Admin Serverless lorsque le système est synchronisé avec Epson Open Platform.

Paramètres réseau

| | |
|---|----|
| Connecter le scanner au réseau. | 17 |
| Ajout ou remplacement d'ordinateurs ou périphériques. | 24 |
| Vérification de l'état de la connexion réseau. | 29 |
| Caractéristiques réseau. | 31 |
| Résolution des problèmes. | 35 |

Connecter le scanner au réseau

Ce chapitre décrit comment connecter le scanner au réseau à l'aide du panneau de commande du scanner.

Remarque:

Si le scanner et l'ordinateur sont connectés au même réseau, vous pouvez également procéder à cette connexion à l'aide du programme d'installation.

Pour lancer le programme d'installation, rendez-vous sur le site Web suivant et saisissez le nom du produit. Accédez à **Installation**, puis procédez à la configuration.

<https://epson.sn>

Vous pouvez consulter les instructions d'utilisation dans les Manuels de film Web. Accédez à l'URL suivante.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

Avant de configurer une connexion réseau

Pour vous connecter au réseau, vérifiez au préalable la méthode de connexion et les informations de configuration pour la connexion.

Collecte d'informations sur les paramètres de connexion

Préparez les informations de réglage nécessaires pour la connexion. Vérifiez les informations suivantes à l'avance.

| Divisions | Éléments | Remarque |
|-----------------------------------|---|---|
| Mode de connexion du périphérique | <input type="checkbox"/> Ethernet <input type="checkbox"/> Wi-Fi | Décidez comment connecter le scanner au réseau. Pour le réseau local câblé, connectez-le au commutateur LAN. Pour le Wi-Fi, connectez-vous au réseau (SSID) du point d'accès. |
| Informations de connexion LAN | <input type="checkbox"/> Adresse IP <input type="checkbox"/> Masque de sous-réseau <input type="checkbox"/> Passerelle par défaut | Sélectionnez l'adresse IP à attribuer au scanner. Lorsque vous attribuez l'adresse IP de manière statique, toutes les valeurs sont requises. Lorsque vous attribuez dynamiquement l'adresse IP à l'aide de la fonction DHCP, ces informations ne sont pas nécessaires car elles sont définies automatiquement. |
| Informations de connexion Wi-Fi | <input type="checkbox"/> SSID <input type="checkbox"/> Mot de passe | Il s'agit du SSID (nom du réseau) et du mot de passe du point d'accès auquel le scanner se connecte. Si le filtrage d'adresse MAC a été défini, enregistrez l'adresse MAC du scanner à l'avance pour enregistrer le scanner. Voir ci-dessous les normes prises en charge. « Caractéristiques réseau » à la page 31 |
| Informations du serveur DNS | <input type="checkbox"/> Adresse IP du serveur DNS principal <input type="checkbox"/> Adresse IP du serveur DNS secondaire | Ces informations sont requises pour spécifier les serveurs DNS. Le serveur DNS secondaire est défini lorsque le système a une configuration redondante et qu'il existe un serveur DNS secondaire. Si vous faites partie d'une petite organisation et que vous ne configurez pas le serveur DNS, définissez l'adresse IP du routeur. |

| Divisions | Éléments | Remarque |
|-------------------------------|---|---|
| Informations du serveur Proxy | <input type="checkbox"/> Nom du serveur Proxy | Définissez ce paramètre lorsque votre environnement réseau utilise le serveur proxy pour accéder à Internet depuis l'Intranet et que vous utilisez la fonction à laquelle le scanner accède directement depuis Internet. Pour les fonctions suivantes, le scanner se connecte directement à Internet. <input type="checkbox"/> Epson Connect Services <input type="checkbox"/> Services Cloud d'autres entreprises <input type="checkbox"/> Mise à jour du micrologiciel <input type="checkbox"/> Envoi d'images numérisées à SharePoint(WebDAV) |
| Information du numéro de port | <input type="checkbox"/> Numéro de port à libérer | Vérifiez le numéro de port utilisé par le scanner et l'ordinateur, puis libérez le port qui est bloqué par un pare-feu, si nécessaire. Reportez-vous à ce qui suit pour connaître le numéro de port utilisé par le scanner. « Utilisation du port pour le scanner » à la page 33 |

Attribution d'adresse IP

Voici les types d'attribution d'adresse IP.

Adresse IP statique :

Attribuer manuellement au scanner (hôte) l'adresse IP prédéterminée.

Les informations de connexion au réseau (masque de sous-réseau, passerelle par défaut, serveur DNS, etc.) doivent être définies manuellement.

L'adresse IP ne change jamais, même lorsque l'appareil est éteint. Cela est par conséquent utile lorsque vous voulez gérer des appareils au sein d'un environnement dans lequel vous ne pouvez pas changer l'adresse IP, ou si vous voulez gérer des appareils utilisant l'adresse IP. Nous recommandons des paramètres pour les scanners, serveurs, etc. auxquels de nombreux ordinateurs accèdent. Attribuez également une adresse IP fixe afin que l'adresse IP ne change pas lors de l'utilisation de fonctions de sécurité telles que le filtrage IPsec/IP.

Attribution automatique à l'aide de la fonction DHCP (adresse IP dynamique) :

Attribuez automatiquement l'adresse IP au scanner (hôte) en utilisant la fonction DHCP du serveur DHCP ou du routeur.

Les informations de connexion au réseau (masque de sous-réseau, passerelle par défaut, serveur DNS, etc.) sont définies automatiquement, de sorte que vous puissiez facilement connecter le périphérique au réseau.

Si le périphérique ou le routeur est éteint, ou en fonction des paramètres du serveur DHCP, l'adresse IP peut changer lors de la reconnexion.

Nous vous recommandons de gérer les périphériques et non l'adresse IP, et de communiquer avec les protocoles pouvant suivre l'adresse IP.

Remarque:

Lorsque vous utilisez la fonction de réservation d'adresse IP du DHCP, vous pouvez attribuer la même adresse IP aux périphériques à tout moment.

Serveur DNS et serveur proxy

Le serveur DNS a un nom d'hôte, un nom de domaine pour l'adresse e-mail, etc. en association avec les informations d'adresse IP.

La communication est impossible si l'autre partie est décrite par un nom d'hôte, un nom de domaine, etc. lorsque l'ordinateur ou le scanner réalise une communication IP.

Interroge le serveur DNS pour obtenir ces informations et obtient l'adresse IP de l'autre partie. Ce processus est appelé une résolution de nom.

Par conséquent, les périphériques tels que les ordinateurs et les scanners peuvent communiquer en utilisant l'adresse IP.

La résolution de nom est nécessaire pour que le scanner puisse communiquer en utilisant la fonction d'e-mail ou de connexion Internet.

Définissez les paramètres du serveur DNS lorsque vous utilisez ces fonctions.

Lorsque vous attribuez l'adresse IP du scanner à l'aide de la fonction DHCP du serveur DHCP ou du routeur, elle est automatiquement définie.

Le serveur proxy est placé au niveau de la passerelle entre le réseau et Internet, et il communique avec l'ordinateur, le scanner et Internet (serveur opposé) pour le compte de chacun d'eux. Le serveur opposé communique uniquement avec le serveur proxy. Par conséquent, des informations sur le scanner telles que l'adresse IP et le numéro de port ne peuvent être lues et une sécurité renforcée est attendue.

Lorsque vous vous connectez à Internet via un serveur proxy, configurez le serveur proxy sur le scanner.

Connexion au réseau depuis le panneau de commande

Connectez le scanner au réseau, depuis le panneau de commande du scanner.

Attribution de l'adresse IP

Configurer les éléments de base comme l'adresse de l'hôte, Masque de s-réseau, Passerelle par défaut.

Ce chapitre décrit la procédure de configuration d'une adresse IP statique.

1. Mettez le scanner sous tension.
2. Sélectionnez **Param.** à l'écran d'accueil du panneau de commande du scanner.
3. Sélectionnez **Paramètres réseau > Avancé > TCP/IP.**
4. Sélectionnez **Manuel** pour **Obtenir l'adresse IP.**

Pour configurer l'adresse IP automatiquement à l'aide de la fonction DHCP du routeur, sélectionnez **Auto.** Dans ce cas, l'**Adresse IP**, le **Masque de s-réseau** et la **Passerelle par défaut** décrits aux étapes 5 à 6 sont également définis automatiquement, passez à l'étape 7.

5. Saisissez l'adresse IP.

Le curseur passe au segment suivant ou au segment précédent, séparé par un point si vous sélectionnez ◀ et ▶.

Confirmez la valeur affichée à l'écran précédent.

6. Configurez les options **Masque de s-réseau** et **Passerelle par défaut**.

Confirmez la valeur affichée à l'écran précédent.



Important:

Si la combinaison des Adresse IP, Masque de s-réseau et Passerelle par défaut est incorrecte, **Démarrer configuration** est inactive et il est impossible de poursuivre la configuration. Confirmez que la saisie est exempte d'erreur.

7. Saisissez l'adresse IP du serveur DNS principal.

Confirmez la valeur affichée à l'écran précédent.

Remarque:

Si vous pouvez sélectionner **Auto** comme paramètre d'attribution de l'adresse IP, vous pouvez sélectionner les paramètres du serveur DNS via **Manuel** ou **Auto**. Si vous ne pouvez pas obtenir automatiquement l'adresse du serveur DNS, sélectionnez **Manuel**, puis saisissez l'adresse du serveur DNS. Saisissez ensuite directement l'adresse du serveur DNS secondaire. Si vous sélectionnez **Auto**, allez à l'étape 9.

8. Saisissez l'adresse IP du serveur DNS secondaire.

Confirmez la valeur affichée à l'écran précédent.

9. Touchez **Démarrer configuration**.

Configuration du serveur proxy

Configurez le serveur proxy si les deux conditions suivantes sont remplies.

- Le serveur proxy est conçu pour une connexion Internet.
- Lorsque vous utilisez une fonction dans laquelle un scanner se connecte directement à Internet, comme le service Epson Connect ou les services Cloud d'une autre entreprise.

1. Sélectionnez **Param.** sur l'écran d'accueil.

Lorsque vous effectuez des réglages après la configuration de l'adresse IP, l'écran **Avancé** s'affiche. Passez à l'étape 3.

2. Sélectionnez **Paramètres réseau > Avancé**.

3. Sélectionnez **Serveur Proxy**.

4. Sélectionnez **Utiliser** pour **Param. Serveur proxy**.

5. Entrez l'adresse du serveur proxy au format IPv4 ou FQDN.

Confirmez la valeur affichée à l'écran précédent.

6. Saisissez le numéro de port du serveur proxy.

Confirmez la valeur affichée à l'écran précédent.

7. Touchez **Démarrer configuration**.

Connexion à Ethernet

Connectez le scanner au réseau à l'aide d'un câble LAN, puis vérifiez la connexion.

1. Connectez le scanner et le concentrateur (commutateur LAN) à l'aide d'un câble LAN.
2. Sélectionnez  sur l'écran d'accueil.
3. Sélectionnez **Routeur**.
4. Assurez-vous que les paramètres Connexion et Adresse IP sont corrects.
5. Touchez **Fermer**.

Connexion au réseau local sans fil (Wi-Fi)

Vous pouvez connecter le scanner au réseau local sans fil (Wi-Fi) de plusieurs manières. Choisissez la méthode de connexion correspondant à l'environnement et aux conditions que vous utilisez.

Si vous connaissez les informations de routeur sans fil, comme le SSID et le mot de passe, vous pouvez définir les paramètres manuellement.

Si le routeur sans fil prend en charge WPS, vous pouvez effectuer les réglages par simple pression sur un bouton.

Une fois le scanner relié au réseau, connectez-y l'appareil que vous voulez utiliser (ordinateur, périphérique intelligent, tablette, etc.)

Remarque quant à l'utilisation d'une connexion Wi-Fi 5 GHz

Ce produit utilise normalement le canal W52 (c36) lors d'une connexion à Wi-Fi Direct (PA unique). Étant donné que le canal d'une connexion au réseau local sans fil (Wi-Fi) est choisi manuellement, il peut être différent de celui utilisé pour une connexion Wi-Fi Direct simultanée. Si les canaux diffèrent, les communications de données avec le scanner peuvent être lentes. Si cela n'interfère pas avec votre utilisation, connectez-vous au SSID dans la bande 2,4 GHz. Dans la bande de fréquences 2,4 GHz, les canaux utilisés correspondent.

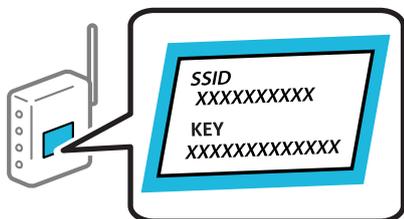
Si vous souhaitez vous connecter au LAN sans fil 5 GHz, nous vous recommandons de désactiver Wi-Fi Direct.

Définissez les paramètres Wi-Fi en saisissant le SSID et le mot de passe

Vous pouvez configurer un réseau Wi-Fi en saisissant manuellement les informations nécessaires à la connexion à un point d'accès à partir du panneau de commande du scanner. Pour procéder à la configuration à l'aide de cette méthode, vous devez disposer du SSID et du mot de passe du routeur sans fil.

Remarque:

Si vous utilisez un routeur sans fil dont les paramètres par défaut n'ont pas été modifiés, le SSID et le mot de passe figurent sur l'étiquette. Si vous ne connaissez pas le SSID et le mot de passe, contactez la personne qui a configuré le routeur sans fil ou reportez-vous à la documentation fournie avec le routeur sans fil.



1. Appuyez sur  à l'écran d'accueil.

2. Sélectionnez **Routeur**.

3. Appuyez sur **Commencer la configuration**.

Si la connexion réseau est déjà définie, les informations de connexion s'affichent. Appuyez sur **Passez en connexion Wi-Fi** ou **Modifier les param.** pour modifier les paramètres.

4. Sélectionnez **Assistant de configuration Wi-Fi**.

5. Suivez les instructions à l'écran pour sélectionner le SSID, saisissez le mot de passe pour le routeur sans fil, et démarrez la configuration.

Si vous souhaitez vérifier le statut de connexion réseau pour le scanner après que la configuration est terminée, voir le lien d'informations liées ci-dessous pour plus d'informations.

Remarque:

- Si vous ne connaissez pas le SSID, déterminez s'il figure sur l'étiquette du routeur sans fil. Si vous utilisez un routeur sans fil dont les paramètres par défaut n'ont pas été modifiés, le SSID à utiliser figure sur l'étiquette. Si vous ne trouvez aucune information, consultez la documentation fournie avec le routeur sans fil.
- Le mot de passe est sensible à la casse.
- Si vous ne connaissez pas le mot de passe, déterminez s'il figure sur l'étiquette du point d'accès. Sur l'étiquette, le mot de passe peut être écrit « Network Key », « Wireless Password », etc. Si vous utilisez un routeur sans fil dont les paramètres par défaut n'ont pas été modifiés, le mot de passe à utiliser figure sur l'étiquette.
- Si vous ne voyez pas le SSID auquel vous souhaitez vous connecter, utilisez un logiciel ou une application pour configurer le Wi-Fi depuis votre ordinateur ou périphérique intelligent, tel qu'un smartphone ou une tablette. Pour plus d'informations, saisissez « <https://epson.sn> » dans votre navigateur pour accéder au site Web, saisissez le nom de votre produit, et allez dans **Installation**.

Informations connexes

➔ « Vérification de l'état de la connexion réseau » à la page 29

Définition des paramètres Wi-Fi par configuration du bouton poussoir (WPS)

Vous pouvez configurer automatiquement un réseau Wi-Fi en appuyant sur une touche au niveau du routeur sans fil. Si les conditions suivantes sont réunies, vous pouvez utiliser cette méthode.

- Le routeur sans fil prend en charge WPS (Wi-Fi Protected Setup).
- L'actuelle connexion Wi-Fi a été établie en appuyant sur une touche au niveau du routeur sans fil.

Remarque:

Si vous ne parvenez pas à trouver la touche ou si vous procédez à la configuration à l'aide du logiciel, reportez-vous à la documentation fournie avec le routeur sans fil.

1. Appuyez sur  à l'écran d'accueil.

2. Sélectionnez **Routeur**.

3. Touchez **Commencer la configuration**.

Si la connexion réseau est déjà définie, les informations de connexion s'affichent. Appuyez sur **Passez en connexion Wi-Fi**, ou **Modifier les param.** pour modifier les paramètres.

4. Sélectionnez **Config. boutons poussoirs (WPS)**.

5. Suivez les instructions affichées à l'écran.

Si vous souhaitez vérifier le statut de connexion réseau pour le scanner après que la configuration est terminée, voir le lien d'informations liées ci-dessous pour plus d'informations.

Remarque:

En cas d'échec de la connexion, redémarrez le routeur sans fil, rapprochez-le du scanner et réessayez.

Informations connexes

➔ [« Vérification de l'état de la connexion réseau » à la page 29](#)

Définition des paramètres Wi-Fi par Paramétrage de code PIN (WPS)

Vous pouvez automatiquement vous connecter à un routeur sans fil en utilisant un code PIN. Vous pouvez utiliser cette méthode de configuration si votre routeur sans fil est compatible WPS (Wi-Fi Protected Setup). Utilisez un ordinateur pour saisir un code PIN au niveau du routeur sans fil.

1. Appuyez sur  à l'écran d'accueil.

2. Sélectionnez **Routeur**.

3. Touchez **Commencer la configuration**.

Si la connexion réseau est déjà définie, les informations de connexion s'affichent. Appuyez sur **Passez en connexion Wi-Fi**, ou **Modifier les param.** pour modifier les paramètres.

4. Sélectionnez **Autres > Config. code PIN (WPS)**

5. Suivez les instructions affichées à l'écran.

Si vous souhaitez vérifier le statut de connexion réseau pour le scanner après que la configuration est terminée, voir le lien d'informations liées ci-dessous pour plus d'informations.

Remarque:

Reportez-vous à la documentation fournie avec votre routeur sans fil pour plus de détails concernant la saisie du code PIN.

Informations connexes

➔ [« Vérification de l'état de la connexion réseau » à la page 29](#)

Ajout ou remplacement d'ordinateurs ou périphériques

Connexion à un scanner déjà présent sur le réseau

Si le scanner a déjà été connecté au réseau, vous pouvez connecter un ordinateur ou un périphérique intelligent à celui-ci grâce au réseau.

Utilisation d'un scanner réseau depuis un autre ordinateur

Nous vous conseillons d'utiliser le programme d'installation pour connecter le scanner à un ordinateur.

Pour lancer le programme d'installation, rendez-vous sur le site Web suivant et saisissez le nom du produit. Accédez à **Installation**, puis procédez à la configuration.

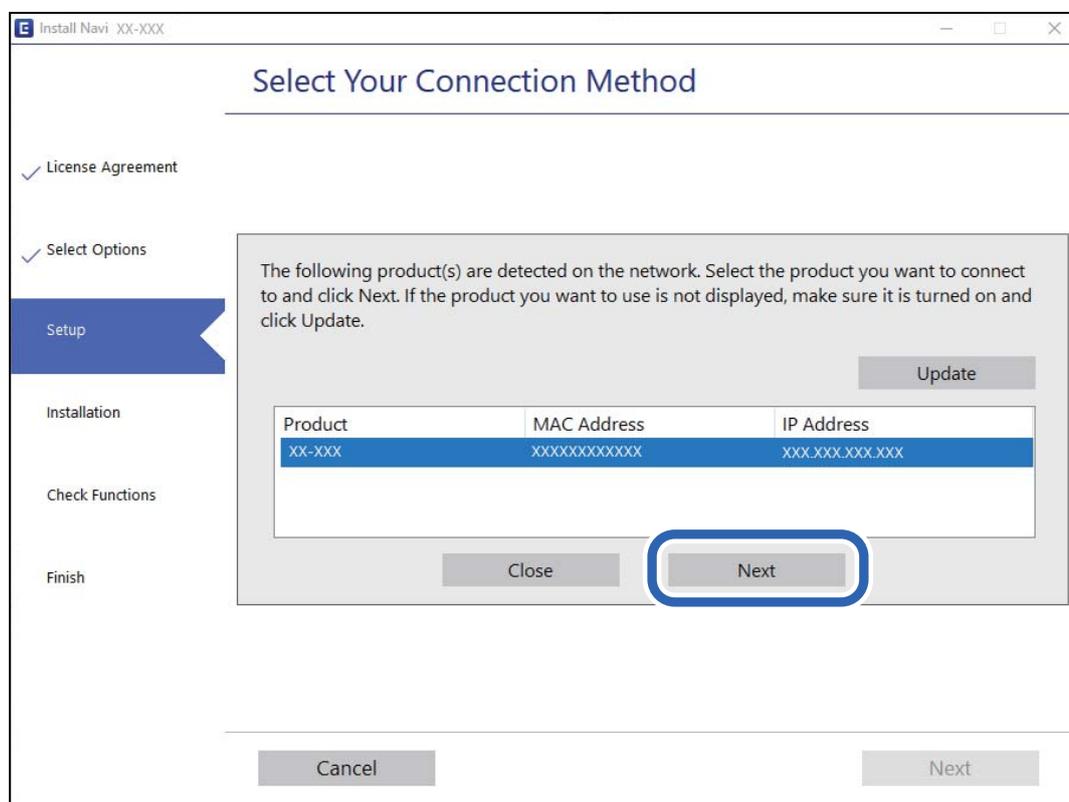
<https://epson.sn>

Vous pouvez consulter les instructions d'utilisation dans les Manuels de film Web. Accédez à l'URL suivante.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

Sélection du scanner

Suivez les instructions à l'écran jusqu'à ce que l'écran suivant s'affiche, sélectionnez le nom du scanner auquel vous souhaitez vous connecter, puis cliquez sur **Suivant**.



Suivez les instructions à l'écran.

Utilisation d'un scanner réseau depuis un périphérique intelligent

Vous pouvez connecter un périphérique intelligent au scanner grâce à l'une des méthodes suivantes.

Connexion par le biais d'un routeur sans fil

Connectez le périphérique intelligent au même réseau Wi-Fi (SSID) que le scanner.

Reportez-vous à la section suivante pour plus d'informations.

« Réglages pour connexion à un appareil intelligent » à la page 28

Connexion par Wi-Fi Direct

Connectez directement le périphérique intelligent au scanner, sans passer par un routeur sans fil.

Reportez-vous à la section suivante pour plus d'informations.

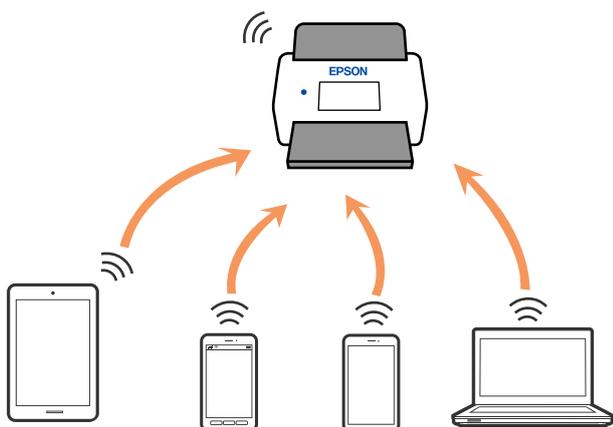
« Connexion directe d'un périphérique intelligent et le scanner (Wi-Fi Direct) » à la page 25

Connexion directe d'un périphérique intelligent et le scanner (Wi-Fi Direct)

Wi-Fi Direct (Simple AP) vous permet de connecter un périphérique intelligent au scanner sans passer par un routeur sans fil, et ainsi numériser directement depuis le périphérique intelligent.

À propos d'Wi-Fi Direct

Utilisez cette méthode de connexion lorsque vous n'utilisez pas la Wi-Fi à la maison ou au bureau, ou lorsque vous voulez connecter directement le scanner et le smartphone ou la tablette. Dans ce mode, le scanner est un routeur sans fil et vous pouvez connecter jusqu'à quatre appareils au scanner, sans utiliser de routeur sans fil standard. Toutefois, les appareils reliés directement au scanner ne peuvent pas communiquer entre eux par son intermédiaire.



Le scanner peut être connecté simultanément en Wi-Fi ou Ethernet, et Wi-Fi Direct (Simple AP). Cependant, si vous commencez une connexion réseau en mode Wi-Fi Direct (Simple AP) lorsque le scanner est connecté par Wi-Fi, le Wi-Fi est coupé provisoirement.

Connexion à un périphérique intelligent à l'aide de Wi-Fi Direct

Cette méthode vous permet de connecter directement le scanner aux périphériques intelligents sans routeur sans fil.

1. Sélectionnez  sur l'écran d'accueil.
2. Sélectionnez **Wi-Fi Direct**.
3. Sélectionnez **Commencer la configuration**.
4. Lancez Epson Smart Panel sur votre périphérique intelligent.
5. Suivez les instructions affichées sur le Epson Smart Panel pour connecter votre scanner.
Une fois que votre périphérique intelligent est connecté au scanner, passez à l'étape suivante.
6. Sur le panneau de commande du scanner, sélectionnez **Terminer**.

Arrêt d'une connexion Wi-Fi Direct (Simple AP)

Vous pouvez désactiver une connexion Wi-Fi Direct (Simple AP) de deux manières différentes : désactivez toutes les connexions à l'aide du panneau de commande du scanner, ou désactivez chaque connexion depuis l'ordinateur ou l'appareil connecté.

Si vous souhaitez désactiver toutes les connexions, sélectionnez  > **Wi-Fi Direct** > **Commencer la configuration** > **Changer** > **Désactiver Wi-Fi Direct**.



Important:

Le fait de désactiver la connexion par Wi-Fi Direct (Simple AP) déconnecte tous les ordinateurs et appareils connectés reliés au scanner via Wi-Fi Direct (Simple AP).

Remarque:

Si vous souhaitez déconnecter un périphérique spécifique, procédez à la déconnexion à partir du périphérique plutôt que du scanner. Choisissez l'une des méthodes suivantes pour désactiver la connexion Wi-Fi Direct (Simple AP) depuis l'appareil.

- Désactivez la connexion Wi-Fi au nom de réseau du scanner (SSID).
- Connectez-vous à un autre nom de réseau (SSID).

Modifier les paramètres de Wi-Fi Direct (Simple AP) tels que le SSID

Lorsque la connexion Wi-Fi Direct (Simple AP) est activée, vous pouvez modifier les paramètres dans  > **Wi-Fi Direct** > **Commencer la configuration** > **Changer**, et les éléments suivants s'affichent.

Changer le nom du réseau

Modifiez le nom du réseau (SSID) Wi-Fi Direct (Simple AP) utilisé pour se connecter au scanner à votre nom arbitraire. Vous pouvez définir le nom du réseau (SSID) en caractères ASCII affichés sur le clavier virtuel du panneau de commande. Vous pouvez saisir jusqu'à 22 caractères.

Lorsque vous changez le nom du réseau (SSID), tous les périphériques connectés sont déconnectés. Utilisez le nouveau nom de réseau (SSID) si vous souhaitez reconnecter le périphérique.

Changer le mot de passe

Modifiez le mot de passe Wi-Fi Direct (Simple AP) pour la connexion au scanner avec votre valeur arbitraire. Vous pouvez définir le mot de passe en caractères ASCII affichés sur le clavier virtuel du panneau de commande. Vous pouvez saisir de 8 à 22 caractères.

Lorsque vous changez le mot de passe, tous les périphériques connectés sont déconnectés. Utilisez le nouveau mot de passe si vous souhaitez reconnecter le périphérique.

Modifier la plage de fréquence

Modifiez la plage de fréquence de Wi-Fi Direct utilisée pour vous connecter au scanner. Vous avez le choix entre 2,4 et 5 GHz.

Lorsque vous changez de plage de fréquence, tous les appareils qui y sont connectés sont déconnectés. Reconnectez l'appareil.

Veillez noter que si vous passez à la plage de fréquence de 5 GHz, vous ne pourrez pas reconnecter les appareils qui ne prennent pas en charge cette plage de 5 GHz.

Il est possible que ce paramètre ne s'affiche pas selon la région.

Désactiver Wi-Fi Direct

Désactivez les paramètres Wi-Fi Direct (Simple AP) du scanner. Lorsque vous le désactivez, tous les périphériques connectés au scanner en connexion Wi-Fi Direct (AP simple) sont déconnectés.

Rest param défaut

Restaurez tous les paramètres Wi-Fi Direct (Simple AP) à leurs valeurs par défaut.

Les informations de connexion Wi-Fi Direct (AP simple) du périphérique intelligent enregistré sur le scanner sont supprimées.

Remarque:

*Vous pouvez également définir les paramètres suivants dans l'onglet **Réseau** > **Wi-Fi Direct** de Web Config du panneau de contrôle de l'imprimante.*

Activation ou désactivation de Wi-Fi Direct (Simple AP)

Modification du nom du réseau (SSID)

Modification du mot de passe

Modification de la plage de fréquence

Il est possible que ce paramètre ne s'affiche pas selon la région.

Restauration des paramètres Wi-Fi Direct (Simple AP)

Réinitialisation de la connexion réseau

Cette section explique comment procéder aux réglages de la connexion réseau et changer la méthode de connexion lorsque vous remplacez votre routeur sans fil ou votre ordinateur.

Lors d'un changement de routeur sans fil

Lorsque vous changez de routeur sans fil, réglez la connexion entre l'ordinateur ou le périphérique intelligent et le scanner.

Vous devez définir ces paramètres si vous changez de fournisseur d'accès Internet, etc.

Réglages pour connexion à l'ordinateur

Nous vous conseillons d'utiliser le programme d'installation pour connecter le scanner à un ordinateur.

Pour lancer le programme d'installation, rendez-vous sur le site Web suivant et saisissez le nom du produit. Accédez à **Installation**, puis procédez à la configuration.

<https://epson.sn>

Vous pouvez consulter les instructions d'utilisation dans les Manuels de film Web. Accédez à l'URL suivante.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

Sélection d'une méthode de connexion

Suivez les instructions à l'écran. À l'écran **Sélectionnez l'option Installer**, sélectionnez **Configurer à nouveau la connexion Imprimante (pour un nouveau routeur réseau ou une modification de l'USB vers le réseau, etc.)**, puis cliquez sur **Suivant**.

Suivez les instructions qui s'affichent à l'écran pour terminer la configuration.

Si vous ne pouvez pas vous connecter, reportez-vous aux informations suivantes pour essayer de résoudre le problème.

« Impossible de se connecter à un réseau » à la page 35

Réglages pour connexion à un appareil intelligent

Vous pouvez utiliser le scanner depuis un appareil connecté, à la condition qu'ils soient tous les deux connectés au même réseau Wi-Fi (SSID). Pour utiliser le scanner depuis un appareil intelligent, rendez-vous sur le site Web suivant, puis saisissez le nom du produit. Accédez à **Installation**, puis procédez à la configuration.

<https://epson.sn>

Accédez au site Web depuis l'appareil intelligent que vous souhaitez connecter au scanner.

Lors d'un changement d'ordinateur

Lorsque vous changez d'ordinateur, réglez la connexion entre celui-ci et le scanner.

Réglages pour connexion à l'ordinateur

Nous vous conseillons d'utiliser le programme d'installation pour connecter le scanner à un ordinateur.

Pour lancer le programme d'installation, rendez-vous sur le site Web suivant et saisissez le nom du produit. Accédez à **Installation**, puis procédez à la configuration.

<https://epson.sn>

Vous pouvez consulter les instructions d'utilisation dans les Manuels de film Web. Accédez à l'URL suivante.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

Suivez les instructions à l'écran.

Modification de la méthode de connexion à l'ordinateur

Cette section indique comment changer de méthode de connexion lorsque l'ordinateur et le scanner sont connectés.

Passer d'une connexion réseau Ethernet à Wi-Fi

Passage d'une connexion Ethernet au Wi-Fi depuis le panneau de commande du scanner. La méthode utilisée pour changer de type de connexion est la même que pour paramétrer la connexion Wi-Fi.

Informations connexes

➔ « [Connexion au réseau local sans fil \(Wi-Fi\)](#) » à la page 21

Passer d'une connexion réseau Wi-Fi à Ethernet

Procédez comme suit pour passer d'une connexion Wi-Fi à Ethernet.

1. Sélectionnez **Param.** à l'écran d'accueil.
2. Sélectionnez **Paramètres réseau > Config LAN filaire.**
3. Suivez les instructions affichées à l'écran.

Passer d'une connexion USB à une connexion réseau

Utilisez le programme d'installation et paramétrez une autre méthode de connexion.

Rendez-vous sur le site Web suivant, puis saisissez le nom du produit. Accédez à **Installation**, puis procédez à la configuration.

<https://epson.sn>

Sélection de Changer de méthode de connexion

Suivez les instructions indiquées dans chaque fenêtre. À l'écran **Sélectionnez l'option Installer**, sélectionnez **Configurer à nouveau la connexion Imprimante (pour un nouveau routeur réseau ou une modification de l'USB vers le réseau, etc.)**, puis cliquez sur **Suivant**.

Sélectionnez la connexion réseau que vous souhaitez utiliser, **Connecter via réseau sans fil (Wi-Fi)** ou **Connecter via LAN câblé (Ethernet)** puis cliquez sur **Suivant**.

Suivez les instructions qui s'affichent à l'écran pour terminer la configuration.

Vérification de l'état de la connexion réseau

Vous pouvez vérifier l'état de la connexion réseau de la façon suivante.

Vérification de l'état de la connexion réseau depuis le panneau de commande

Vous pouvez vérifier le statut de la connexion réseau à l'aide de l'icône réseau ou des informations réseau du panneau de commande du scanner.

Vérification de l'état de la connexion réseau à l'aide de l'icône réseau

Vous pouvez vérifier le statut de la connexion réseau et la puissance du signal radio à l'aide de l'icône réseau de l'écran d'accueil du scanner.



| | |
|--|--|
| | Affiche l'état de la connexion réseau. Sélectionnez l'icône pour vérifier et modifier les paramètres actuels. Il s'agit du raccourci vers le menu suivant. Param. > Paramètres réseau > Configuration Wi-Fi |
| | Le scanner n'est pas connecté à un réseau sans fil (Wi-Fi). |
| | Le scanner recherche un SSID, une adresse IP non connectée ou a un problème avec un réseau sans fil (Wi-Fi). |
| | Le scanner est connecté à un réseau sans fil (Wi-Fi). Le nombre de barres indique la force du signal de la connexion. Plus le nombre de barres est élevé, plus le signal est fort. |
| | Le scanner n'est pas connecté à un réseau sans fil (Wi-Fi) en mode Wi-Fi Direct (Simple AP). |
| | Le scanner est connecté à un réseau sans fil (Wi-Fi) en mode Wi-Fi Direct (Simple AP). |
| | Le scanner n'est pas connecté à un réseau filaire (Ethernet) ou celui-ci n'est pas activé. |
| | Le scanner est connecté à un réseau filaire (Ethernet). |

Consultation des informations détaillées liées au réseau sur le panneau de commande

Si votre scanner est connecté au réseau, vous pouvez également afficher d'autres informations liées au réseau en sélectionnant les menus réseau que vous souhaitez consulter.

1. Sélectionnez **Param.** sur l'écran d'accueil.
2. Sélectionnez **Paramètres réseau > État réseau.**

3. Pour consulter les informations, sélectionnez les menus que vous souhaitez afficher.

État LAN câblé/Wi-Fi

Affiche les informations liées au réseau (nom du périphérique, connexion, force du signal, etc.) pour les connexions Ethernet ou Wi-Fi.

État Wi-Fi Direct

Indique si Wi-Fi Direct est activé ou désactivé, le SSID, le mot de passe etc. pour les connexions Wi-Fi Direct.

État serveur de messagerie

Affiche les informations liées au réseau pour le serveur de messagerie électronique.

Caractéristiques réseau

Caractéristiques du Wi-Fi

Reportez-vous au tableau ci-dessous pour connaître les caractéristiques du Wi-Fi.

| | |
|--|--|
| Pays ou régions à l'exception de ceux répertoriés ci-dessous | Tableau A |
| Irlande, Royaume-Uni, Autriche, Allemagne, Liechtenstein, Suisse, France, Belgique, Luxembourg, Pays-Bas, Italie, Portugal, Espagne, Danemark, Finlande, Norvège, Suède, Islande, Croatie, Chypre, Grèce, Macédoine du Nord, Serbie, Slovénie, Malte, Bosnie-Herzégovine, Kosovo, Monténégro, Albanie, Bulgarie, Tchéquie, Estonie, Hongrie, Lettonie, Lituanie, Pologne, Roumanie, Slovaquie, Israël, Australie, Nouvelle-Zélande, Taïwan | Tableau B |
| Turquie | DS-900WN : Numéros de série commençant par XDA8 : Tableau A Numéros de série commençant par XDA7 : Tableau B |
| | DS-800WN : Numéros de série commençant par XDA2 : Tableau A Numéros de série commençant par XD9Z : Tableau B |

Tableau A

| | |
|---|--|
| Normes | IEEE 802.11b/g/n*1 |
| Plage de fréquences | 2 400–2 483,5 MHz |
| Puissance maximale de la radiofréquence émise | 20 dBm (EIRP) |
| Canaux | 1/2/3/4/5/6/7/8/9/10/11/12/13 |
| Modes de connexion | Infrastructure, Wi-Fi Direct (PA unique)*2*3 |

| | |
|-------------------------|---|
| Protocole de sécurité*4 | WEP (64/128bit), WPA2-PSK (AES)*5, WPA3-SAE (AES), WPA2/WPA3-Enterprise |
|-------------------------|---|

*1 Disponible uniquement pour le HT20.

*2 Non compatible avec la norme IEEE 802.11b.

*3 Les modes Infrastructure et Wi-Fi Direct ou une connexion Ethernet peuvent être utilisés simultanément.

*4 Le Wi-Fi Direct ne prend en charge que le WPA2-PSK (AES).

*5 Conforme aux normes WPA2 avec gestion de WPA/WPA2 Personal.

Tableau B

| | | | |
|-------------------------|---|---------|---|
| Normes | IEEE 802.11a/b/g/n*1/ac | | |
| Plages de fréquences | IEEE 802.11b/g/n : 2,4 GHz, IEEE 802.11a/n/ac : 5 GHz | | |
| Canaux | Wi-Fi | 2,4 GHz | 1/2/3/4/5/6/7/8/9/10/11/12*2/13*2 |
| | | 5 GHz*3 | W52 (36/40/44/48), W53 (52/56/60/64), W56 (100/104/108/112/116/120/124/128/132/136/140/144), W58 (149/153/157/161/165) |
| | Wi-Fi Direct | 2,4 GHz | 1/2/3/4/5/6/7/8/9/10/11/12*2/13*2 |
| | | 5 GHz*3 | W52 (36/40/44/48) W58 (149/153/157/161/165) |
| Modes de connexion | Infrastructure, Wi-Fi Direct (PA unique)*4, *5 | | |
| Protocole de sécurité*6 | WEP (64/128bit), WPA2-PSK (AES)*7, WPA3-SAE (AES), WPA2/WPA3-Enterprise | | |

*1 Disponible uniquement pour le HT20.

*2 Non disponible à Taiwan.

*3 La disponibilité de ces canaux et l'utilisation des produits en extérieur sur ces canaux varient en fonction de la localisation. Pour plus d'informations, visitez le site Web <http://support.epson.net/wifi5ghz/>

*4 Non compatible avec la norme IEEE 802.11b.

*5 Les modes Infrastructure et Wi-Fi Direct ou une connexion Ethernet peuvent être utilisés simultanément.

*6 Le Wi-Fi Direct ne prend en charge que le WPA2-PSK (AES).

*7 Conforme aux normes WPA2 avec gestion de WPA/WPA2 Personal.

Caractéristiques Ethernet

| | |
|-----------------------|---|
| Normes | IEEE802.3i (10BASE-T)*1 IEEE802.3u (100BASE-TX)*1 IEEE802.3ab (1000BASE-T)*1 IEEE802.3az (Ethernet économique)*2 |
| Mode de communication | Auto, Duplex intégral 10 Mbps, Semi-duplex 10 Mbps, Duplex intégral 100 Mbps, Semi-duplex 100 Mbps |

| | |
|------------|-------|
| Connecteur | RJ-45 |
|------------|-------|

- *1 Utilisez un câble STP (paire torsadée blindée) de catégorie 5e ou supérieur pour prévenir le risque d'interférences radio.
- *2 L'appareil connecté doit être conforme aux normes IEEE802.3az.

Fonctionnalités réseau et prise en charge IPv4/IPv6

| Fonctionnalités | Pris en charge |
|---------------------------------------|----------------|
| Epson Scan 2 | IPv4, IPv6 |
| Document Capture Pro/Document Capture | IPv4 |

Protocole de sécurité

| | |
|---------------------------|----------------------|
| IEEE802.1X* | |
| Filtrage IP/IPsec | |
| SSL/TLS | Serveur/client HTTPS |
| SMTPS (STARTTLS, SSL/TLS) | |
| SNMPv3 | |

* Vous devez utiliser un périphérique de connexion conforme à IEEE802.1X.

Utilisation du port pour le scanner

Le scanner utilise le port suivant. L'administrateur réseau doit rendre ces ports disponibles, si nécessaire.

Lorsque l'expéditeur (client) est le scanner

| Utiliser | Destination (Serveur) | Protocole | Numéro de port | |
|---|-----------------------|----------------------|-----------------------|-----|
| Envoi de fichiers (lorsque la numérisation vers le dossier réseau est utilisée depuis le scanner) | Serveur FTP/FTPS | FTP/FTPS (TCP) | 20 | |
| | | | 21 | |
| | Serveur du fichier | SMB (TCP) | NetBIOS (UDP) | 445 |
| | | | | 137 |
| | | | | 138 |
| | | | | 139 |
| | Serveur WebDAV | Protocole HTTP (TCP) | Protocole HTTPS (TCP) | 80 |
| | | | | 443 |

| Utiliser | Destination (Serveur) | Protocole | Numéro de port |
|--|-----------------------|---|----------------|
| Envoi de l'email (Lorsque la numérisation vers e-mail est utilisée depuis le scanner) | Serveur SMTP | SMTP (TCP) | 25 |
| | | SMTP SSL/TLS (TCP) | 465 |
| | | SMTP STARTTLS (TCP) | 587 |
| POP avant la connexion SMTP (Lorsque la numérisation vers l'e-mail est utilisée depuis le scanner) | Serveur POP | POP3 (TCP) | 110 |
| Lors de l'utilisation d'Epson Connect | Serveur Epson Connect | HTTPS | 443 |
| | | XMPP | 5222 |
| Recueil d'informations sur l'utilisateur (Utilisez les contacts du scanner) | Serveur LDAP | LDAP (TCP) | 389 |
| | | LDAP SSL/TLS (TCP) | 636 |
| | | LDAP STARTTLS (TCP) | 389 |
| Authentification de l'utilisateur lors du recueil d'informations sur l'utilisateur (Lors de l'utilisation des contacts du scanner) Authentification de l'utilisateur lors de l'utilisation de la numérisation vers le dossier réseau (SMB) du scanner | Serveur KDC | Kerberos | 88 |
| Contrôle WSD | Ordinateur client | WSD (TCP) | 5357 |
| Recherche d'un ordinateur lors de la numérisation push depuis une application | Ordinateur client | Découverte de la numérisation poussée du réseau | 2968 |

Lorsque l'expéditeur (client) est l'ordinateur client

| Utiliser | Destination (Serveur) | Protocole | Numéro de port |
|---|-----------------------|--------------------------------|----------------|
| Recherche du scanner à partir d'une application comme EpsonNet Config ou un pilote de scanner. | Scanner | ENPC (UDP) | 3289 |
| Recherche et configuration des informations MIB à partir d'une application comme EpsonNet Config ou un pilote de scanner. | Scanner | SNMP (UDP) | 161 |
| Recherche scanner WSD | Scanner | WS-Discovery (UDP) | 3702 |
| Transfert des données de numérisation depuis une application | Scanner | Numérisation réseau (TCP) | 1865 |
| Collecte des informations sur la tâche lors de la numérisation push depuis une application | Scanner | Numérisation poussée du réseau | 2968 |
| Web Config | Scanner | HTTP (TCP) | 80 |
| | | HTTPS (TCP) | 443 |

Résolution des problèmes

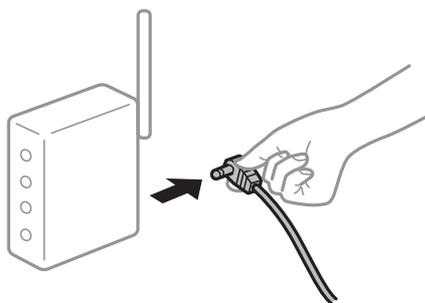
Impossible de se connecter à un réseau

Ce problème peut provenir de l'un des éléments suivants.

■ Un problème est survenu au niveau de la connexion Wi-Fi des périphériques réseau.

Solutions

Éteignez les appareils que vous voulez connecter au réseau. Attendez 10 secondes puis allumez les appareils dans l'ordre suivant : routeur sans fil, ordinateur ou périphérique intelligent, puis scanner. Rapprochez le scanner et l'ordinateur ou le périphérique intelligent du routeur sans fil, pour faciliter les communications radio, puis essayez de redéfinir les paramètres réseau.



■ Les appareils ne reçoivent aucun signal du routeur sans fil, car ils sont trop éloignés.

Solutions

Après avoir rapproché l'ordinateur ou le périphérique intelligent et le scanner du routeur sans fil, éteignez celui-ci et rallumez-le.

■ Lorsque vous changez de routeur sans fil, les paramètres ne correspondent plus au nouveau routeur.

Solutions

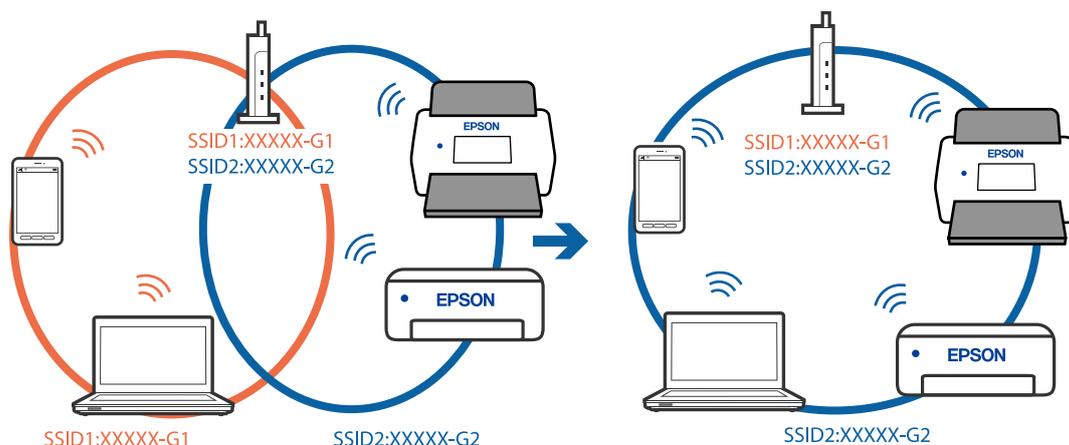
Modifiez les paramètres de connexion afin qu'ils correspondent au nouveau routeur sans fil.

■ Les SSID utilisés par l'ordinateur et le périphérique intelligent ne sont pas les mêmes.

Solutions

Si vous utilisez plusieurs routeurs sans fil en même temps ou si votre routeur sans fil diffuse plusieurs SSID et que les périphériques sont connectés à des SSID différents, vous ne pouvez pas vous connecter au routeur sans fil.

Connectez l'ordinateur, le smartphone ou la tablette au même SSID que le scanner.



■ Votre routeur sans fil propose une fonction d'isolation.

Solutions

La plupart des routeurs sans fil présentent une fonctionnalité d'isolation qui empêche les appareils connectés de communiquer entre eux. Si vous ne parvenez pas à établir de communication entre le scanner et l'ordinateur ou le périphérique connecté, pourtant sur le même réseau, désactivez cette isolation au niveau du routeur sans fil. Reportez-vous au manuel fourni avec le routeur sans fil pour plus de détails.

■ L'adresse IP n'est pas correctement attribuée.

Solutions

Si l'adresse IP attribuée au scanner est 169.254.XXX.XXX et le masque de sous-réseau 255.255.0.0, l'adresse IP peut ne pas être correctement attribuée.

Sélectionnez **Param. > Paramètres réseau > Avancé > Config TCP/IP** sur le panneau de commande du scanner et vérifiez l'adresse IP et le masque de sous-réseau attribués au scanner.

Redémarrez le routeur sans fil ou réinitialisez les paramètres réseau du scanner.

■ Les paramètres réseau de l'ordinateur posent problème.

Solutions

Essayez d'accéder à un site Web depuis votre ordinateur pour vérifier que ses paramètres réseau sont corrects. Si vous n'arrivez pas à accéder au Web, le problème vient de l'ordinateur.

Vérifiez de la connexion réseau de l'ordinateur. Reportez-vous à la documentation fournie avec l'ordinateur pour plus de détails.

■ Le scanner est connecté en Ethernet par le biais de périphériques compatibles avec la norme IEEE 802.3az (Green Ethernet).

Solutions

Selon votre concentrateur ou routeur, vous pourrez rencontrer les problèmes suivants lorsque vous connectez le scanner par Ethernet à l'aide d'appareils compatibles avec la norme IEEE 802.3az (Green Ethernet).

- La connexion est instable, le scanner est sans cesse déconnecté et reconnecté.
- La connexion au scanner est impossible.

- La vitesse de communication est basse.

Procédez comme suit pour désactiver IEEE 802.3az au niveau du scanner et établir une connexion.

1. Débranchez le câble Ethernet reliant l'ordinateur au scanner.
2. Si l'option IEEE 802.3az est activée sur l'ordinateur, désactivez-la.
Reportez-vous à la documentation fournie avec l'ordinateur pour plus de détails.
3. Connectez directement l'ordinateur au scanner à l'aide d'un câble Ethernet.
4. Sur le scanner, vérifiez les paramètres réseau.
Sélectionnez **Param.** > **Paramètres réseau** > **État réseau** > **État LAN câblé/Wi-Fi**.
5. Vérifiez l'adresse IP du scanner.
6. Sur l'ordinateur, lancez Web Config.
Ouvrez un navigateur Web et saisissez l'adresse IP du scanner.
[« Comment exécuter Web Config dans un navigateur Web »](#) à la page 39
7. Sélectionnez l'onglet **Réseau** > **Réseau local câblé**.
8. Sélectionnez **ARRÊT** pour **IEEE 802.3az**.
9. Cliquez sur **Suivant**.
10. Cliquez sur **OK**.
11. Débranchez le câble Ethernet reliant l'ordinateur au scanner.
12. Si vous avez désactivé l'option IEEE 802.3az sur l'ordinateur à l'étape 2, réactivez-la.
13. Rebranchez le câble Ethernet que vous avez débranché à l'étape 1 entre l'ordinateur et le scanner.
Si le problème persiste, c'est qu'il vient d'un autre appareil que le scanner.

■ Le scanner est hors tension.

Solutions

Vérifiez que le scanner est sous tension.

Attendez également que le voyant d'état arrête de clignoter, indiquant que le scanner est prêt à procéder à la numérisation.

Logiciel pour la configuration du scanner

| | |
|---|----|
| Application de configuration des opérations du scanner (Web Config) | 39 |
| Epson Device Admin. | 40 |

Application de configuration des opérations du scanner (Web Config)

Web Config est une application qui fonctionne dans un navigateur Web, par exemple Microsoft Edge ou Safari, sur un ordinateur ou un appareil intelligent. Vous pouvez vérifier le statut du scanner ou modifier les paramètres du service réseau et du scanner. Connectez le scanner et l'ordinateur ou l'appareil au même réseau pour pouvoir utiliser Web Config.

Les navigateurs suivants sont pris en charge. Utilisez la version la plus récente.

Microsoft Edge, Windows Internet Explorer, Firefox, Chrome, Safari

Remarque:

Vous serez peut-être amené à saisir le mot de passe administrateur lors de l'utilisation de cet appareil. Reportez-vous à ce qui suit pour en savoir plus sur le mot de passe administrateur.

[« Remarques concernant le mot de passe administrateur » à la page 11](#)

Informations connexes

➔ [« Accès impossible à Web Config » à la page 67](#)

Comment exécuter Web Config dans un navigateur Web

Ce scanner est livré avec un logiciel intégré nommé Web Config (une page Web dans laquelle vous pouvez effectuer des réglages). Pour accéder à Web Config, utilisez un navigateur et saisissez l'adresse IP d'un scanner connecté au réseau.

1. Vérifiez l'adresse IP du scanner.

Sélectionnez **Param.** > **Paramètres réseau** > **État réseau** sur le panneau de commande du scanner. Sélectionnez ensuite la méthode de connexion active (**État LAN câblé/Wi-Fi** ou **État Wi-Fi Direct**) pour vérifier l'adresse IP du scanner.

Exemple d'adresse IP : 192.168.100.201

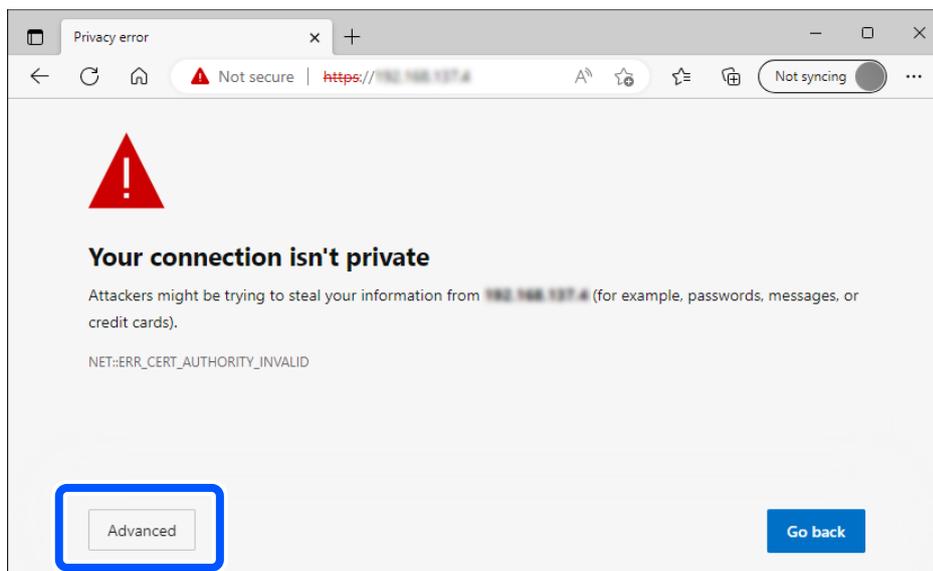
2. Lancez un navigateur depuis un ordinateur ou un appareil intelligent, puis saisissez l'adresse IP du scanner dans la barre d'adresse.

Format : http://adresse IP du scanner/

Exemple : http://192.168.100.201/

Si un écran d'avertissement s'affiche dans votre navigateur, vous pouvez l'ignorer en toute sécurité et afficher la page Web (Web Config). Étant donné que le scanner utilise un certificat autosigné lors d'un accès HTTPS, un avertissement s'affiche lorsque vous lancez Web Config ; mais il n'indique pas un problème et vous pouvez l'ignorer. Selon votre navigateur, vous devrez peut-être cliquer sur **Paramètres avancés** pour afficher la page Web.

Exemple : pour Microsoft Edge



Remarque:

Si aucun écran d'avertissement ne s'affiche, passez à l'étape suivante.

Pour les adresses IPv6, utilisez le format suivant.

Format : `http://[adresse IP du scanner]/`

Exemple : `http://[2001:db8::1000:1]/`

3. Pour modifier les paramètres du scanner, vous devrez vous connecter en tant qu'administrateur dans Web Config.

Cliquez sur **se connecter** en haut à droite de l'écran. Saisissez le **Nom d'utilisateur** et le **MdPasse actuel**, puis cliquez sur **OK**.

Les éléments suivants indiquent les valeurs initiales des informations d'administration de Web Config.

·Nom d'utilisateur : aucun (vierge)

·Mot de passe : indiqué sur l'étiquette collée sur le produit.

Si une étiquette « PASSWORD » se trouve à l'arrière, saisissez le nombre à 8 chiffres indiqué dessus. Si aucune étiquette « PASSWORD » n'est présente, saisissez le numéro de série situé à l'arrière du produit en guise de mot de passe administrateur initial.

Remarque:

Si **déconnexion** s'affiche en haut à droite de l'écran, vous êtes déjà connecté en tant qu'administrateur.

Vous serez automatiquement déconnecté après environ 20 minutes d'inactivité.

Epson Device Admin

Epson Device Admin est une application multifonctionnelle qui vous permet de gérer des périphériques sur un réseau.

Vous pouvez utiliser des modèles de configuration pour appliquer des paramètres unifiés à plusieurs scanners sur un réseau, ce qui permet d'installer et de gérer plusieurs scanners.

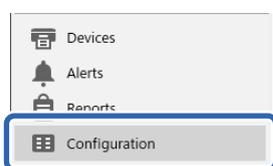
Vous pouvez télécharger Epson Device Admin depuis le site Web d'assistance Epson. Pour plus de détails sur l'utilisation de cette application, consultez la documentation ou l'aide pour Epson Device Admin.

Modèle de configuration

Création du modèle de configuration

Créez le nouveau modèle de configuration.

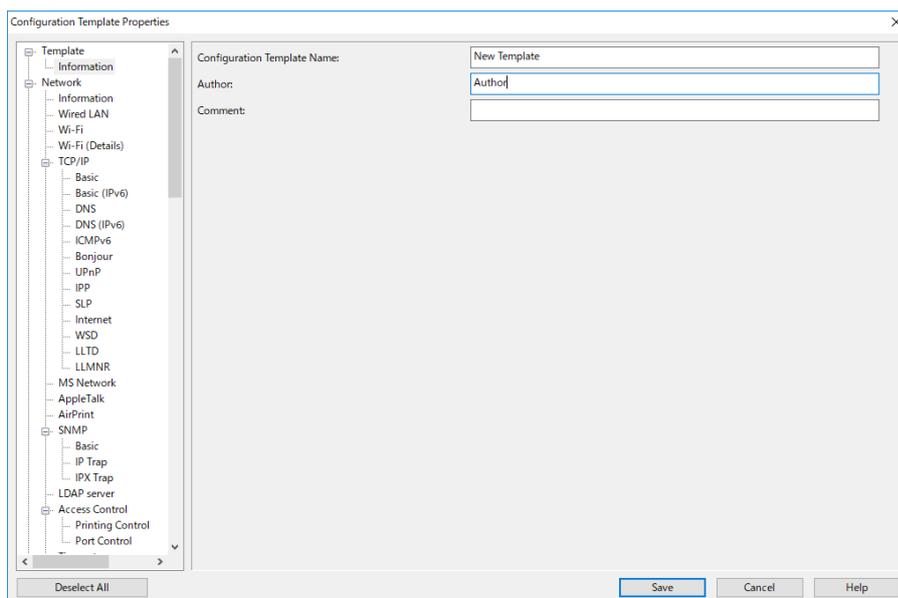
1. Lancez l'application Epson Device Admin.
2. Sélectionnez **Configuration** dans le menu des tâches de la barre latérale.



3. Sélectionnez **Nouveau** dans le menu ruban.



4. Réglez chaque élément.



| Élément | Explication |
|--------------------------------|---|
| Nom du modèle de configuration | Nom du modèle de configuration. Saisissez jusqu'à 1024 caractères Unicode (UTF-8). |
| Auteur | Informations sur le créateur du modèle. Saisissez jusqu'à 1024 caractères Unicode (UTF-8). |
| Commentaire | Saisissez des informations arbitraires. Saisissez jusqu'à 1024 caractères Unicode (UTF-8). |

- Sélectionnez les éléments que vous souhaitez définir sur la gauche.

Remarque:

Cliquez sur les éléments de menu à gauche pour basculer entre les écrans. La valeur définie est uniquement conservée si vous changez d'écran, elle ne l'est pas si vous annulez l'écran. Lorsque vous avez terminé de définir les paramètres, cliquez sur **Enregistrer**.

Application du modèle de configuration

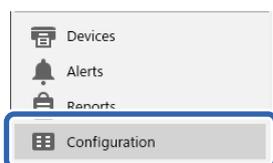
Appliquez le modèle de configuration enregistré au scanner. Les éléments sélectionnés sur le modèle sont appliqués. Si le scanner cible ne dispose pas de la fonction appropriée, elle n'est pas appliquée.

Remarque:

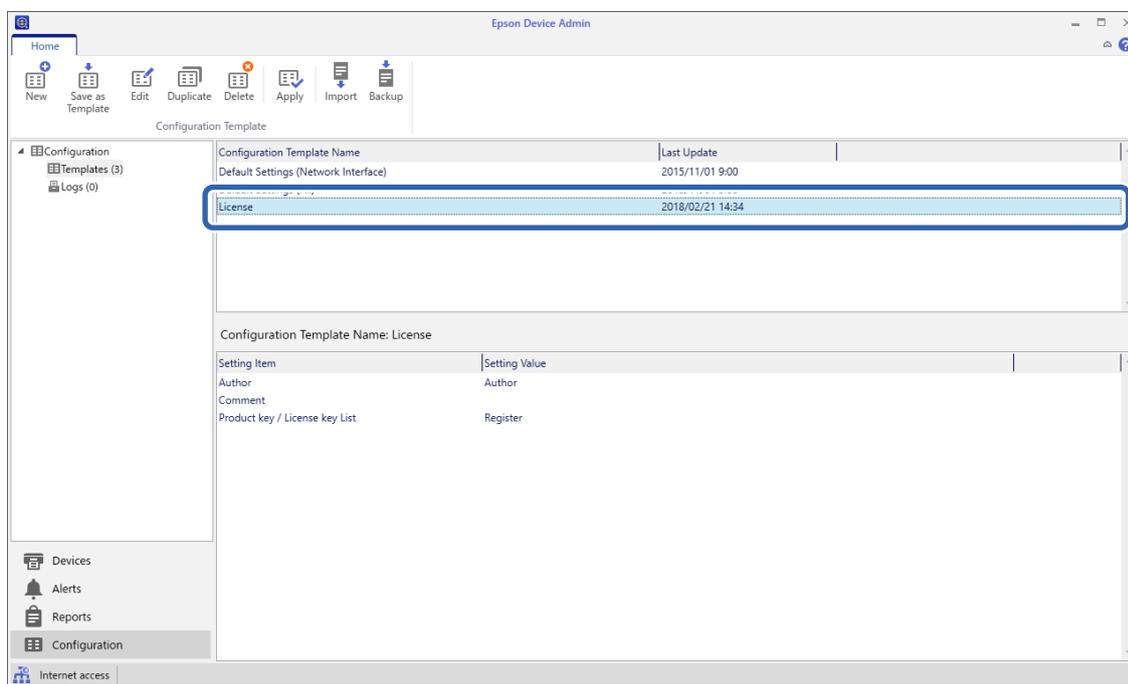
Si un mot de passe administrateur est défini sur le scanner, configurez le mot de passe au préalable.

- Dans le menu ruban de l'écran de la liste de périphériques, sélectionnez **Options > Gestion des mots de passe**.
- Sélectionnez **Activer la gestion automatique des mots de passe** et cliquez sur **Gestion des mots de passe**.
- Sélectionnez le scanner approprié, puis cliquez sur **Modifier**.
- Définissez le mot de passe, puis cliquez sur **OK**.

- Sélectionnez **Configuration** dans le menu des tâches de la barre latérale.



- Sélectionnez le modèle de configuration que vous souhaitez appliquer dans **Nom du modèle de configuration**.



- Cliquez sur **Appliquer** dans le menu ruban.
L'écran de sélection de périphérique s'affiche.

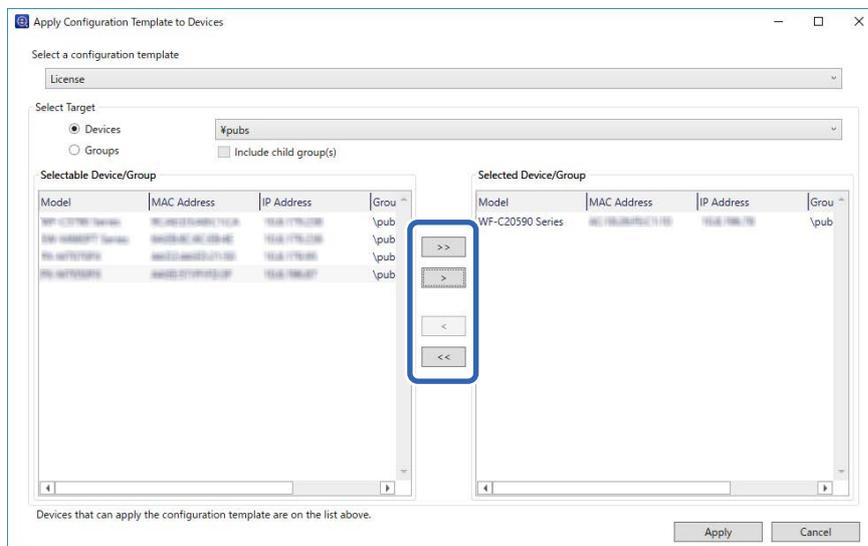


- Sélectionnez le modèle de configuration que vous souhaitez appliquer.

Remarque:

- Lorsque vous sélectionnez **Imprimantes** et des groupes contenant des périphériques dans le menu déroulant, chaque périphérique est affiché.
- Les groupes s'affichent lorsque vous sélectionnez **Groupes**. Sélectionnez **Inclure groupe(s) d'enfants** pour sélectionner automatiquement des groupes d'enfants dans le groupe sélectionné.

- Déplacez le scanner ou les groupes auxquels vous souhaitez appliquer le modèle vers **Appareil/Groupe sélectionné**.



- Cliquez sur **Appliquer**.

Un écran de confirmation d'application du modèle de configuration s'affiche.

- Cliquez sur **OK** pour appliquer le modèle de configuration.

- Lorsqu'un message s'affiche vous informant que la procédure est terminée, cliquez sur **OK**.

- Cliquez sur **Détails** et vérifiez les informations.

Si s'affiche sur les éléments que vous avez appliqués, l'application s'est déroulée avec succès.

- Cliquez sur **Fermer**.

Paramètres requis pour la numérisation

| | |
|--|----|
| Enregistrer un serveur de messagerie. | 46 |
| Créer un dossier réseau. | 49 |
| Mise à disposition des contacts. | 56 |
| Configuration de AirPrint. | 66 |
| Problèmes lors de la préparation de la numérisation du réseau. | 67 |

Enregistrer un serveur de messagerie

Vérifiez les éléments suivants avant de configurer le serveur de messagerie.

- Le scanner est connecté au réseau
- Informations de configuration du serveur de messagerie

Si vous faites appel à un serveur de messagerie qui utilise Internet, vérifiez les paramètres auprès de votre fournisseur ou de son site Web.

Comment enregistrer

Rendez-vous dans Web Config, sélectionnez l'onglet **Réseau > Serveur d'email > De base**.

« [Comment exécuter Web Config dans un navigateur Web](#) » à la page 39

Vous pouvez également effectuer ces réglages depuis le panneau de commande du scanner. Sélectionnez **Param.** > **Paramètres réseau > Avancé > Serveur d'email > Param. serveur**.

Éléments de configuration du serveur de messagerie

| Élément | Paramètres et explication | |
|----------------------------|--|--|
| Méthode d'authentification | Définissez le mode d'authentification permettant au scanner d'accéder au serveur de messagerie. | |
| | Désactiver | L'authentification est désactivée en cas de communication avec un serveur de messagerie. |
| | SMTP-AUTH | Le serveur de messagerie doit être compatible avec l'authentification SMTP. |
| | POP avant SMTP | Configurez le serveur POP3 si vous utilisez ce paramètre. |
| Compte authentifié | Si vous avez réglé le paramètre Méthode d'authentification sur SMTP-AUTH ou POP avant SMTP , saisissez le nom du compte authentifié. Saisissez entre 0 et 255 caractères au format ASCII (0x20 à 0x7E). | |
| Mot de passe authentifié | Si vous avez réglé le paramètre Méthode d'authentification sur SMTP-AUTH ou POP avant SMTP , saisissez le mot de passe d'authentification. Saisissez entre 0 et 20 caractères au format ASCII (0x20 à 0x7E). | |
| Adr. messagerie expéditeur | Définissez l'adresse e-mail qui sera utilisée pour envoyer les e-mails depuis le scanner. Bien qu'il soit possible d'utiliser une adresse e-mail existante, nous vous recommandons de configurer une adresse e-mail dédiée afin de la distinguer des e-mails envoyés par le scanner. Saisissez entre 0 et 255 caractères au format ASCII (0x20 à 0x7E), sauf : () < > [] ; ¥. Le premier caractère ne peut être un point (. | |
| Adresse du serveur SMTP | Saisissez entre 0 et 255 caractères en utilisant A – Z a – z 0 – 9 . -. Vous pouvez utiliser le format IPv4 ou FQDN. | |
| Numéro port serveur SMTP | Saisissez un nombre entre 1 et 65535. | |

| Élément | Paramètres et explication | |
|---|--|--|
| Connexion sécurisée | Spécifiez la méthode de connexion sécurisée pour le serveur de messagerie. | |
| | Aucun | Si vous sélectionnez POP avant SMTP dans Méthode d'authentification , la méthode de connexion est définie sur Aucun . |
| | SSL/TLS | Cette option est disponible lorsque la Méthode d'authentification est réglée sur Désactiver ou SMTP-AUTH . |
| | STARTTLS | Cette option est disponible lorsque la Méthode d'authentification est réglée sur Désactiver ou SMTP-AUTH . |
| Validation certificat (Web Config uniquement) | Le certificat est validé lorsque cette option est activée. Nous vous recommandons de régler ce paramètre sur Activer si le paramètre Connexion sécurisée est réglé sur autre chose que Aucun . | |
| Adresse du serveur POP3 | Si vous avez réglé le paramètre Méthode d'authentification sur POP avant SMTP , saisissez l'adresse du serveur POP3. Saisissez entre 0 et 255 caractères parmi A – Z, a – z et 0 – 9. Vous pouvez utiliser le format IPv4 ou FQDN. | |
| Numéro port serveur POP3 | Défini lorsque vous sélectionnez POP avant SMTP dans Méthode d'authentification . Saisissez un nombre entre 1 et 65535. | |

Informations connexes

➔ [« Comment exécuter Web Config dans un navigateur Web » à la page 39](#)

Vérifier la connexion à un serveur de messagerie

1. Sélectionnez le menu de test de la connexion.

Configuration depuis Web Config :

Sélectionnez l'onglet Réseau > Serveur d'email > Test de connexion > Démarrer.

Configuration depuis le panneau de commande :

Sélectionnez Param. > Paramètres réseau > Avancé > Serveur d'email > Vérification connexion.

Le test de connexion au serveur de messagerie est lancé.

2. Consultez les résultats du test.

Si le message **Le test de connexion a réussi.** s'affiche, alors le test a réussi.

Si une erreur s'affiche, suivez les instructions contenues dans le message pour la résoudre.

[« Références du test de connexion au serveur de messagerie » à la page 48](#)

Références du test de connexion au serveur de messagerie

| Message | Cause |
|--|---|
| Erreur de communication avec le serveur SMTP. Vérifiez l'élément suivant. - Paramètres réseau | <p>Ce message s'affiche lorsque</p> <ul style="list-style-type: none"> <input type="checkbox"/> Le scanner n'est pas connecté à un réseau <input type="checkbox"/> Le serveur SMTP est indisponible <input type="checkbox"/> La connexion au réseau a été interrompue lors de la communication <input type="checkbox"/> Les données reçues sont incomplètes |
| Erreur de communication avec le serveur POP3. Vérifiez l'élément suivant. - Paramètres réseau | <p>Ce message s'affiche lorsque</p> <ul style="list-style-type: none"> <input type="checkbox"/> Le scanner n'est pas connecté à un réseau <input type="checkbox"/> Le serveur POP3 est indisponible <input type="checkbox"/> La connexion au réseau a été interrompue lors de la communication <input type="checkbox"/> Les données reçues sont incomplètes |
| Une erreur est survenue lors de la connexion au serveur SMTP. Vérifiez les éléments suivants. - Adresse du serveur SMTP - Serveur DNS | <p>Ce message s'affiche lorsque</p> <ul style="list-style-type: none"> <input type="checkbox"/> La connexion à un serveur DNS a échoué <input type="checkbox"/> La résolution de nom d'un serveur SMTP a échoué |
| Une erreur est survenue lors de la connexion au serveur POP3. Vérifiez les éléments suivants. - Adresse du serveur POP3 - Serveur DNS | <p>Ce message s'affiche lorsque</p> <ul style="list-style-type: none"> <input type="checkbox"/> La connexion à un serveur DNS a échoué <input type="checkbox"/> La résolution de nom d'un serveur POP3 a échoué |
| Erreur d'authentification sur serveur SMTP. Vérifiez les éléments suivants. - Méthode d'authentification - Compte authentifié - Mot de passe authentifié | <p>Ce message s'affiche lorsque l'authentification au serveur SMTP a échoué.</p> |
| Erreur d'authentification sur serveur POP3. Vérifiez les éléments suivants. - Méthode d'authentification - Compte authentifié - Mot de passe authentifié | <p>Ce message s'affiche lorsque l'authentification au serveur POP3 a échoué.</p> |
| Méthode de communication non prise en charge. Vérifiez ce qui suit. - Adresse du serveur SMTP - Numéro port serveur SMTP | <p>Ce message s'affiche lorsque vous essayez de communiquer avec des protocoles non pris en charge.</p> |
| La connexion au serveur SMTP a échoué. Remplacez Connexion sécurisée par Aucun. | <p>Ce message s'affiche lorsqu'une incompatibilité SMTP survient entre un serveur et un client, ou lorsque le serveur ne prend pas en charge la connexion sécurisée SMTP (connexion SSL).</p> |
| La connexion au serveur SMTP a échoué. Remplacez Connexion sécurisée par SSL/TLS. | <p>Ce message s'affiche lorsqu'une incompatibilité SMTP survient entre un serveur et un client, ou lorsque le serveur demande d'utiliser une connexion SSL/TLS dans le cas d'une connexion SMTP sécurisée.</p> |
| La connexion au serveur SMTP a échoué. Remplacez Connexion sécurisée par STARTTLS. | <p>Ce message s'affiche lorsqu'une incompatibilité SMTP survient entre un serveur et un client, ou lorsque le serveur demande d'utiliser une connexion STARTTLS dans le cas d'une connexion SMTP sécurisée.</p> |
| La connexion n'est pas de confiance. Vérifiez ce qui suit. - Date et heure | <p>Ce message s'affiche lorsque la date et l'heure du scanner sont incorrectes ou que le certificat a expiré.</p> |
| La connexion n'est pas de confiance. Vérifiez ce qui suit. - Certificat CA | <p>Ce message s'affiche lorsque le scanner ne dispose pas d'un certificat racine correspondant au serveur ou qu'aucun Certificat CA n'a été importé.</p> |

| Message | Cause |
|---|--|
| La connexion n'est pas de confiance. | Ce message s'affiche lorsque le certificat obtenu est endommagé. |
| Échec de l'authentification au serveur SMTP. Remplacez Méthode d'authentification par SMTP-AUTH. | Ce message s'affiche lorsqu'une incompatibilité de méthode d'authentification se produit entre un serveur et un client. Le serveur prend en charge SMTP-AUTH. |
| Échec de l'authentification au serveur SMTP. Remplacez Méthode d'authentification par POP avant SMTP. | Ce message s'affiche lorsqu'une incompatibilité de méthode d'authentification se produit entre un serveur et un client. Le serveur ne prend pas en charge SMTP-AUTH. |
| Adr. messagerie expéditeur est incorrect. Modifiez l'adresse e-mail pour votre service e-mail. | Ce message s'affiche lorsque l'adresse e-mail de l'expéditeur spécifiée est erronée. |
| Impossible d'accéder au produit tant que le traitement n'est pas terminé. | Ce message s'affiche lorsque le scanner est occupé. |

Créer un dossier réseau

Créez un dossier réseau sur votre ordinateur. L'ordinateur doit être connecté au même réseau que le scanner.

La méthode de création d'un dossier réseau varie en fonction de votre environnement. Voici un exemple de création d'un dossier réseau sur le bureau d'un ordinateur dont l'environnement est le suivant.

- Système d'exploitation : Windows 10
- Emplacement de création du dossier partagé : bureau
- Chemin d'accès au dossier : C:\Utilisateurs\xxxx\Bureau\scan_folder (créer un dossier intitulé « scan_folder » sur le bureau)

1. Sur l'ordinateur sur lequel vous souhaitez créer un dossier réseau, ouvrez une session disposant des droits d'administration.

Remarque:

Si vous ne savez pas quel compte utilisateur dispose des droits d'administration, adressez-vous à l'administrateur de votre ordinateur.

2. Vérifiez que le nom de l'appareil (nom de l'ordinateur) ne contient aucun caractère à deux octets. Cliquez sur le bouton Démarrer de Windows, puis sélectionnez  **Paramètres** > **Système** > **À propos de**.

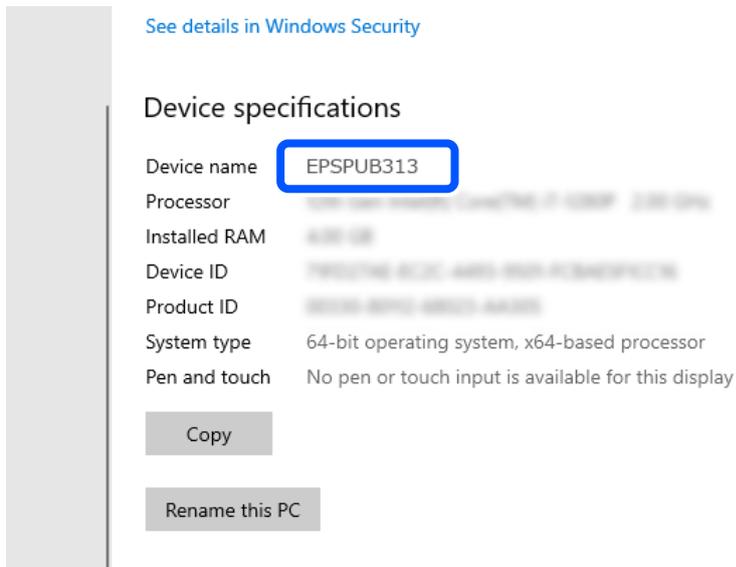
Remarque:

Si des caractères à deux octets sont présents dans le nom de l'appareil, l'enregistrement des fichiers peut échouer.

3. Vérifiez que le nom affiché dans **Spécifications de l'appareil** > **Nom de l'appareil** ne contient aucun caractère à deux octets.

Les noms d'appareil comportant uniquement des caractères à un octet ne devraient poser aucun problème. Fermez l'écran.

Exemple : EPSPUB313



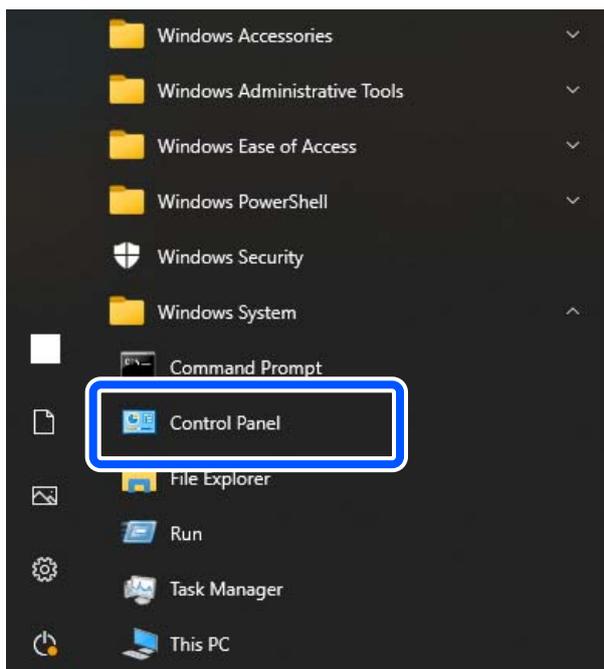
Important:

Si le nom de l'appareil contient des caractères à deux octets, utilisez un ordinateur qui n'utilise pas de tels caractères ou renommez l'appareil.

Si vous devez modifier le nom de l'appareil, avertissez-en l'administrateur au préalable afin d'éviter tout problème de gestion des ordinateurs ou d'accès aux ressources.

Vérifiez ensuite les paramètres de votre ordinateur.

4. Cliquez sur le bouton Démarrer de Windows, puis sélectionnez **Système Windows > Panneau de configuration**.



5. Dans le Panneau de configuration, cliquez sur **Réseau et Internet > Centre Réseau et partage > Modifier les paramètres de partage avancés**.

Le profil du réseau s'affiche.

6. Sous **Partage de fichiers et d'imprimantes**, vérifiez que l'option **Activer le partage de fichiers et d'imprimantes** pour le profil du réseau (profil actuel).

Si cette option est déjà sélectionnée, cliquez sur **Annuler** et fermez la fenêtre.

Si vous avez modifié des paramètres, cliquez sur **Enregistrer les modifications** et fermez la fenêtre.

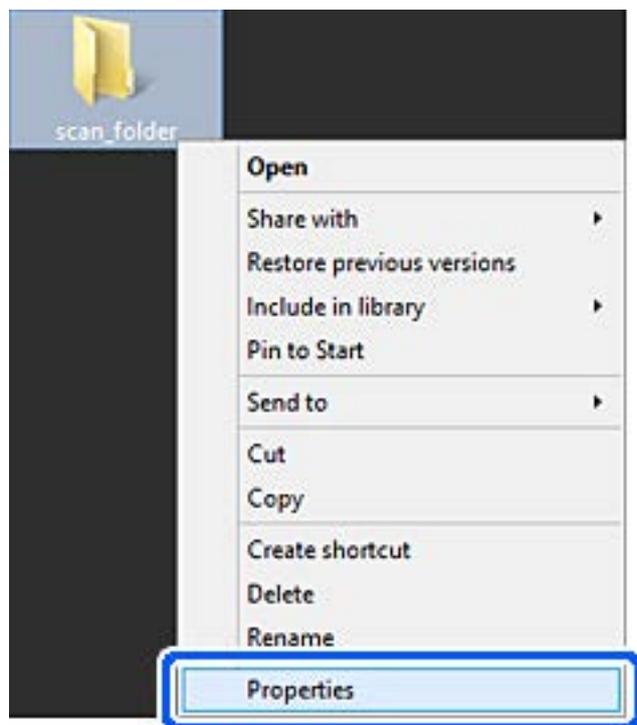
Créez ensuite un dossier réseau.

7. Créez un dossier sur le bureau et donnez-lui un nom.

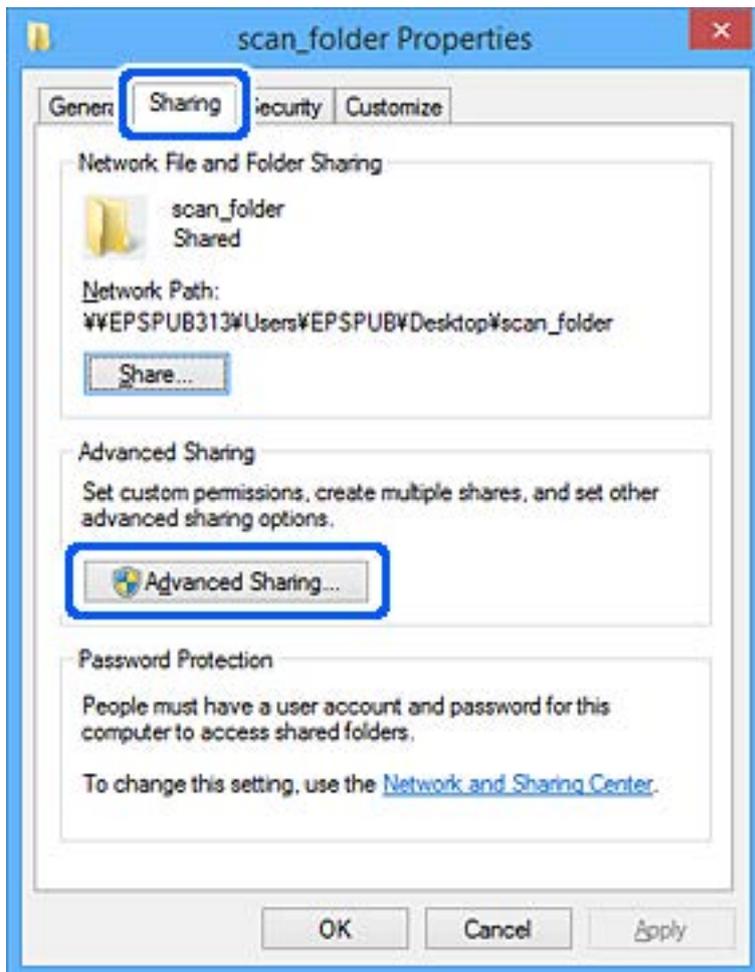
Saisissez entre 1 et 12 caractères alphanumériques pour donner un nom au dossier. En fonction de votre environnement, si le nom dépasse 12 caractères, vous pourriez avoir des problèmes pour y accéder.

Exemple : scan_folder

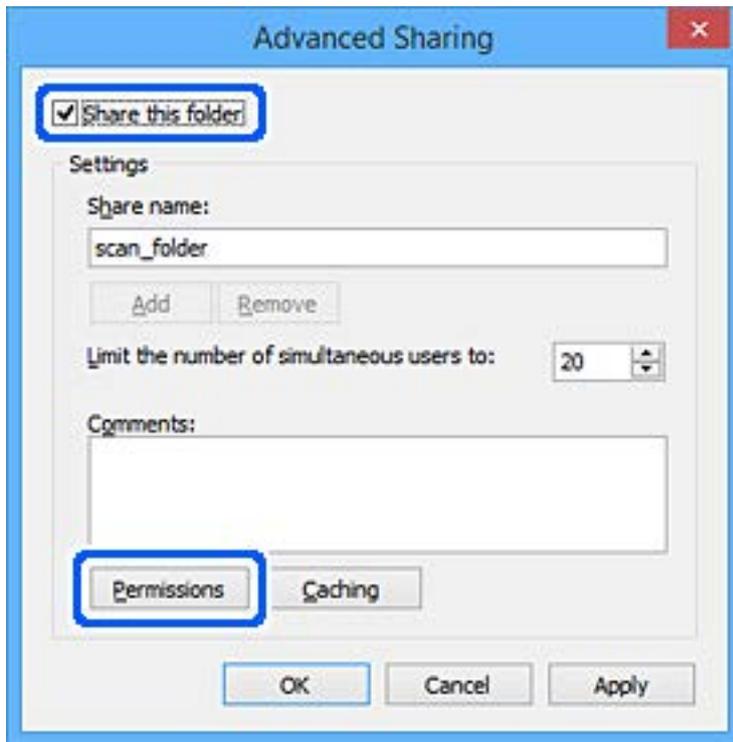
8. Faites un clic droit sur le dossier et sélectionnez **Propriétés**.



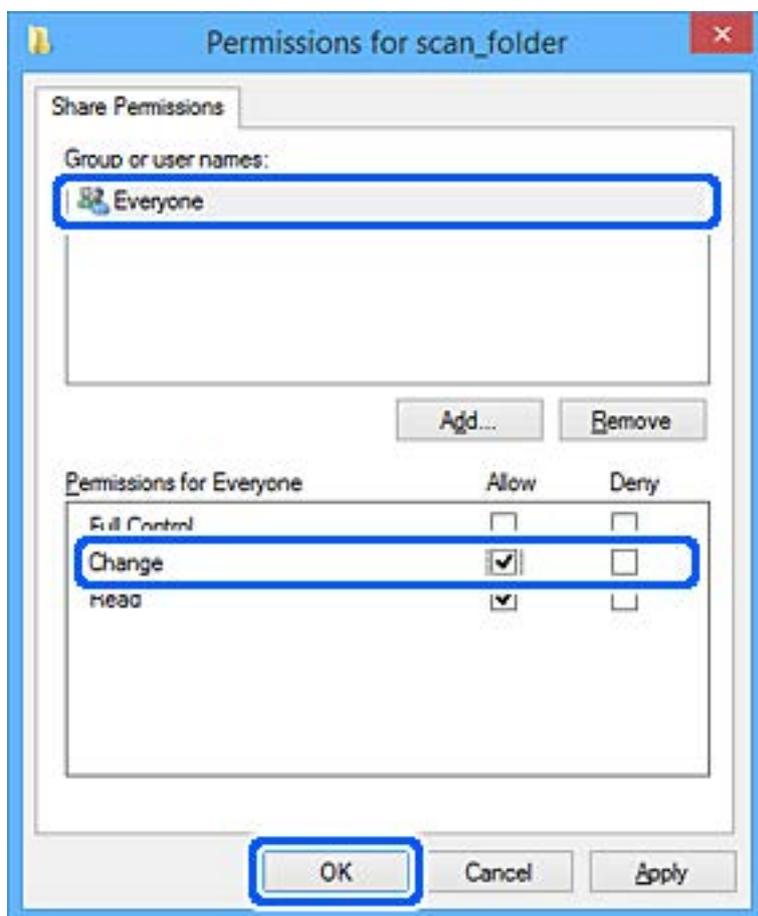
9. Cliquez sur **Partage avancé** dans l'onglet **Partage**.



10. Sélectionnez **Partager ce dossier**, puis cliquez sur **Autorisations**.



11. Sélectionnez **Tout le monde** dans **Noms de groupes ou d'utilisateurs**, sélectionnez **Autoriser** en regard de **Modifier**, puis cliquez sur **OK**.

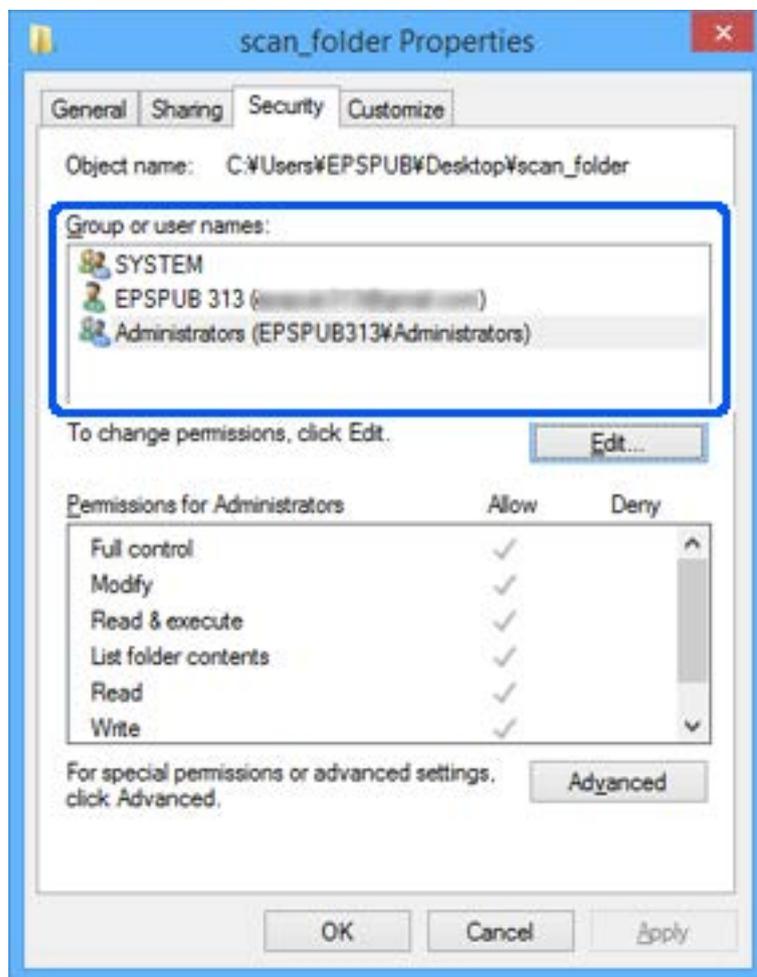


12. Cliquez sur **OK** pour fermer cet écran et revenir à la fenêtre Propriétés.

Remarque:

Vous pouvez consulter les groupes ou utilisateurs qui disposent d'un accès au dossier réseau dans l'onglet **Sécurité** > **Noms de groupes ou d'utilisateurs**.

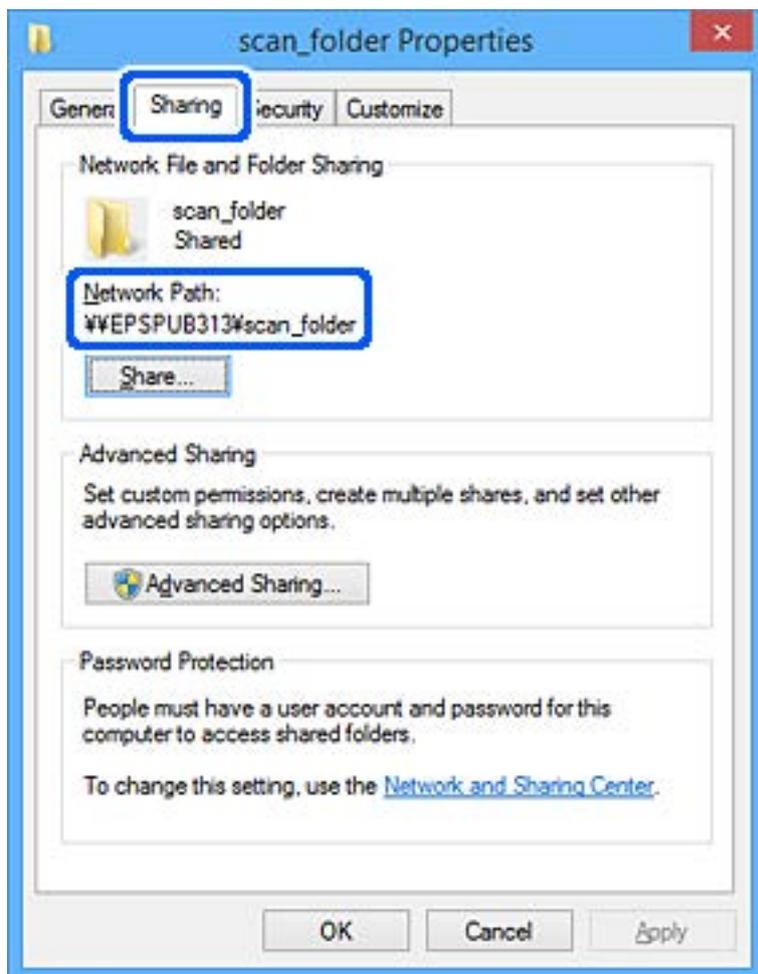
Exemple : lorsque l'utilisateur connecté à l'ordinateur et les administrateurs ont accès au dossier réseau



13. Sélectionnez l'onglet **Partage**.

Le chemin réseau du dossier réseau s'affiche. Cela est utilisé lors de l'enregistrement dans les contacts du scanner. Prenez-en note.

Exemple : \\EPSPUB313\scan_folder



14. Cliquez sur **Fermer** ou **OK** pour fermer la fenêtre.

La création d'un dossier réseau est terminée.

Mise à disposition des contacts

L'enregistrement de destinataires dans la liste de contacts du scanner vous permet de facilement de saisir le destinataire lors de la numérisation.

Vous pouvez enregistrer les types de destinataires suivants dans la liste de contacts. Vous pouvez entrer jusqu'à 300 entrées au total.

Remarque:

Vous pouvez également utiliser le serveur LDAP (recherche LDAP) pour saisir le destinataire.

| | |
|----------------------|---|
| Adresse électronique | Destinataire pour l'email. Il faut configurer les paramètres de serveur de l'email à l'avance. |
| Dossier réseau | Destinataire des données numérisées. Vous devez préparer le dossier réseau à l'avance. |

Informations connexes

➔ « [Coopération entre le serveur LDAP et les utilisateurs](#) » à la page 63

Comparaison des outils de configuration des contacts

Trois outils permettent de configurer les contacts du scanner : Web Config, Epson Device Admin et le panneau de commande du scanner. Les différences entre les trois outils sont répertoriées dans le tableau ci-dessous.

| Fonctionnalités | Web Config* | Epson Device Admin | Panneau de commande du scanner |
|---|-------------|--------------------|--------------------------------|
| Enregistrement d'une destination | ✓ | ✓ | ✓ |
| Modification d'une destination | ✓ | ✓ | ✓ |
| Ajout d'un groupe | ✓ | ✓ | ✓ |
| Modification d'un groupe | ✓ | ✓ | ✓ |
| Suppression d'une destination ou de groupes | ✓ | ✓ | ✓ |
| Suppression de toutes les destinations | ✓ | ✓ | - |
| Importation d'un fichier | ✓ | ✓ | - |
| Exportation vers un fichier | ✓ | ✓ | - |

* Connectez-vous en tant qu'administrateur pour modifier les paramètres.

Enregistrement d'une destination dans les contacts à l'aide de Web Config

Remarque:

Vous pouvez également enregistrer les contacts depuis le panneau de commande du scanner.

1. Accédez à Web Config et sélectionnez l'onglet **Numériser > Contacts**.
2. Sélectionnez le numéro à enregistrer, puis cliquez sur **Modifier**.
3. Saisissez le **Nom** et l'**Mot d'index**.
4. Sélectionnez le type de destination pour l'option **Type**.

Remarque:

*Vous ne pouvez pas modifier l'option **Type** une fois l'enregistrement terminé. Si vous voulez changer le type, supprimez la destination avant de la réenregistrer.*

5. Saisissez une valeur pour chaque élément, puis cliquez sur **Appliquer**.

Informations connexes

➔ [« Comment exécuter Web Config dans un navigateur Web » à la page 39](#)

Éléments de configuration de la destination

| Éléments | Paramètres et explication |
|---------------------------|--|
| Paramètres communs | |
| Nom | Saisissez un nom d'utilisateur au format Unicode (UTF-16) de moins de 30 caractères à afficher dans les contacts. Laissez le champ vide si vous ne voulez pas en spécifier. |
| Mot d'index | Saisissez un nom d'utilisateur au format Unicode (UTF-16) de 30 caractères au maximum pour effectuer une recherche parmi vos contacts depuis le panneau de commande du scanner. Laissez le champ vide si vous ne voulez pas en spécifier. |
| Type | Sélectionnez le type d'adresse que vous souhaitez enregistrer. |
| Affect à l'util fréquente | Sélectionnez pour définir l'adresse enregistrée comme adresse fréquemment utilisée. Une fois l'adresse définie comme fréquemment utilisée, elle s'affiche en haut de l'écran des numérisations et vous pouvez indiquer la destination sans afficher les contacts. |
| Email | |
| Adresse de la messagerie | Saisissez entre 1 et 255 caractères en utilisant A – Z a – z 0 – 9 ! # \$ % & ' * + - . / = ? ^ _ { } ~ @. |
| Dossier réseau (SMB) | |
| Enregistrer | \\« Chemin d'accès » Saisissez l'emplacement du dossier cible en utilisant entre 1 et 253 caractères au format Unicode (UTF-16) sans compter « \ ». Saisissez le chemin réseau affiché à l'écran des propriétés du dossier. Reportez-vous à ce qui suit pour en savoir plus sur la configuration du chemin réseau. « Créer un dossier réseau » à la page 49 |
| Nom d'utilisateur | Saisissez un nom d'utilisateur au format Unicode (UTF-16) de moins de 30 caractères pour accéder à un dossier réseau. Évitez toutefois d'utiliser des caractères de contrôle (0x00 à 0x1f et 0x7F). |
| Mot de passe | Saisissez un mot de passe entre 0 et 20 caractères au format Unicode (UTF-16) pour accéder au dossier réseau. Évitez toutefois d'utiliser des caractères de contrôle (0x00 à 0x1f et 0x7F). |
| FTP | |
| Connexion sécurisée | Sélectionnez FTP ou FTPS selon le protocole de transfert de fichiers pris en charge par le serveur FTP. Sélectionnez FTPS pour permettre au scanner de communiquer en appliquant des mesures de sécurité. |
| Enregistrer | Saisissez le nom du serveur en utilisant entre 1 et 253 caractères au format Unicode (UTF-16) sans compter « ftp:// » ou « ftps:// ». |

| Éléments | Paramètres et explication |
|-----------------------|---|
| Nom d'utilisateur | Saisissez un nom d'utilisateur de 30 caractères au maximum au format Unicode (UTF-16) pour accéder à un serveur FTP. Évitez toutefois d'utiliser des caractères de contrôle (0x00 à 0x1f et 0x7F). Si le serveur autorise les connexions anonymes, saisissez un nom d'utilisateur comme Anonyme ou FTP. Laissez le champ vide si vous ne voulez pas en spécifier. |
| Mot de passe | Saisissez un mot de passe entre 0 et 20 caractères au format Unicode (UTF-16) pour accéder à un serveur FTP. Évitez toutefois d'utiliser des caractères de contrôle (0x00 à 0x1f et 0x7F). Laissez le champ vide si vous ne voulez pas en spécifier. |
| Mode de connexion | Sélectionnez le mode de connexion dans le menu. Si un pare-feu est configuré entre le scanner et le serveur FTP, sélectionnez Mode passif . |
| Numéro de port | Saisissez un numéro de port du serveur FTP compris entre 1 et 65535. |
| Validation certificat | Le certificat du serveur FTP est validé lorsque cette option est activée. Disponible lorsque l'option FTPS est réglée sur Connexion sécurisée . Pour que cette option fonctionne, importez le Certificat CA dans le scanner. |
| SharePoint(WebDAV)* | |
| Connexion sécurisée | Sélectionnez HTTP ou HTTPS selon le protocole de transfert de fichiers pris en charge par le serveur. Sélectionnez HTTPS pour permettre au scanner de communiquer en appliquant des mesures de sécurité. |
| Enregistrer | Saisissez le nom du serveur en utilisant entre 1 et 253 caractères au format Unicode (UTF-16) sans compter « http:// » ou « https:// ». |
| Nom d'utilisateur | Saisissez un nom d'utilisateur de 30 caractères au maximum au format Unicode (UTF-16) pour accéder à un serveur. Évitez toutefois d'utiliser des caractères de contrôle (0x00 à 0x1f et 0x7F). Laissez le champ vide si vous ne voulez pas en spécifier. |
| Mot de passe | Saisissez un mot de passe entre 0 et 20 caractères au format Unicode (UTF-16) pour accéder à un serveur. Évitez toutefois d'utiliser des caractères de contrôle (0x00 à 0x1f et 0x7F). Laissez le champ vide si vous ne voulez pas en spécifier. |
| Validation certificat | Le certificat du serveur est validé lorsque cette option est activée. Disponible lorsque l'option HTTPS est réglée sur Connexion sécurisée . Pour que cette option fonctionne, importez le Certificat CA dans le scanner. |
| Serveur proxy | Indiquez si vous souhaitez utiliser un serveur proxy. |

* SharePoint Online n'est pas pris en charge lors de la numérisation vers un dossier réseau depuis le panneau de commande du scanner.

Si vous souhaitez enregistrer l'image numérisée dans SharePoint Online, utilisez Document Capture Pro après avoir installé le SharePoint Online Connector. Reportez-vous au manuel de Document Capture Pro pour en savoir plus.

<https://support.epson.net/dcp/>

Enregistrement des destinations en tant que groupe à l'aide de Web Config

Si le type de destination est défini sur **Email**, vous pouvez enregistrer les destinations en tant que groupe.

1. Accédez à Web Config et sélectionnez l'onglet **Numériser > Contacts**.
2. Sélectionnez le numéro à enregistrer, puis cliquez sur **Modifier**.
3. Sélectionnez un groupe dans **Type**.
4. Cliquez sur **Sélectionner** pour **Contact(s) pour Groupe**.
Les destinations disponibles s'affichent.
5. Sélectionnez les destinations que vous voulez enregistrer dans le groupe, puis cliquez sur **Sélectionner**.
6. Saisissez le **Nom** et l'**Mot d'index**.
7. Sélectionnez si vous souhaitez assigner ou non le groupe enregistré dans le groupe fréquemment utilisé.

Remarque:

Les destinations peuvent être enregistrées dans plusieurs groupes.

8. Cliquez sur **Appliquer**.

Informations connexes

➔ « [Comment exécuter Web Config dans un navigateur Web](#) » à la page 39

Sauvegarde et importation de contacts

Vous pouvez sauvegarder et importer des contacts à l'aide d'outils comme Web Config.

Pour Web Config, vous pouvez sauvegarder les contacts en exportant les paramètres du scanner qui incluent les contacts. Le fichier exporté ne peut être modifié, car il est exporté en tant que fichier binaire.

Les contacts sont remplacés lors de l'importation des paramètres du scanner dans le scanner.

Pour Epson Device Admin, seuls les contacts peuvent être exportés à partir de l'écran des propriétés du périphérique. Si vous n'exportez pas les éléments liés à la sécurité, vous pouvez également modifier les contacts exportés et les importer, car ils peuvent être enregistrés en fichier SYLK ou CSV.

Importation de contacts à l'aide de Web Config

Si vous avez un scanner qui vous permet de sauvegarder des contacts et est compatible avec ce scanner, vous pouvez facilement enregistrer des contacts en important le fichier de sauvegarde.

Remarque:

Pour obtenir des instructions sur la façon de sauvegarder les contacts du scanner, reportez-vous au manuel fourni avec le scanner.

Suivez les étapes ci-dessous pour importer les contacts dans le scanner.

1. Accédez à Web Config, sélectionnez l'onglet **Gestion des périphériques > Exporter et importer valeur de paramètre > Importer**.
2. Sélectionnez le fichier de sauvegarde créé dans **Fichier**, saisissez le mot de passe, puis cliquez sur **Suivant**.
3. Cochez la case **Contacts**, puis **Suivant**.

Sauvegarde de contacts avec Web Config

Les données de contact risquent d'être perdues suite à une anomalie de fonctionnement du scanner. Il est conseillé d'effectuer une sauvegarde des données à chaque mise à jour des données. Epson ne sera pas tenue responsable de la perte de données, de la sauvegarde ou de la restauration de données et/ou paramètres et ce, même pendant une période de garantie.

Avec Web Config, vous pouvez sauvegarder sur l'ordinateur les données des contacts enregistrés dans le scanner.

1. Accédez à Web Config, puis sélectionnez l'onglet **Gestion des périphériques > Exporter et importer valeur de paramètre > Exporter**.
2. Sélectionnez la case à cocher **Contacts** dans la catégorie **Numériser**.
3. Saisissez un mot de passe pour déchiffrer le fichier exporté.
Vous avez besoin du mot de passe pour importer le fichier. Laissez le champ vide si vous ne souhaitez pas chiffrer le fichier.
4. Cliquez sur **Exporter**.

Exportation et enregistrement de contacts en volume à l'aide d'un outil

Si vous utilisez Epson Device Admin, vous pouvez ne sauvegarder que les contacts et modifier les fichiers exportés, puis tout enregistrer d'un coup.

C'est utile lorsque vous ne voulez sauvegarder que les contacts, ou remplacer le scanner et transférer les contacts de l'ancienne vers la nouvelle.

Exportation des contacts

Enregistrez les informations des contacts dans le fichier.

Vous pouvez modifier les fichiers enregistrés au format SYLK ou csv à l'aide d'une application de feuille de calcul ou un éditeur de texte. Vous pouvez vous tous les enregistrés à la fois à la suite d'une suppression ou d'un ajout d'informations.

Les informations qui incluent des éléments de sécurité, tels que des mots de passe et des informations personnelles, peuvent être enregistrées au format binaire avec mot de passe. Vous ne pouvez pas modifier le fichier. Il peut être utilisé comme fichier de sauvegarde d'informations, éléments de sécurité y compris.

1. Lancez Epson Device Admin.
2. Sélectionnez **Imprimantes** dans le menu des tâches de la barre latérale.
3. Sélectionnez le périphérique que vous souhaitez configurer dans la liste.
4. Cliquez sur **Configuration des périphériques** dans l'onglet **Accueil** du menu ruban.
Une fois le mot de passe administrateur défini, saisissez le mot de passe et cliquez sur **OK**.
5. Cliquez sur **Commun > Contacts**.

6. Sélectionnez le format d'exportation dans **Exporter** > **Exporter éléments**.

Tous les éléments

Exportez le fichier binaire chiffré. Sélectionnez le cas dans lequel vous souhaitez inclure les éléments de sécurité, tels que le mot de passe et les informations personnelles. Vous ne pouvez pas modifier le fichier. Si vous le sélectionnez, vous devez définir le mot de passe. Cliquez **Configuration** et définissez un mot de passe entre 8 et 63 caractères en ASCII. Ce mot de passe est requis lors de l'importation du fichier binaire.

Éléments sauf Informations de sécurité

Exportez les fichiers au format SYLK ou au format csv. Sélectionnez le cas dans lequel vous souhaitez modifier les informations du fichier exporté.

7. Cliquez sur **Exporter**.

8. Spécifiez l'emplacement d'enregistrement du fichier, le type de fichier, puis cliquez sur **Enregistrer**.

Le message de finalisation s'affiche.

9. Cliquez sur **OK**.

Vérifiez que le fichier est enregistré à l'endroit spécifié.

Importation des contacts

Importez les informations des contacts dans le fichier.

Vous pouvez importer les fichiers enregistrés au format SYLK ou csv, ainsi que le fichier binaire sauvegardé qui inclut les éléments de sécurité.

1. Lancez Epson Device Admin.

2. Sélectionnez **Imprimantes** dans le menu des tâches de la barre latérale.

3. Sélectionnez le périphérique que vous souhaitez configurer dans la liste.

4. Cliquez sur **Configuration des périphériques** dans l'onglet **Accueil** du menu ruban.

Une fois le mot de passe administrateur défini, saisissez le mot de passe et cliquez sur **OK**.

5. Cliquez sur **Commun** > **Contacts**.

6. Cliquez sur **Parcourir** dans **Importer**.

7. Sélectionnez le fichier que vous souhaitez importer, puis cliquez sur **Ouvrir**.

Lorsque vous sélectionnez le fichier binaire, saisissez le mot de passe que vous avez défini lors de l'exportation du fichier dans **Mot de passe**.

8. Cliquez sur **Importer**.

L'écran de confirmation s'affiche.

9. Cliquez sur **OK**.

Le résultat de validation s'affiche.

Édition des informations chargées

Cliquez lorsque vous souhaitez modifier les informations individuellement.

- Chargement de plus de fichier

Cliquez sur lorsque vous souhaitez importer plusieurs fichiers.

10. Cliquez sur **Importer**, puis sur **OK** dans le dernier écran de l'importation.

Revenez à l'écran des propriétés du périphérique.

11. Cliquez sur **Transmettre**.

12. Cliquez sur **OK** dans le message de confirmation.

Les paramètres sont envoyés au scanner.

13. Cliquez sur **OK** à l'écran confirmant l'envoi.

Les informations du scanner sont mises à jour.

Ouvrez les contacts à partir de Web Config ou du panneau de commande du scanner, puis vérifiez que le contact est mis à jour.

Coopération entre le serveur LDAP et les utilisateurs

Vous pouvez définir les informations d'adresse enregistrées sur le serveur LDAP comme destination d'un e-mail lorsque vous coopérez avec le serveur LDAP.

Configuration du serveur LDAP

Pour utiliser les informations du serveur LDAP, enregistrez-les sur le scanner.

1. Accédez à Web Config et sélectionnez l'onglet **Réseau** > **Serveur LDAP** > **De base**.
2. Saisissez une valeur pour chaque élément.
3. Sélectionnez **OK**.

Les paramètres que vous avez sélectionnés s'affichent.

Éléments de configuration du serveur LDAP

| Éléments | Paramètres et explication |
|--------------------------|---|
| Utiliser le Serveur LDAP | Sélectionnez Utiliser ou Ne pas utiliser . |
| Adresse du serveur LDAP | Saisissez l'adresse du serveur LDAP. Saisissez 1 à 255 caractères au format IPv4, IPv6 ou FQDN. Pour le format FQDN, vous pouvez utiliser des caractères alphanumériques ASCII (0x20–0x7E) et « - », sauf pour le début et la fin de l'adresse. |
| Num. port serveur LDAP | Saisissez le numéro de port du serveur LDAP entre 1 et 65535. |
| Connexion sécurisée | Choisissez la méthode d'authentification pour que le scanner accède au serveur LDAP. |

| Éléments | Paramètres et explication |
|---------------------------------------|--|
| Validation certificat | Lorsque cette option est activée, le certificat du serveur LDAP est validé. Nous vous recommandons de sélectionner la valeur Activer . Pour que cette option fonctionne, vous devez importer le Certificat CA dans le scanner. |
| Expiration recherche (sec) | Définissez le temps de recherche observé avant qu'une erreur de délai dépassé ne survienne, entre 5 et 300. |
| Méthode d'authentification | Sélectionnez l'une des méthodes. Si vous sélectionnez L'authentification Kerberos , sélectionnez Paramètres Kerberos pour effectuer les réglages de Kerberos. Pour réaliser une L'authentification Kerberos, les conditions suivantes sont nécessaires. <ul style="list-style-type: none"> <input type="checkbox"/> Le scanner et le serveur DNS parviennent à communiquer. <input type="checkbox"/> L'heure du scanner, le serveur KDC et le serveur nécessaire à l'authentification (serveur LDAP, serveur SMTP ou serveur de fichiers) sont synchronisés. <input type="checkbox"/> Lorsque le serveur de service est attribué en tant qu'adresse IP, le FQDN de ce serveur est enregistré dans la zone de résolution inverse du serveur DNS. |
| Domaine Kerberos à utiliser | Si vous sélectionnez L'authentification Kerberos pour Méthode d'authentification , sélectionnez le domaine Kerberos que vous souhaitez utiliser. |
| DN administrateur / Nom d'utilisateur | Saisissez le nom d'utilisateur pour le serveur LDAP en Unicode (UTF-8) et en moins de 128 caractères. Vous ne pouvez pas utiliser des caractères de contrôle, tels que 0x00–0x1F et 0x7F. Ce paramètre n'est pas utilisé lorsque Authentification anonyme est sélectionné pour Méthode d'authentification . Laissez le champ vide si vous ne voulez pas en spécifier. |
| Mot de passe | Saisissez le mot de passe pour le serveur d'authentification LDAP en Unicode (UTF-8) et en moins de 128 caractères. Vous ne pouvez pas utiliser des caractères de contrôle, tels que 0x00–0x1F et 0x7F. Ce paramètre n'est pas utilisé lorsque Authentification anonyme est sélectionné pour Méthode d'authentification . Laissez le champ vide si vous ne voulez pas en spécifier. |

Paramètres Kerberos

Si vous sélectionnez **L'authentification Kerberos** pour **Méthode d'authentification de Serveur LDAP > De base**, définissez les paramètres Kerberos suivants dans l'onglet **Réseau > Paramètres Kerberos**. Vous pouvez enregistrer jusqu'à 10 paramètres pour les paramètres Kerberos.

| Éléments | Paramètres et explication |
|---------------------------|---|
| Domaine | Saisissez le domaine de l'authentification Kerberos en 255 caractères ASCII (0x20–0x7E) maximum. Laissez le champ vide si vous ne voulez pas en enregistrer. |
| Adresse KDC | Saisissez l'adresse du serveur d'authentification Kerberos. Saisissez jusqu'à 255 caractères dans le format IPv4, IPv6 ou FQDN. Laissez le champ vide si vous ne voulez pas en enregistrer. |
| Numéro de port (Kerberos) | Saisissez le numéro de port du serveur Kerberos entre 1 et 65535. |

Configuration des paramètres de recherche du serveur LDAP

Vous pouvez utiliser l'adresse e-mail enregistrée sur le serveur LDAP lors de la configuration des paramètres de recherche.

1. Accédez à Web Config et sélectionnez l'onglet **Réseau > Serveur LDAP > Paramètres de recherche**.
2. Saisissez une valeur pour chaque élément.
3. Cliquez sur **OK** pour afficher le résultat du paramètre.
Les paramètres que vous avez sélectionnés s'affichent.

Éléments de configuration de recherche du serveur LDAP

| Éléments | Paramètres et explication |
|---|---|
| Base de recherche (Nom distingué) | Si vous souhaitez rechercher un domaine arbitraire, spécifiez le nom de domaine du serveur LDAP. Saisissez entre 0 et 128 caractères Unicode (UTF-8). Laissez ce champ vide si vous ne recherchez pas d'attribut arbitraire. Exemple de répertoire du serveur local : dc=server,dc=local |
| Nombre d'entrées de recherche | Spécifiez le nombre d'entrées de recherche, entre 5 et 500. Le nombre d'entrées de recherche spécifié est enregistré et affiché temporairement. Même si le nombre d'entrées de recherche est supérieur au nombre spécifié et qu'un message d'erreur apparaît, la recherche peut malgré tout être effectuée. |
| Attribut Nom d'utilisateur | Spécifiez le nom d'attribut à afficher lors de la recherche des noms d'utilisateur. Saisissez entre 1 et 255 caractères Unicode (UTF-8). Le premier caractère doit être a-z ou A-Z. Exemple : cn, uid |
| Attr affich Nom utilisateur | Spécifiez le nom d'attribut à afficher comme nom d'utilisateur. Saisissez entre 0 et 255 caractères Unicode (UTF-8). Le premier caractère doit être a-z ou A-Z. Exemple : cn, sn |
| Attribut de l'adresse email | Spécifiez le nom d'attribut à afficher lors de la recherche d'adresses e-mail. Saisissez une combinaison entre 1 et 255 caractères en utilisant A-Z, a-z, 0-9 et -. Le premier caractère doit être a-z ou A-Z. Exemple : courrier |
| Attribut arbitraire 1 - Attribut arbitraire 4 | Vous pouvez spécifier d'autres attributs arbitraires à rechercher. Saisissez entre 0 et 255 caractères Unicode (UTF-8). Le premier caractère doit être a-z ou A-Z. Laissez ce champ vide si vous ne souhaitez pas rechercher d'attributs arbitraires. Exemple : o, ou |

Vérification de la connexion à un serveur LDAP

Réalisez le test de connexion au serveur LDAP en utilisant le paramètre défini dans **Serveur LDAP > Paramètres de recherche**.

1. Accédez à Web Config et sélectionnez l'onglet **Réseau > Serveur LDAP > Test de connexion**.

2. Sélectionnez **Démarrer**.

Le test de connexion commence. Le rapport de vérification s'affiche le fois le test terminé.

Références de test de la connexion au serveur LDAP

| Messages | Explication |
|---|---|
| Le test de connexion a réussi. | Ce message s'affiche une fois la connexion au serveur correctement établie. |
| Le test de connexion a échoué. Vérifier les paramètres. | Ce message s'affiche pour les raisons suivantes : <input type="checkbox"/> L'adresse du serveur LDAP ou le numéro de port est incorrect. <input type="checkbox"/> Une erreur d'expiration est survenue. <input type="checkbox"/> Ne pas utiliser est sélectionné pour Utiliser le Serveur LDAP . <input type="checkbox"/> Si L'authentification Kerberos est sélectionné pour Méthode d'authentification , les paramètres tels que Domaine, Adresse KDC et Numéro de port (Kerberos) sont incorrects. |
| Le test de connexion a échoué. Vérifiez les date et heure sur votre produit ou sur le serveur. | Ce message s'affiche lorsque la connexion échoue en raison d'une différence entre l'heure du scanner et du serveur LDAP. |
| Échec authentification. Vérifier les paramètres. | Ce message s'affiche pour les raisons suivantes : <input type="checkbox"/> Nom d'utilisateur et/ou Mot de passe est incorrect. <input type="checkbox"/> Si L'authentification Kerberos est sélectionné pour Méthode d'authentification , l'heure et la date ne sont peut-être pas configurées. |
| Impossible d'accéder au produit tant que le traitement n'est pas terminé. | Ce message s'affiche lorsque le scanner est occupé. |

Configuration de AirPrint

Accédez à Web Config, sélectionnez l'onglet **Réseau**, puis sélectionnez **Configuration d'AirPrint**.

| Éléments | Explication |
|------------------------|---|
| Nom du service Bonjour | Saisissez un nom de service Bonjour, en utilisant du texte ASCII (0x20–0x7E) et jusqu'à 41 caractères. |
| Emplacement de Bonjour | Saisissez une description de l'emplacement du scanner à l'aide de texte Unicode (UTF-8) et jusqu'à 127 octets. |
| Wide-Area Bonjour | Définissez si vous souhaitez utiliser Wide-Area Bonjour. Si vous l'utilisez, le scanner doit être enregistré sur le serveur DNS afin de rechercher le scanner dans le secteur. |
| Activer AirPrint | Active Bonjour et AirPrint (service de numérisation). Cette touche est uniquement disponible lorsque AirPrint est désactivé. Remarque: Si AirPrint est désactivé, Mopria la numérisation depuis Chromebooks, Windows, et l'application Mopria Scan sont également désactivées. |

Problèmes lors de la préparation de la numérisation du réseau

Conseils pour résoudre les problèmes

Vérification du message d'erreur

En cas de problème, vérifiez d'abord la présence de messages sur le panneau de commande du scanner ou sur l'écran du pilote. Si l'option de notification par e-mail est active lorsque les événements se produisent, vous pouvez rapidement connaître le statut actuel.

Vérification du statut de communication

Vérifiez l'état de la communication de l'ordinateur serveur ou de l'ordinateur client à l'aide de la commande ping et ipconfig.

Test de connexion

Pour vérifier la connexion entre le scanner et le serveur de messagerie, effectuez un test de connexion à partir du scanner. Vérifiez également la connexion entre l'ordinateur client et le serveur pour vérifier l'état de la communication.

Initialisation des paramètres

Si les paramètres et l'état de la communication ne présentent aucun problème, le problème peut être résolu en désactivant ou en initialisant les paramètres réseau du scanner avant de les reconfigurer.

Accès impossible à Web Config

■ L'adresse IP n'est pas attribuée au scanner.

Solutions

Une adresse IP valide peut ne pas être attribuée au scanner. Configurez l'adresse IP depuis le panneau de commande du scanner. Vous pouvez vérifier les paramètres définis à partir du panneau de commande du scanner.

■ Le navigateur Web ne prend pas en charge le niveau de chiffrement pour SSL/TLS.

Solutions

SSL/TLS a le Force du cryptage. Vous pouvez ouvrir Web Config dans un navigateur Web qui prend en charge les chiffrements en masse, comme indiqué ci-dessous. Vérifiez que vous utilisez un navigateur pris en charge.

- 80 bits : AES256/AES128/3DES
- 112 bits : AES256/AES128/3DES
- 128 bits : AES256/AES128
- 192 bits : AES256
- 256 bits : AES256

■ **Le Certificat signé CA a expiré.**

Solutions

En cas de problème avec la date d'expiration du certificat, le message « Le certificat a expiré » est affiché lors de la connexion à Web Config via une communication SSL/TLS (https). Si le message s'affiche avant la date d'expiration, assurez-vous que la date du scanner est correctement configurée.

■ **Le nom commun du certificat et du scanner ne correspondent pas.**

Solutions

Si le nom commun au certificat et au scanner ne correspondent pas, le message « Le nom commun au certificat de sécurité et à l'imprimante... » s'affiche lors de l'accès à Web Config via une communication SSL/TLS (https). Ce message s'affiche car les adresses IP suivantes ne correspondent pas.

- L'adresse IP du scanner est saisie dans le nom commun pour créer un Certificat auto-signé ou CSR
- L'adresse IP saisie sur le navigateur Web lors de l'exécution de Web Config

Pour un Certificat auto-signé, mettez à jour le certificat.

Pour Certificat signé CA, prenez à nouveau le certificat pour le scanner.

■ **Le paramètre du serveur proxy de l'adresse locale n'est pas réglé sur le navigateur Web.**

Solutions

Lorsque le scanner est configuré pour utiliser un serveur proxy, configurez le navigateur Web afin qu'il ne se connecte pas à l'adresse locale via le serveur proxy.

- Windows :

Sélectionnez **Panneau de commande > Réseau et Internet > Options Internet > Connexions > Paramètres LAN > Serveur Proxy**, puis effectuez une configuration qui empêche l'utilisation du serveur Proxy pour le réseau local (adresses locales).

- Mac OS :

Sélectionnez **Préférences système (ou Paramètres système) > Réseau > Avancé > Proxy**, puis enregistrez l'adresse locale de **Ignorer les paramètres du proxy pour ces hôtes et domaines**.

Exemple :

192.168.1.* : Adresse locale 192.168.1.XXX, masque de sous-réseau 255.255.255.0

192.168.*.* : Adresse locale 192.168.XXX.XXX, masque de sous-réseau 255.255.0.0

■ **Le protocole DHCP est désactivé dans les paramètres de l'ordinateur.**

Solutions

Si le protocole DHCP, servant à obtenir une adresse IP automatiquement, est désactivé au niveau de l'ordinateur, il ne sera pas possible d'accéder à Web Config. Activez le protocole DHCP.

Exemple pour Windows 10 :

Dans le Panneau de configuration, cliquez sur **Réseau et Internet > Centre réseau et partage > Modifier les paramètres de la carte**. Ouvrez l'écran des propriétés de la connexion que vous utilisez, puis accédez à l'écran des propriétés de **Protocole Internet version 4 (TCP/IPv4)** ou **Protocole Internet version 6 (TCP/IPv6)**. Vérifiez que l'option **Obtenir une adresse IP automatiquement** est sélectionnée à l'écran qui s'affiche.

Personnalisation de l'affichage du panneau de commande

| | |
|--|----|
| Enregistrement de Prédéfinis. | 70 |
| Modifier l'écran d'accueil du panneau de commande. | 72 |

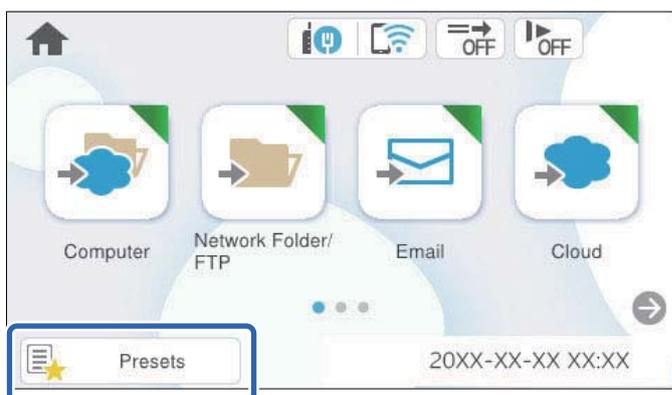
Enregistrement de Prédéfinis

Vous pouvez enregistrer les paramètres fréquemment utilisés en tant que **Prédéfinis**. Vous pouvez enregistrer jusqu'à 48 préréglages.

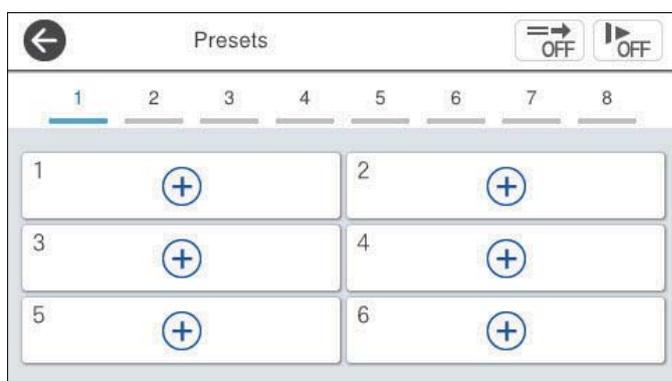
Remarque:

- Vous pouvez enregistrer les paramètres actuels en sélectionnant  à l'écran de lancement de la numérisation.
- Vous pouvez également enregistrer **Prédéf.** dans Web Config.
Sélectionnez l'onglet **Numériser** > **Prédéf.**.
- Si vous avez sélectionné **Numér. vers ordi** au moment de l'enregistrement, vous pouvez sauvegarder la tâche en tant que **Prédéf.** dans Document Capture Pro. Cette opération n'est possible que pour les ordinateurs connectés à un réseau. Enregistrez la tâche au préalable dans Document Capture Pro.
- Si la fonction d'authentification est activée, seul l'administrateur peut enregistrer des **Prédéf.**.

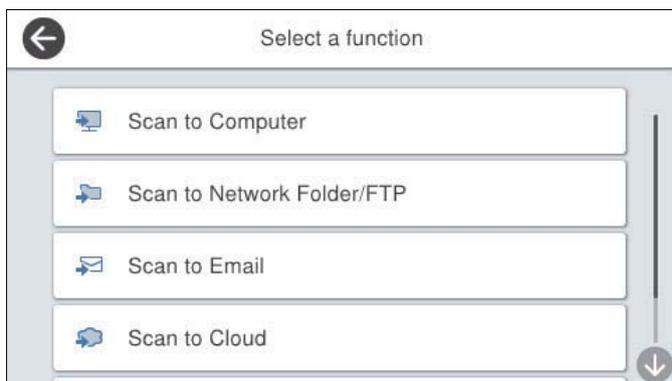
1. Sélectionnez **Prédéfinis** à l'écran d'accueil du panneau de commande du scanner.



2. Sélectionnez .



3. Sélectionnez le menu que vous souhaitez utiliser pour enregistrer un préréglage.



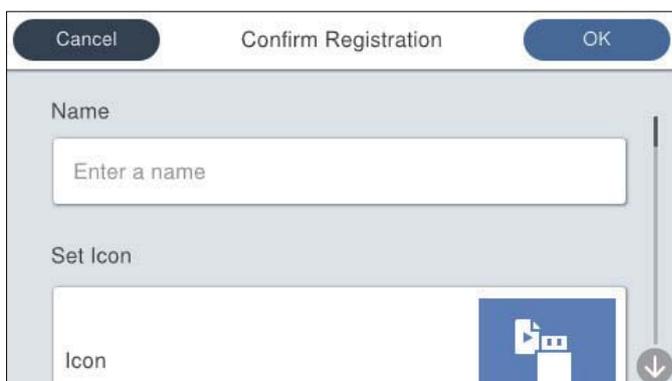
4. Définissez chaque élément, puis sélectionnez .

Remarque:

Si vous avez sélectionné **Numér. vers ordi**, sélectionnez l'ordinateur sur lequel Document Capture Pro est installé, puis sélectionnez une tâche enregistrée. Cette opération n'est possible que pour les ordinateurs connectés à un réseau.

5. Définissez les paramètres de présélection.

- Nom** : définissez le nom.
- Définissez l'icône** : choisissez l'image et la couleur à afficher pour l'icône.
- Paramètre Envoi rapide** : lance immédiatement la numérisation sans confirmation lorsque la présélection est sélectionnée.
- Contenu** : vérifiez les paramètres de numérisation.



6. Sélectionnez OK.

Options des menus de Prédéfinis

Vous pouvez modifier les paramètres d'un préréglage en sélectionnant  pour chaque préréglage.

Changer le nom :

permet de modifier le nom du préréglage.

Changez l'icône :

permet de modifier l'icône et la couleur du préréglage.

Paramètre Envoi rapide :

lance immédiatement la numérisation sans confirmation lorsque le préréglage est sélectionné.

Modifier la position :

modifie l'ordre d'affichage des préréglages.

Supprimer :

supprime le préréglage sélectionné.

Ajoutez ou supprimez l'icône sur l'Accueil :

ajoute ou supprime l'icône de préréglage de l'écran d'accueil.

Confirmer Détails :

permet d'afficher les paramètres d'un préréglage. Vous pouvez charger le préréglage en sélectionnant **Utilisez ce param..**

Modifier l'écran d'accueil du panneau de commande

Vous pouvez personnaliser l'écran d'accueil en sélectionnant **Param.** > **Modifier Accueil** sur le panneau de commande du scanner.

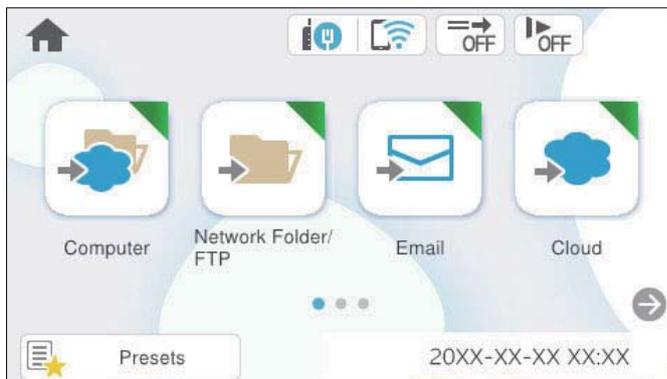
- Mise en page : modifie la méthode d'affichage des icônes de menu.
[« Modification de Mise en page de l'écran d'accueil » à la page 72](#)
- Ajouter icône : ajoute des icônes aux **Prédéfinis** paramètres que vous avez effectués, ou restaure des icônes qui ont été supprimées de l'écran.
[« Ajouter icône » à la page 73](#)
- Supprimer icône : supprime les icônes de l'écran d'accueil.
[« Supprimer icône » à la page 74](#)
- Déplacer icône : modifie l'ordre d'affichage des icônes.
[« Déplacer icône » à la page 75](#)
- Restaurer affich des icônes par défaut : restaure les paramètres d'affichage par défaut pour l'écran d'accueil.

Modification de Mise en page de l'écran d'accueil

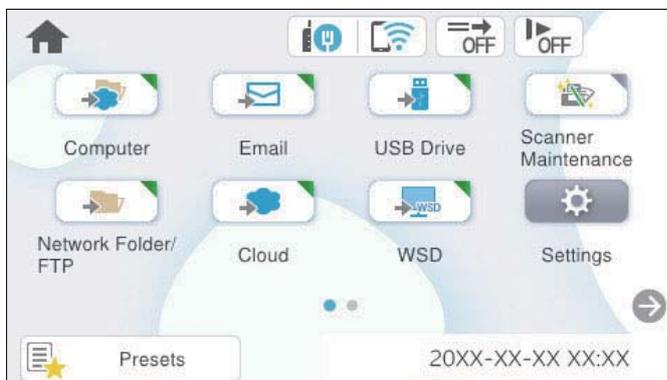
1. Sélectionnez **Param.** > **Modifier Accueil** > **Mise en page** sur le panneau de commande du scanner.

2. Sélectionnez **Ligne** ou **Matrice**.

Ligne :



Matrice :



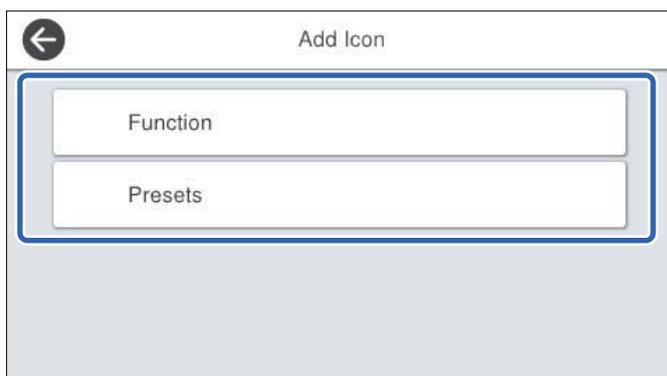
3. Sélectionnez  pour revenir à l'écran d'accueil et consulter celui-ci.

Ajouter icône

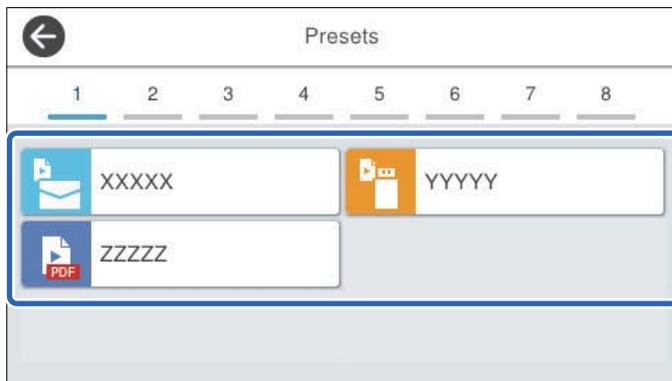
1. Sélectionnez **Param.** > **Modifier Accueil** > **Ajouter icône** sur le panneau de commande du scanner.

2. Sélectionnez **Fonction** ou **Prédéfinis**.

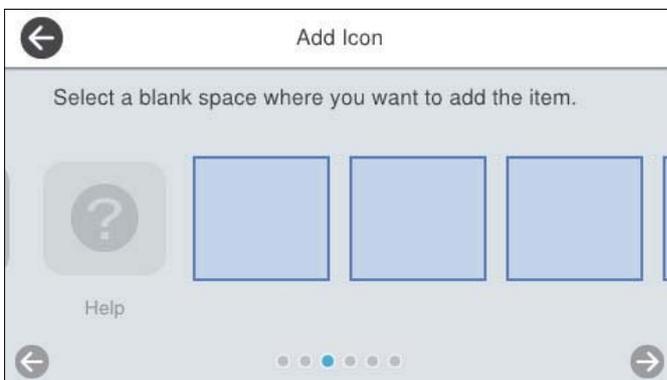
- Fonction** : affiche les fonctions par défaut indiquées sur l'écran d'accueil.
- Prédéfinis** : affiche les préréglages enregistrés.



3. Sélectionnez l'élément que vous souhaitez ajouter à l'écran d'accueil.



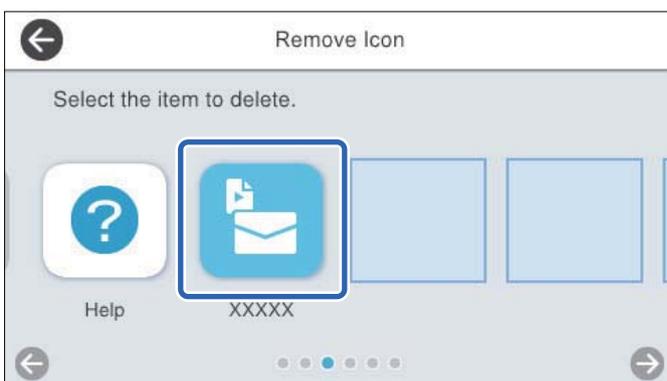
4. Sélectionnez l'espace vide dans lequel vous souhaitez installer l'élément.
Si vous souhaitez ajouter plusieurs icônes, répétez les étapes 3 à 4.



5. Sélectionnez  pour revenir à l'écran d'accueil et consulter celui-ci.

Supprimer icône

1. Sélectionnez **Param.** > **Modifier Accueil** > **Supprimer icône** sur le panneau de commande du scanner.
2. Sélectionnez l'icône que vous souhaitez supprimer.



3. Sélectionnez **Oui** pour terminer.

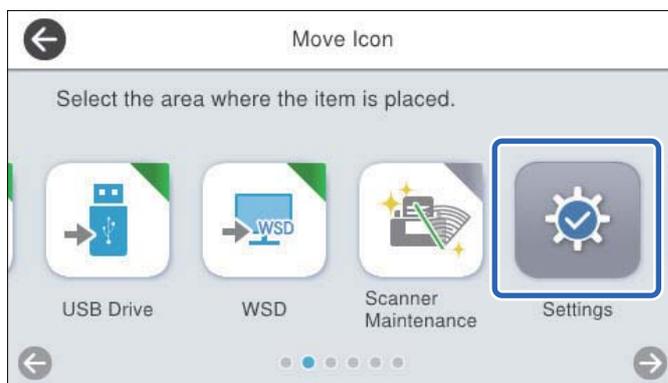
Si vous souhaitez supprimer plusieurs icônes, répétez la procédure 2 à 3.

4. Sélectionnez  pour revenir à l'écran d'accueil et consulter celui-ci.

Déplacer icône

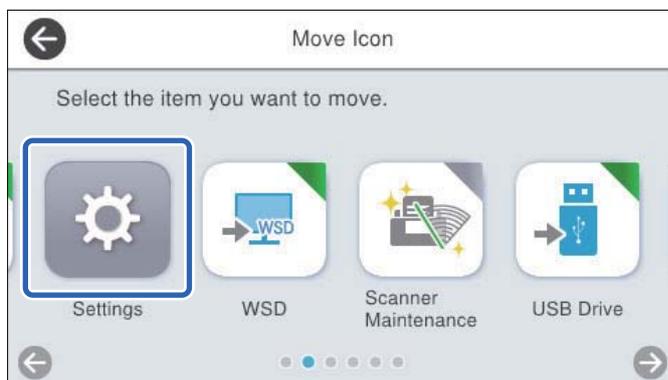
1. Sélectionnez **Param.** > **Modifier Accueil** > **Déplacer icône** sur le panneau de commande du scanner.

2. Sélectionnez l'icône que vous souhaitez déplacer.



3. Sélectionnez le cadre de destination.

Si une autre icône est déjà définie dans le cadre de destination, les icônes sont remplacées.



4. Sélectionnez  pour revenir à l'écran d'accueil et consulter celui-ci.

Paramètres de sécurité de base

| | |
|---|----|
| Présentation des fonctions de sécurité du produit. | 77 |
| Réglages de l'administrateur. | 77 |
| Limitation des fonctionnalités disponibles (Contrôle d'accès). | 83 |
| Désactivation de l'interface externe. | 85 |
| Activation de la vérification du programme au démarrage. | 86 |
| Désactiver la numérisation via le réseau depuis votre ordinateur. | 86 |
| Activation ou désactivation de la numérisation avec WSD. | 86 |
| Contrôler un scanner à distance. | 87 |
| Restauration des paramètres par défaut. | 89 |
| Informations Epson Remote Services. | 89 |
| Résolution des problèmes. | 89 |

Présentation des fonctions de sécurité du produit

Cette section présente la fonction de sécurité des périphériques Epson.

| Nom de la fonctionnalité | Type de fonctionnalité | Ce qu'il faut configurer | Ce qu'il faut prévenir |
|---|--|--|---|
| Configurer le mot de passe administrateur | Verrouille les paramètres système, tels que la configuration de la connexion pour le réseau ou USB. | Un administrateur définit un mot de passe pour le périphérique. Vous pouvez régler ou modifier les réglages depuis Web Config et le panneau de commande du scanner. | Empêcher de lire et de modifier illégalement les informations stockées dans le périphérique, telles que l'identifiant, le mot de passe, les paramètres réseau etc. Réduisez également de nombreux risques tels que la fuite d'informations pour l'environnement réseau ou la politique de sécurité. |
| Réglages du contrôle d'accès | Si vous vous connectez avec un compte utilisateur enregistré à l'avance, vous pouvez utiliser le périphérique. | Enregistrez un compte utilisateur. Vous pouvez enregistrer jusqu'à 10 comptes utilisateur. | La restriction des utilisateurs empêche l'utilisation non autorisée du périphérique. |
| Configuration de l'interface externe | Contrôle l'interface qui est connectée au périphérique. | Activez ou désactivez la connexion USB avec l'ordinateur. | Connexion USB de l'ordinateur : empêche une utilisation non autorisée du périphérique en interdisant la numérisation sans passer par le réseau. |

Informations connexes

- ➔ « Configurer le mot de passe administrateur » à la page 77
- ➔ « Désactivation de l'interface externe » à la page 85

Réglages de l'administrateur

Configurer le mot de passe administrateur

Lorsque vous choisissez un mot de passe administrateur, vous pouvez empêcher les utilisateurs de modifier les paramètres d'administration du système. Les valeurs par défaut sont fixées au moment de l'achat. Vous pouvez les modifier selon vos besoins.

Remarque:

Les valeurs par défaut des informations d'administration sont indiquées ci-dessous.

- Nom d'utilisateur (utilisé dans Web Config uniquement) : aucun (vierge)
- Mot de passe : indiqué sur l'étiquette collée sur le produit.

Si une étiquette « PASSWORD » se trouve à l'arrière, saisissez le nombre à 8 chiffres indiqué dessus. Si aucune étiquette « PASSWORD » n'est présente, saisissez le numéro de série situé à l'arrière du produit en guise de mot de passe administrateur initial.

Vous pouvez modifier le mot de passe administrateur à l'aide de Web Config, du panneau de commande du scanner ou d'Epson Device Admin. Si vous utilisez Epson Device Admin, reportez-vous au manuel d'Epson Device Admin ou à l'aide associée.

Modifier le mot de passe administrateur avec Web Config

Modifiez le mot de passe administrateur dans Web Config.

1. Rendez-vous dans à Web Config et sélectionnez l'onglet **Sécurité produit > Modifier le MdPasse administrateur**.
2. Saisissez les informations requises dans **MdPasse actuel**, **Nom d'utilisateur**, **Nouveau MdPasse**, puis **Confirmez le nouveau MdPasse**.

Le nouveau mot de passe doit contenir entre 8 et 20 caractères ou symboles alphanumériques d'un seul octet.

Remarque:

Les valeurs par défaut des informations d'administration sont indiquées ci-dessous.

- Nom d'utilisateur : aucun (vierge)
- Mot de passe : indiqué sur l'étiquette collée sur le produit.

Si une étiquette « PASSWORD » se trouve à l'arrière, saisissez le nombre à 8 chiffres indiqué dessus. Si aucune étiquette « PASSWORD » n'est présente, saisissez le numéro de série situé à l'arrière du produit en guise de mot de passe administrateur initial.



Important:

Veillez à ne pas oublier le mot de passe administrateur que vous avez choisi. Si vous oubliez votre mot de passe, vous ne pourrez pas le réinitialiser et devrez solliciter l'aide d'un personnel de service.

3. Sélectionnez **OK**.

Informations connexes

➔ [« Comment exécuter Web Config dans un navigateur Web » à la page 39](#)

Modifier le mot de passe administrateur depuis le panneau de commande du scanner

Vous pouvez modifier le mot de passe de l'administrateur depuis le panneau de commande du scanner.

1. Sélectionnez **Param.** sur le panneau de commande du scanner.
2. Sélectionnez **Administration système > Param admin**.
3. Sélectionnez **Mot de passe Admin > Changer**.
4. Saisissez le mot de passe actuel.

Remarque:

Le mot de passe administrateur initial (par défaut) au moment de l'achat est indiqué sur l'étiquette collée sur le produit. Si une étiquette « PASSWORD » se trouve à l'arrière, saisissez le nombre à 8 chiffres indiqué dessus. Si aucune étiquette « PASSWORD » n'est présente, saisissez le numéro de série situé à l'arrière du produit en guise de mot de passe administrateur initial.

5. Saisissez votre nouveau mot de passe.

Le nouveau mot de passe doit contenir entre 8 et 20 caractères ou symboles alphanumériques d'un seul octet.



Important:

Veillez à ne pas oublier le mot de passe administrateur que vous avez choisi. Si vous oubliez votre mot de passe, vous ne pourrez pas le réinitialiser et devrez solliciter l'aide d'un personnel de service.

6. Saisissez à nouveau le nouveau mot de passe pour le confirmer.

Un message de finalisation s'affiche.

Utilisation de Verrouiller le réglage pour le panneau de commande

Vous pouvez utiliser Verrouiller le réglage pour verrouiller le panneau de commande afin d'empêcher les utilisateurs de modifier des éléments liés aux paramètres du système.

Paramètre Verrouiller le réglage depuis le panneau de commande

1. Si vous souhaitez annuler le **Verrouiller le réglage** une fois qu'il a été activé, touchez  en haut à droite de l'écran d'accueil pour vous connecter en tant qu'administrateur.

L'option  ne s'affiche pas lorsque **Verrouiller le réglage** est désactivé. Si vous souhaitez activer ce paramètre, passez à l'étape suivante.

2. Sélectionnez **Param..**
3. Sélectionnez **Administration système > Param admin.**
4. Sélectionnez **Activé** ou **Off** en tant que **Verrouiller le réglage**.

Configuration de Verrouiller le réglage depuis Web Config

1. Sélectionnez l'onglet **Gestion des périphériques > Panneau de commande**.
2. Sélectionnez **MARCHE** ou **ARRÊT** pour **Verrouillage du panneau**.
3. Cliquez sur **OK**.

Informations connexes

➔ [« Comment exécuter Web Config dans un navigateur Web » à la page 39](#)

Champ d'action de Verrouiller le réglage dans le menu Param.

Voici la liste des éléments du menu **Param.** verrouillés par la fonction Verrouiller le réglage sur le panneau de commande.

✓ : à verrouiller.

- : ne peut pas être verrouillé.

| Menu Param. | | Verrouiller le réglage |
|------------------------|---|------------------------|
| Param de base | | - |
| | Luminosité LCD | - |
| | Sons | - |
| | Minut. veille | ✓ |
| | Temporisation arrêt | ✓ |
| | Aliment. directe | ✓ |
| | Régl. Date/Heure | ✓ |
| | Langue/Language | ✓/!-* |
| | Clavier (Il se peut que cette fonctionnalité ne soit pas disponible dans votre zone géographique.) | - |
| | Expiration opération | ✓ |
| | PC Connexion via USB | ✓ |
| Paramètres du scanner | | - |
| | Lent | - |
| | Minuterie d'arrêt double chargement | ✓ |
| | Fonction DFDS | - |
| | Protection papier | ✓ |
| | Détection de poussière sur la vitre | ✓ |
| | Détection par ultrasons de double alim | ✓ |
| | Expiration du Mode Alimentation automatique | ✓ |
| | Confirmer destinataire | ✓ |
| Modifier Accueil | | ✓ |
| | Mise en page | ✓ |
| | Ajouter icône | ✓ |
| | Supprimer icône | ✓ |
| | Déplacer icône | ✓ |
| | Restaurer affich des icônes par défaut | ✓ |
| Paramètres utilisateur | | ✓ |

| Menu Param. | | Verrouiller le réglage |
|-----------------------------|--------------------------|------------------------|
| | Dossier réseau/FTP | ✓ |
| | Email | ✓ |
| | Cloud | ✓ |
| | Clé USB | ✓ |
| Paramètres réseau | | ✓ |
| | Configuration Wi-Fi | ✓ |
| | Config LAN filaire | ✓ |
| | État réseau | ✓ |
| | Avancé | ✓ |
| Paramètres du service Web | | ✓ |
| | Services Epson Connect | ✓ |
| Document Capture Pro | | - |
| | Modifier les param. | ✓ |
| Gestionnaire de Contacts | | - |
| | Enreg./Supprimer | ✓/!* |
| | Fréquent | - |
| | Voir options | - |
| | Options de recherche | - |
| Administration système | | ✓ |
| | Gestionnaire de Contacts | ✓ |
| | Param admin | ✓ |
| | Restrictions | ✓ |
| | Contrôle d'accès | ✓ |
| | Chiffrement mot de passe | ✓ |
| | Recherche client | ✓ |
| | Paramètres WSD | ✓ |
| | Rest param défaut | ✓ |
| | Mise à jour firmware | ✓ |
| Informations sur l'appareil | | - |

| Menu Param. | | Verrouiller le réglage |
|---|--|------------------------|
| | Numéro de série | - |
| | Version actuelle | - |
| | Nbre total de numérisations | - |
| | Nbre de numérisations recto | - |
| | Nbre de numér Rec/Ver | - |
| | Nb de numéri. Feuille support | - |
| | Nb de nums ap remplacement du rouleau | - |
| | Nb de nums ap Nettoyage ordinaire | - |
| | État du dispositif d'authentification | - |
| | Informations Epson Open Platform | - |
| |  (Réinitialiser le nombre de numérisations) | ✓ |
| Entretien du scanner | | - |
| | Nettoyage des rouleaux | - |
| | Remplacement du rouleau | - |
| | Réinitialiser le nombre de numérisations | ✓ |
| | Comment remplacer | - |
| | Nettoyage ordinaire | - |
| | Réinitialiser le nombre de numérisations | ✓ |
| | Comment nettoyer | - |
| | Nettoyage de la vitre | - |
| Paramètre d'alerte de remplacement de rouleau | | ✓ |
| | Param cptage alertes | ✓ |
| Paramètres d'alerte de nettoyage classique | | ✓ |
| | Paramètre d'alerte d'avertissement | ✓ |
| | Param cptage alertes | ✓ |

* Vous pouvez spécifier si vous souhaitez autoriser ou pas des changements dans **Administration système > Restrictions**.

Connexion en tant qu'administrateur depuis le panneau de commande

Lorsque **Verrouiller le réglage** est activé, vous pouvez utiliser n'importe laquelle des méthodes suivantes pour vous connecter depuis le panneau de commande du scanner.

1. Touchez  dans l'angle supérieur droit de l'écran.
 2. Lorsque l'écran **Sélect. l'utilisateur** s'affiche, sélectionnez **Administrateur**.
 3. Saisissez le mot de passe pour vous connecter.
Un message Connexion terminée s'affiche, puis l'écran d'Accueil s'affiche sur le panneau de commande.
- Pour vous déconnecter, touchez  en haut à droite de l'écran, ou appuyez sur le bouton .

Limitation des fonctionnalités disponibles (Contrôle d'accès)

Vous pouvez restreindre les utilisateurs en enregistrant des comptes utilisateur sur le scanner.

Lorsque Contrôle d'accès est activé, l'utilisateur peut utiliser les fonctions de numérisation en saisissant le mot de passe sur le panneau de commande du scanner et en se connectant. Vous ne pouvez pas numériser si vous ne vous connectez pas.

Vous pouvez numériser depuis un ordinateur en enregistrant votre Nom utilisateur et Mot de passe dans le pilote du scanner (Epson Scan 2). Consultez l'aide Epson Scan 2 ou le *Guide d'utilisation* du produit pour plus d'informations sur les réglages.

Création du compte utilisateur

Vous pouvez créer un compte Contrôle d'accès.

1. Accédez à Web Config, puis sélectionnez l'onglet **Sécurité produit** > **Réglages du contrôle d'accès** > **Paramètres utilisateur**.
2. Cliquez sur **Ajouter** pour le numéro que vous souhaitez enregistrer.

Important:

Lorsque vous utilisez le scanner avec un système d'authentification d'Epson ou d'une autre entreprise, enregistrez le Nom d'utilisateur dans Réglages du contrôle d'accès dans le numéro d'emplacement 2 à 10.

Les applications logicielles telles que le système d'authentification utilisent le numéro d'emplacement 1, de sorte que le nom d'utilisateur ne s'affiche pas sur le panneau de commande du scanner.

3. Définissez chaque élément.
 - Nom d'utilisateur :
Saisissez un nom composé de 1 à 14 caractères alphanumériques à afficher dans la liste des noms d'utilisateurs.
 - Mot de passe :
Saisissez un mot de passe composé de jusqu'à 20 caractères de long au format ASCII (0x20-0x7E). Pour réinitialiser le mot de passe, laissez ce champ vide.
 - Cochez la case pour activer ou désactiver chaque fonction.
Sélectionnez **Numériser** si vous souhaitez autoriser les fonctions de numérisation.

4. Cliquez sur **Appliquer**.

Modification d'un compte utilisateur

Vous pouvez modifier le compte Contrôle d'accès enregistré.

1. Accédez à Web Config, puis sélectionnez l'onglet **Sécurité produit > Réglages du contrôle d'accès > Paramètres utilisateur**.
2. Cliquez sur **Modifier** pour le numéro que vous souhaitez modifier.
3. Modifiez chaque élément.
4. Cliquez sur **Appliquer**.

Suppression d'un compte utilisateur

Vous pouvez supprimer le compte Contrôle d'accès enregistré.

1. Accédez à Web Config, puis sélectionnez l'onglet **Sécurité produit > Réglages du contrôle d'accès > Paramètres utilisateur**.
2. Cliquez sur **Modifier** pour le numéro que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**.



Important:

*Si vous cliquez sur **Supprimer**, le compte utilisateur est supprimé sans qu'un message de confirmation s'affiche. Faites bien attention lorsque vous supprimez un compte.*

Activation du Contrôle d'accès

Lorsqu'on active Contrôle d'accès, seul l'utilisateur enregistré sera en mesure d'utiliser l'imprimante.

Remarque:

Si l'option Réglages du contrôle d'accès est activée, vous devrez avertir l'utilisateur quant aux informations de son compte.

1. Accédez à Web Config, puis sélectionnez l'onglet **Sécurité produit > Réglages du contrôle d'accès > De base**.
2. Sélectionnez **Permet le contrôle d'accès**.

Si vous activez Réglages du contrôle d'accès et numérisez depuis un ordinateur qui ne dispose pas d'informations d'authentification, sélectionnez **Permettre l'impression et la numérisation sans informations d'authentification d'un ordinateur**.

3. Cliquez sur **OK**.

Connexion à un scanner sur lequel Contrôle d'accès est activé

Lorsque **Contrôle d'accès** est activé, vous pouvez utiliser n'importe laquelle des méthodes suivantes pour vous connecter depuis le panneau de commande du scanner.

1. Touchez  dans l'angle supérieur droit de l'écran.
2. Lorsque l'écran **Sélect. l'utilisateur** s'affiche, sélectionnez l'utilisateur.
3. Saisissez le mot de passe pour vous connecter.
Un message Connexion terminée s'affiche, puis l'écran d'Accueil s'affiche sur le panneau de commande.

Pour vous déconnecter, touchez  en haut à droite de l'écran, ou appuyez sur le bouton .

Désactivation de l'interface externe

Vous pouvez désactiver l'interface utilisée pour connecter l'appareil au scanner. Effectuez les paramétrages pour limiter la numérisation autrement que par le réseau.

Remarque:

Vous pouvez également effectuer les paramétrages de restriction sur le panneau de commande du scanner.

*PC Connexion via USB : **Param.** > **Param de base** > **PC Connexion via USB***

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité produit** > **Interface externe**.

2. Sélectionnez **Désactiver** sur les fonctions que vous souhaitez définir.

Sélectionnez **Activer** lorsque vous souhaitez annuler le contrôle.

PC Connexion via USB

Vous pouvez restreindre l'utilisation de la connexion USB à partir de l'ordinateur. Si vous souhaitez la restreindre, sélectionnez **Désactiver**.

3. Cliquez sur **OK**.

4. Vérifiez que le port désactivé ne peut pas être utilisé.

PC Connexion via USB

Si le pilote a été installé sur l'ordinateur

Connectez le scanner à l'ordinateur à l'aide d'un câble USB, puis confirmez que le scanner ne numérise pas.

Si le pilote n'a pas été installé sur l'ordinateur

Windows :

Ouvrez le gestionnaire de périphériques et conservez-le, connectez le scanner à l'ordinateur à l'aide d'un câble USB, puis confirmez que l'affichage du contenu du gestionnaire de périphériques reste le même.

Mac OS :

Connectez le scanner à l'ordinateur à l'aide d'un câble USB, puis confirmez que vous ne pouvez pas ajouter le scanner depuis **Imprimantes et Scanners**.

Informations connexes

➔ « Comment exécuter Web Config dans un navigateur Web » à la page 39

Activation de la vérification du programme au démarrage

Si vous activez la fonctionnalité de vérification du programme au démarrage, le scanner procédera à une telle vérification au démarrage, pour vérifier qu'aucun tiers non autorisé n'a altéré le programme. Si un problème est détecté, le scanner ne démarre pas.

Remarque:

Activer cette fonction augmente le temps de démarrage du scanner.

1. Rendez-vous dans Web Config, puis sélectionnez l'onglet **Sécurité produit** > **Vérification du programme au démarrage**.

Remarque:

Vous pouvez également effectuer ces réglages depuis le panneau de commande du scanner.

Param. > **Administration système** > **Vérif. programme au démarrage**

2. Sélectionnez **MARCHE** pour activer **Vérification du programme au démarrage**.
3. Cliquez sur **OK**.

Désactiver la numérisation via le réseau depuis votre ordinateur

Vous pouvez effectuer ces réglages grâce à Web Config pour désactiver la numérisation via le réseau avec Epson Scan 2 depuis votre ordinateur.

1. Rendez-vous dans Web Config, puis sélectionnez l'onglet **Numériser** > **Numérisation en réseau**.
2. Dans **Epson Scan 2**, décochez la case **Activer la numérisation**.
3. Cliquez sur **Suivant**.
L'écran de confirmation du paramètre s'affiche.
4. Cliquez sur **OK**.

Activation ou désactivation de la numérisation avec WSD

Remarque:

Vous pouvez également effectuer ces réglages depuis le panneau de commande du scanner. Sélectionnez **Param.** > **Administration système** > **Paramètres WSD**.

Vous pouvez activer ou désactiver la numérisation avec WSD.

Si vous ne souhaitez pas que votre ordinateur configure le scanner comme un périphérique de numérisation WSD, désactivez les réglages WSD.

1. Rendez-vous dans Web Config, puis sélectionnez l'onglet **Sécurité réseau > Protocole**.
2. Dans **Paramètres WSD**, modifiez la case **Activer WSD**.
3. Cliquez sur **Suivant**.
L'écran de confirmation du paramètre s'affiche.
4. Cliquez sur **OK**.

Remarque:

Si votre ordinateur configure encore le scanner en tant que périphérique de numérisation WSD, sélectionnez l'onglet **Numériser > Numérisation en réseau**, puis décochez la case **Activer la numérisation dans AirPrint**.

Si AirPrint est désactivé, Mopria la numérisation depuis Chromebooks, Windows, et l'application Mopria Scan sont également désactivées.

Contrôler un scanner à distance

Vérification des informations pour un scanner à distance

Vous pouvez vérifier les informations suivantes du scanner en cours de fonctionnement depuis **État** en utilisant Web Config.

- État du produit
Vérifiez le statut, le service cloud, le numéro du produit, l'adresse MAC etc.
- État réseau
Vérifiez les informations du statut de connexion au réseau, l'adresse IP, le serveur DNS, etc.
- État d'utilisation
Vérifiez le premier jour de numérisation, le nombre de numérisations, etc.
- État matériel
Vérifiez le statut de chaque fonction du scanner.
- Cliché panneau
Affiche un aperçu de l'écran affiché sur le panneau de commande du scanner.

Réception de notifications par courrier électronique en cas d'événements

À propos des notifications par e-mail

C'est la fonction de notification qui, lorsque des événements tels qu'un arrêt de numérisation ou une erreur de scanner se produisent, envoie l'e-mail à l'adresse spécifiée.

Vous pouvez enregistrer jusqu'à cinq destinations et définir des paramètres de notification pour chaque destination.

Pour utiliser cette fonction, vous devez configurer le serveur de messagerie avant de configurer les notifications.

Informations connexes

➔ « [Enregistrer un serveur de messagerie](#) » à la page 46

Configuration de la notification d'e-mail

Configurer la notification d'e-mail à l'aide de Web Config.

1. Accédez à Web Config et sélectionnez l'onglet **Gestion des périphériques > Notification par email**.

2. Définissez le sujet de la notification de l'e-mail.

Sélectionnez le contenu qui s'affiche sur le sujet depuis les deux menus déroulants.

- Les contenus sélectionnés s'affichent en regard de **Sujet**.
- Les mêmes contenus ne peuvent pas être définis à gauche et à droite.
- Lorsque le nombre de caractères dans **Emplacement** dépasse 32 octets, les caractères qui dépassent 32 octets sont omis.

3. Saisissez l'adresse e-mail pour l'envoi de l'e-mail de notification.

Utilisez A-Z a-z 0-9 ! # \$ % & ' * + - . / = ? ^ _ { | } ~ @, et saisissez entre 1 et 255 caractères.

4. Sélectionnez la langue pour les notifications de l'e-mail.

5. Sélectionnez la case à cocher sur l'événement pour lequel vous souhaitez recevoir une notification.

Le nombre de **Paramètres notification** est lié au numéro de destination de **Param. adresse email**.

Exemple :

Si vous souhaitez envoyer une notification à l'adresse e-mail définie pour le numéro 1 dans **Param. adresse email** lorsque le mot de passe administrateur est modifié, sélectionnez la case à cocher pour la colonne **1** sur la ligne **Mot de passe admin changé**.

6. Cliquez sur **OK**.

Confirmez qu'une notification par e-mail sera envoyée en provoquant un événement.

Exemple : le mot de passe administrateur a été modifié.

Informations connexes

➔ « [Comment exécuter Web Config dans un navigateur Web](#) » à la page 39

Éléments pour la notification par email

| Éléments | Paramètres et explication |
|---------------------------|---|
| Mot de passe admin changé | Avertissement lorsque le mot de passe administrateur a été modifié. |
| Erreur scanner | Avertissement lorsque l'erreur du scanner est survenue. |

| Éléments | Paramètres et explication |
|-------------|--|
| Échec Wi-Fi | Avertissement lorsque l'erreur de l'interface LAN sans fil est survenue. |

Utilisation de Web Config pour contrôler l'alimentation du scanner

Si votre ordinateur est distant du scanner, vous pouvez encore utiliser Web Config pour éteindre ou redémarrer le scanner.

1. Rendez-vous dans Web Config, puis sélectionnez l'onglet **Gestion des périphériques > Marche/Arrêt**.
2. Sélectionnez **Éteindre** ou **Redémarrer**.
3. Cliquez sur **Exécuter**.

Restauration des paramètres par défaut

Vous pouvez sélectionner les paramètres réseau ou d'autres paramètres stockés sur le scanner pour les restaurer sur leur valeur par défaut.

1. Rendez-vous dans Web Config, puis sélectionnez l'onglet **Gestion des périphériques > Restaurer param. par défaut**.

Remarque:

Vous pouvez également effectuer ces réglages depuis le panneau de commande du scanner.

Param. > Administration système > Rest param défaut

2. Sélectionnez les éléments que vous souhaitez restaurer.
3. Cliquez sur **Exécuter**.

Terminez en suivant les instructions à l'écran.

Informations Epson Remote Services

Epson Remote Services est un service qui recueille régulièrement des informations sur le scanner sur Internet. Ce service peut être utilisé lorsque des consommables et des pièces de rechange doivent être remplacés ou réapprovisionnés, et pour résoudre rapidement des erreurs ou des problèmes.

Veuillez contacter votre revendeur pour en savoir plus sur les Epson Remote Services.

Résolution des problèmes

Mot de passe administrateur oublié

Vous avez besoin d'aide de la part d'un personnel de service. Contactez votre revendeur local.

Remarque:

Les éléments suivants indiquent les valeurs initiales pour le mot de passe administrateur dans Web Config.

Nom d'utilisateur : aucun (vierge)

Mot de passe : indiqué sur l'étiquette collée sur le produit.

Si une étiquette « PASSWORD » se trouve à l'arrière, saisissez le nombre à 8 chiffres indiqué dessus.

Si aucune étiquette « PASSWORD » n'est présente, saisissez le numéro de série situé à l'arrière du produit en guise de mot de passe administrateur initial.

Si vous restaurez le mot de passe administrateur, il reprendra la valeur qu'il avait au moment de l'achat.

Paramètres de sécurité avancés

| | |
|--|-----|
| Paramètres de sécurité et prévention du danger. | 92 |
| Contrôle à l'aide des protocoles. | 93 |
| Utilisation d'un certificat numérique. | 96 |
| Communication SSL/TLS avec le scanner. | 101 |
| Communication chiffrée par filtrage IPsec/IP. | 103 |
| Connexion du scanner à un réseau IEEE802.1X. | 115 |
| Résolution des problèmes pour la sécurité avancée. | 117 |

Paramètres de sécurité et prévention du danger

Lorsqu'un scanner est connecté à un réseau, vous pouvez y accéder depuis un site distant. De plus, de nombreuses personnes peuvent partager le scanner, ce qui permet d'améliorer l'efficacité opérationnelle et le confort. Cependant, les risques tels que l'accès illégal, l'utilisation illégale et la falsification de données augmentent. Si vous utilisez le scanner dans un environnement dans lequel vous pouvez accéder à Internet, les risques sont même supérieurs.

Pour les scanners qui ne disposent pas d'une protection d'accès de l'extérieur, il est possible de lire les journaux de travaux imprimés qui sont stockés dans l'imprimante depuis Internet.

Afin d'éviter ce risque, les scanners Epson disposent d'une variété de technologies de sécurité.

Configurez le scanner tel que nécessaire conformément aux conditions environnementales établies avec les informations sur l'environnement du client.

| Nom | Type de fonctionnalité | Ce qu'il faut configurer | Ce qu'il faut prévenir |
|------------------------|---|---|--|
| Contrôle du protocole | Contrôle les protocoles et les services à utiliser pour la communication entre les scanners et les ordinateurs, et active et désactive les fonctionnalités. | Un protocole ou service qui s'applique aux fonctionnalités autorisées ou interdites séparément. | Réduction des risques de sécurité pouvant survenir en raison d'une utilisation non autorisée en empêchant les utilisateurs d'utiliser des fonctions inutiles. |
| Communications SSL/TLS | Le contenu de communication est crypté avec des communications SSL/TLS lors de l'accès au serveur Epson sur Internet depuis le scanner, tel que la communication vers l'ordinateur par navigateur Web, à l'aide de Epson Connect, et de la mise à jour du micrologiciel. | Procurez-vous un certificat signé par une autorité de certification puis importez-le dans le scanner. | Effacer une identification du scanner grâce au certificat CA signé par une autorité de certification empêche l'usurpation d'identité et l'accès non autorisé. De plus, les contenus en communication de SSL/TLS sont protégés, et cela empêche la fuite de contenu pour la numérisation de données et d'informations de configuration. |
| IPsec/filtrage IP | Vous pouvez définir d'autoriser et de découper les données d'un client particulier ou d'un type particulier. Étant donné qu'IPsec protège les données grâce à l'unité de paquet IP (cryptage et authentification), vous pouvez communiquer en toute sécurité le protocole non sécurisé. | Créez une politique de base et une politique individuelle pour définir le client ou le type données qui peuvent accéder au scanner. | Protégez l'accès non autorisé, et la falsification et l'interception des données de communication vers le scanner. |
| IEEE 802.1X | Autorise uniquement les utilisateurs authentifiés à se connecter au réseau. Autorise uniquement un utilisateur autorisé à utiliser le scanner. | Paramètre d'authentification au serveur RADIUS (serveur d'authentification). | Protégez l'accès et l'utilisation non autorisés du scanner. |

Informations connexes

➔ [« Contrôle à l'aide des protocoles » à la page 93](#)

- ➔ « Communication SSL/TLS avec le scanner » à la page 101
- ➔ « Communication chiffrée par filtrage IPsec/IP » à la page 103
- ➔ « Connexion du scanner à un réseau IEEE802.1X » à la page 115

Paramètres de la fonction de sécurité

Lorsque vous définissez l'IPsec/filtrage IP ou le IEEE 802.1X, on vous recommande d'accéder à Web Config à l'aide de SSL/TLS pour communiquer les informations de paramètres afin de réduire les risques de sécurité tels que la falsification ou l'interception.

Assurez-vous de configurer le mot de passe administrateur avant de configurer l'IPsec/filtrage IP ou IEEE 802.1X.

Contrôle à l'aide des protocoles

Vous pouvez procéder à la numérisation en utilisant divers chemins et protocoles. Vous pouvez également utiliser la numérisation réseau sur un nombre indéterminé d'ordinateurs du réseau.

Vous pouvez réduire les risques pour la sécurité en limitant la numérisation à certains chemins ou en contrôlant les fonctions disponibles.

Contrôle des protocoles

Configurez les paramètres de protocole pris en charge par le scanner.

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité réseau** tab > **Protocole**.
2. Configurez chaque élément.
3. Cliquez sur **Suivant**.
4. Cliquez sur **OK**.

Les paramètres sont appliqués au scanner.

Informations connexes

- ➔ « Comment exécuter Web Config dans un navigateur Web » à la page 39

Protocoles que vous pouvez activer ou désactiver

| Protocole | Description |
|------------------|--|
| Réglages Bonjour | Vous pouvez spécifier si vous souhaitez utiliser Bonjour. Bonjour permet de rechercher des appareils, numériser avec et ainsi de suite. |
| Paramètres SLP | Vous pouvez activer ou désactiver la fonction SLP. SLP est utilisé pour la numérisation poussée et la recherche de réseau dans EpsonNet Config. |
| Paramètres WSD | Vous pouvez activer ou désactiver la fonction WSD. Lorsque ceci est activé, vous pouvez ajouter des périphériques WSD et numériser depuis le port WSD. |

| Protocole | Description |
|------------------|--|
| Paramètres LLTD | Vous pouvez activer ou désactiver la fonction LLTD. Lorsque celle-ci est activée, elle s'affiche dans la carte réseau Windows. |
| Paramètres LLMNR | Vous pouvez activer ou désactiver la fonction LLMNR. Lorsqu'elle est activée, vous pouvez utiliser la résolution du nom sans NetBIOS même si vous ne pouvez pas utiliser le DNS. |
| Param SNMPv1/v2c | Vous pouvez spécifier si vous souhaitez activer SNMPv1/v2c ou pas. Cette fonction est utilisée pour configurer des périphériques, pour la surveillance, etc. |
| Param SNMPv3 | Vous pouvez spécifier si vous souhaitez activer SNMPv3 ou pas. Cette fonction est utilisée pour chiffrer des périphériques, pour la surveillance, etc. |

Éléments de configuration du protocole

Réglages Bonjour

| Éléments | Valeur du paramètre et description |
|------------------------|---|
| Utiliser Bonjour | Sélectionnez ceci pour effectuer une recherche ou utiliser les périphériques via Bonjour. |
| Nom Bonjour | Affiche le nom Bonjour. |
| Nom du service Bonjour | Affiche le nom de service Bonjour. |
| Emplacement | Affiche le nom de l'emplacement Bonjour. |
| Wide-Area Bonjour | Définissez si vous souhaitez utiliser Wide-Area Bonjour. |

Paramètres SLP

| Éléments | Valeur du paramètre et description |
|-------------|--|
| Activer SLP | Sélectionnez ceci pour activer la fonction SLP. Cela est utilisé en tant que recherche réseau dans EpsonNet Config. |

Paramètres WSD

| Éléments | Valeur du paramètre et description |
|-------------------------------|---|
| Activer WSD | Sélectionnez ceci pour activer l'ajout de périphériques à l'aide de WSD et numérisez depuis le port WSD. |
| Expiration numérisation (sec) | Saisissez la valeur de temporisation de communication pour la numérisation WSD entre 3 et 3 600 secondes. |
| Nom de l'appareil | Affiche le nom du périphérique WSD. |
| Emplacement | Affiche le nom de l'emplacement WSD. |

Paramètres LLTD

| Éléments | Valeur du paramètre et description |
|-------------------|--|
| Activer LLTD | Sélectionnez ceci pour activer LLTD. Le scanner s'affiche sur la carte réseau Windows. |
| Nom de l'appareil | Affiche le nom du périphérique LLTD. |

Paramètres LLMNR

| Éléments | Valeur du paramètre et description |
|---------------|--|
| Activer LLMNR | Sélectionnez ceci pour activer LLMNR. Vous pouvez utiliser la résolution du nom sans NetBIOS, même si vous ne pouvez pas utiliser DNS. |

Param SNMPv1/v2c

| Éléments | Valeur du paramètre et description |
|-----------------------------------|--|
| Activer SNMPv1/v2c | Sélectionnez pour activer SNMPv1/v2c. |
| Autorité accès | Définissez l'autorité d'accès lorsque SNMPv1/v2c est activé. Sélectionnez En lecture seule ou Lecture/écriture . |
| Nom communauté (lecture seule) | Saisissez de 0 à caractères 32 ASCII (0x20 à 0x7E). |
| Nom communauté (lecture/écriture) | Saisissez de 0 à caractères 32 ASCII (0x20 à 0x7E). |

Param SNMPv3

| Éléments | Valeur du paramètre et description |
|---------------------------|--|
| Activer SNMPv3 | SNMPv3 est activé lorsque la case est cochée. |
| Nom d'utilisateur | Saisissez entre 1 et 32 caractères lors de l'utilisation de caractères de 1 octet. |
| Param authentification | |
| Algorithme | Sélectionnez un algorithme pour une authentification pour SNMPv3. |
| Mot de passe | Saisissez le mot de passe pour une authentification pour SNMPv3. Saisissez entre 8 et 32 caractères dans ASCII (0x20–0x7E). Laissez le champ vide si vous ne voulez pas en spécifier. |
| Confirmer le mot de passe | Saisissez le mot de passe que vous avez configuré pour le confirmer. |
| Param cryptage | |

| Éléments | | Valeur du paramètre et description |
|--------------|---------------------------|--|
| | Algorithme | Sélectionnez un algorithme pour un cryptage pour SNMPv3. |
| | Mot de passe | Saisissez un mot de passe pour un cryptage pour SNMPv3. Saisissez entre 8 et 32 caractères dans ASCII (0x20–0x7E). Laissez le champ vide si vous ne voulez pas en spécifier. |
| | Confirmer le mot de passe | Saisissez le mot de passe que vous avez configuré pour le confirmer. |
| Nom contexte | | Saisissez entre 32 caractères ou moins en Unicode (UTF-8). Laissez le champ vide si vous ne voulez pas en spécifier. Le nombre de caractères pouvant être saisi varie en fonction de la langue. |

Utilisation d'un certificat numérique

À propos de la certification numérique

Certificat signé CA

Ce certificat a été signé par l'autorité de certification (AC). Vous pouvez l'obtenir pour vous conformer à l'autorité de certification. Ce certificat atteste l'existence du scanner et sert à garantir la sécurité des données de communications SSL/TLS.

Dans le cas de communications SSL/TLS, il sert de certificat serveur.

Lorsqu'il est utilisé pour un filtrage IPsec/IP ou une communication IEEE 802.1X, c'est un certificat de serveur.

Certificat AC

Ce certificat fait partie de la chaîne du Certificat signé CA et est également appelé certificat AC intermédiaire. Il est utilisé par le navigateur Web pour valider le chemin du certificat du scanner lors d'un accès au serveur distant ou Web Config.

Dans le cas d'un certificat AC, choisissez quand valider le chemin du certificat serveur lors d'un accès depuis le scanner. Pour le scanner, choisissez de valider le chemin du Certificat signé CA pour les connexions SSL/TLS.

Vous pouvez obtenir le certificat AC du scanner auprès de l'autorité de certification qui a émis le certificat AC.

En outre, vous pouvez obtenir le certificat AC servant à valider le serveur distant auprès de l'autorité de certification qui a émis le Certificat signé CA de ce serveur.

Certificat auto-signé

Ce certificat est émis et signé par le scanner lui-même. Il est également appelé certificat racine. Étant donné que l'imprimante s'atteste elle-même, il n'est pas digne de confiance et n'empêche pas l'usurpation.

Utilisez le certificat pour configurer les paramètres de sécurité et établir une communication SSL/TLS simple sans le Certificat signé CA.

Si vous utilisez ce certificat pour une communication SSL/TLS, il est possible qu'une alerte de sécurité s'affiche sur un navigateur Web, car ce certificat n'est pas enregistré au niveau d'un tel navigateur. Vous pouvez uniquement utiliser le Certificat auto-signé pour les communications SSL/TLS.

Informations connexes

- ➔ [« Configuration d'un Certificat signé CA » à la page 97](#)
- ➔ [« Mise à jour d'un certificat à signature automatique » à la page 100](#)

➔ « Configuration d'un Certificat CA » à la page 101

Configuration d'un Certificat signé CA

Obtention d'un certificat signé par une autorité de certification

Pour obtenir un certificat signé par une autorité de certification, créez une demande de signature de certificat (CSR, Certificate Signing Request) et envoyez-la à l'autorité de certification. Vous pouvez créer une CSR à l'aide du logiciel Web Config et d'un ordinateur.

Procédez comme suit pour créer une CSR et obtenir un certificat signé par une autorité de certification à l'aide du logiciel Web Config. Lors de la création de la CSR à l'aide du logiciel Web Config, le certificat est au format PEM/DER.

1. Accédez à Web Config, puis sélectionnez l'onglet **Sécurité réseau**. Sélectionnez ensuite **SSL/TLS > Certificat** ou **IPsec/filtrage IP > Certificat client** ou **IEEE802.1X > Certificat client**.

Quoi que vous choisissiez, vous pouvez obtenir le même certificat et l'utiliser en commun.

2. Cliquez sur **Générer** sous **CSR**.

La page de création de CSR s'affiche.

3. Saisissez une valeur pour chaque élément.

Remarque:

Les abréviations et la longueur de clé disponibles varient en fonction de l'autorité de certification. Créez la demande en fonction des règles de chaque autorité de certification.

4. Cliquez sur **OK**.

Un message de finalisation s'affiche.

5. Sélectionnez l'onglet **Sécurité réseau**. Sélectionnez ensuite **SSL/TLS > Certificat** ou **IPsec/filtrage IP > Certificat client** ou **IEEE802.1X > Certificat client**.

6. Cliquez sur un des boutons de téléchargement **CSR** en fonction du format défini par chaque autorité de certification pour télécharger la demande de signature de certificat sur un ordinateur.



Important:

Ne générez pas de nouvelle demande de signature de certificat. Si vous le faites, vous pourriez ne pas être en mesure d'importer un Certificat signé CA émis.

7. Envoyez la demande de signature de certificat à une autorité de certification et obtenez un Certificat signé CA. Respectez les règles de chaque autorité de certification en ce qui concerne la forme et la méthode d'envoi.

8. Enregistrez le Certificat signé CA sur un ordinateur connecté au scanner.

L'obtention du Certificat signé CA est terminée une fois le certificat enregistré au niveau de la destination.

Informations connexes

➔ « Comment exécuter Web Config dans un navigateur Web » à la page 39

Éléments de configuration CSR

| Éléments | Paramètres et explication |
|--|--|
| Longueur de la clé | Sélectionnez une longueur de clé pour un CSR. |
| Nom commun | <p>Vous pouvez saisir entre 1 et 128 caractères. S'il s'agit d'une adresse IP, cela doit être une adresse IP statique. Vous pouvez saisir de 1 à 5 adresses IPv4, adresses IPv6, noms d'hôte, FQDN en les séparant avec des virgules.</p> <p>Le premier élément est enregistré sur le nom commun, et d'autres éléments sont stockés sur le champ alias de l'objet du certificat.</p> <p>Exemple :</p> <p>Adresse IP du scanner : 192.0.2.123, Nom du scanner : EPSONA1B2C3</p> <p>Nom commun : EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123</p> |
| Organisation/ Unité organisationnelle/ Localité/ État / Province | Vous pouvez saisir entre 0 et 64 caractères en ASCII (0x20–0x7E). Vous pouvez diviser les noms distinctifs par des virgules. |
| Pays | Saisissez un code de pays avec un nombre à deux chiffres spécifié par ISO-3166. |
| Adr. messagerie expéditeur | Vous pouvez saisir l'adresse email du destinataire pour le paramètre de serveur de messagerie. Saisissez la même adresse email que le Adr. messagerie expéditeur pour l'onglet Réseau > Serveur d'email > De base . |

Importation d'un certificat signé par une autorité de certification

Importez le Certificat signé CA obtenu dans le scanner.



Important:

- Assurez-vous que la date et l'heure du scanner sont correctement définies. Le certificat peut être invalide.
- Si vous obtenez un certificat à l'aide d'une demande de signature de certificat créée à partir du logiciel Web Config, vous pouvez importer le certificat une fois.

1. Accédez à Web Config, puis sélectionnez l'onglet **Sécurité réseau**. Sélectionnez ensuite **SSL/TLS > Certificat** ou **IPsec/filtrage IP > Certificat client** ou **IEEE802.1X > Certificat client**.
2. Cliquez sur **Importer**
La page d'importation des certificats s'affiche.
3. Saisissez une valeur pour chaque élément. Définissez le **Certificat CA 1** et le **Certificat CA 2** lorsque vous vérifiez le chemin du certificat dans le navigateur Web qui accède au scanner.

Les paramètres requis varient selon l'emplacement de création de la demande de signature de certificat et le format de fichier du certificat. Définissez les paramètres requis conformément à ce qui suit.

- Certificat au format PEM/DER obtenu à partir du logiciel Web Config
 - Clé privée** : ne configurez pas cette option car le scanner contient une clé privée.
 - Mot de passe** : ne pas configurer.
 - Certificat CA 1/Certificat CA 2** : en option

- Certificat au format PEM/DER obtenu à partir d'un ordinateur
 - Clé privée : vous devez définir cette option.
 - Mot de passe : ne pas configurer.
 - Certificat CA 1/Certificat CA 2 : en option
- Certificat au format PKCS#12 obtenu à partir d'un ordinateur
 - Clé privée : ne pas configurer.
 - Mot de passe : en option
 - Certificat CA 1/Certificat CA 2 : ne pas configurer.

4. Cliquez sur **OK**.

Un message de finalisation s'affiche.

Remarque:

Cliquez sur **Confirmer** pour vérifier les informations du certificat.

Informations connexes

➔ [« Comment exécuter Web Config dans un navigateur Web » à la page 39](#)

Éléments de paramètre d'importation de certificat CA signé par une autorité de certification

| Éléments | Paramètres et explication |
|--|--|
| Certificat de serveur ou Certificat client | Sélectionnez un format de certificat. Pour une connexion SSL/TLS, le Certificat de serveur s'affiche. Pour IPsec/filtrage IP ou IEEE 802.1X, le Certificat client s'affiche. |
| Clé privée | Si vous obtenez un certificat du format PEM/DER en utilisant un CSR créé depuis un ordinateur, spécifiez un fichier clé privé qui correspond à un certificat. |
| Mot de passe | Si le format de fichier est Certificat avec clé privée (PKCS#12) , saisissez le mot de passe pour chiffrer la clé privée définie lorsque vous obtenez le certificat. |
| Certificat CA 1 | Si le format de votre certificat est Certificat (PEM / DER) , importez un certificat d'une autorité certifiée qui délivre un Certificat signé CA utilisé en tant que certificat du serveur. Spécifiez un fichier si nécessaire. |
| Certificat CA 2 | Si le format de votre certificat est Certificat (PEM / DER) , importez un certificat d'une autorité certifiée qui délivre un Certificat CA 1. Spécifiez un fichier si nécessaire. |

Suppression d'un certificat signé par une autorité de certification

Vous pouvez supprimer un certificat importé une fois le certificat expiré ou s'il n'est plus nécessaire de chiffrer la connexion.

 **Important:**

Si vous obtenez un certificat à l'aide d'une demande de signature de certificat créée à partir du logiciel Web Config, vous ne pouvez importer de nouveau un certificat supprimé. Vous devez alors créer une demande de signature de certificat et obtenir de nouveau un certificat.

1. Accédez à la configuration Web, puis sélectionnez l'onglet **Sécurité réseau**. Sélectionnez ensuite **SSL/TLS > Certificat** ou **IPsec/filtrage IP > Certificat client** ou **IEEE802.1X > Certificat client**.
2. Cliquez sur **Supprimer**.
3. Confirmez que vous souhaitez supprimer le certificat dans le message qui s'affiche.

Informations connexes

➔ « [Comment exécuter Web Config dans un navigateur Web](#) » à la page 39

Mise à jour d'un certificat à signature automatique

Le Certificat auto-signé étant émis par le scanner, vous pouvez le mettre à jour lorsqu'il a expiré ou lorsque le contenu décrit n'est plus le même.

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité réseau** tab > **SSL/TLS > Certificat**.
2. Cliquez sur **Mettre à jour**.
3. Saisissez le paramètre **Nom commun**.

Vous pouvez saisir jusqu'à 5 adresses IPv4, adresses IPv6, noms d'hôte, noms de domaine complet compris entre 1 et 128 caractères et les séparer par des virgules. Le premier paramètre est stocké dans le nom commun et les autres sont stockés dans le champ d'alias pour l'objet du certificat.

Exemple :

Adresse IP du scanner : 192.0.2.123, Nom du scanner : EPSONA1B2C3

Nom commun : EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123

4. Définissez la période de validité du certificat.
5. Cliquez sur **Suivant**.
Un message de confirmation s'affiche.
6. Cliquez sur **OK**.
Le scanner est mis à jour.

Remarque:

Vous pouvez vérifier les informations de certificat dans l'onglet **Sécurité réseau > SSL/TLS > Certificat > Certificat auto-signé** et cliquez sur **Confirmer**.

Informations connexes

➔ « [Comment exécuter Web Config dans un navigateur Web](#) » à la page 39

Configuration d'un Certificat CA

Lorsque vous définissez le Certificat CA, vous pouvez valider le trajet vers le certificat CA du serveur auquel le scanner accède. Cela peut empêcher l'usurpation d'identité.

Vous pouvez obtenir le Certificat CA auprès de l'Autorité de certification où le Certificat signé CA a été délivré.

Importation d'un Certificat CA

Importez le Certificat CA vers le scanner.

1. Accédez à Web Config, puis sélectionnez l'onglet **Sécurité réseau > Certificat CA**.
2. Cliquez sur **Importer**.
3. Spécifiez le Certificat CA que vous souhaitez importer.
4. Cliquez sur **OK**.

Lorsque l'importation est terminée, vous êtes redirigé vers l'écran **Certificat CA**, et le Certificat CA s'affiche.

Informations connexes

➔ « [Comment exécuter Web Config dans un navigateur Web](#) » à la page 39

Suppression d'un Certificat CA

Vous pouvez supprimer le Certificat CA importé.

1. Accédez à Web Config puis sélectionnez l'onglet **Sécurité réseau > Certificat CA**.
2. Cliquez sur **Supprimer** en regard du Certificat CA que vous souhaitez supprimer.
3. Confirmez que vous souhaitez supprimer le certificat dans le message qui s'affiche.
4. Cliquez sur **Redémarrer réseau**, puis vérifiez que le Certificat CA supprimé n'est pas répertorié sur l'écran mis à jour.

Informations connexes

➔ « [Comment exécuter Web Config dans un navigateur Web](#) » à la page 39

Communication SSL/TLS avec le scanner

Lorsque le certificat du serveur est défini pour utiliser des communications SSL/TLS (Secure Sockets Layer/Transport Layer Security) avec le scanner, vous pouvez chiffrer le chemin de communication entre les ordinateurs. Procédez ainsi si vous voulez empêcher des accès à distance non autorisés.

Configuration des paramètres SSL/TLS de base

Si le scanner prend en charge la fonction HTTPS du serveur, vous pouvez utiliser une communication SSL/TLS pour crypter les communications. Vous pouvez configurer et gérer le scanner à l'aide de Web Config tout en assurant la sécurité.

Configurer la force de cryptage et la fonction de redirection.

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité réseau** > **SSL/TLS** > **De base**.
2. Sélectionnez une valeur pour chaque élément.
 - Force du cryptage
Sélectionnez le niveau de force de cryptage.
 - Rediriger HTTP vers HTTPS
Redirigez vers HTTPS lorsqu'on accède à HTTP.
3. Cliquez sur **Suivant**.
Un message de confirmation s'affiche.
4. Cliquez sur **OK**.
Le scanner est mis à jour.

Informations connexes

➔ [« Comment exécuter Web Config dans un navigateur Web » à la page 39](#)

Configuration d'un certificat de serveur pour le scanner

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité réseau** > **SSL/TLS** > **Certificat**.
2. Spécifiez un certificat à utiliser sur **Certificat de serveur**.
 - Certificat auto-signé
Un certificat à signature automatique est généré par le scanner. Si vous n'obtenez pas un certificat CA signé par une autorité de certification, sélectionnez l'élément suivant.
 - Certificat signé CA
Si vous obtenez et importez un certificat CA signé par une autorité de certification à l'avance, vous pouvez préciser ceci.
3. Cliquez sur **Suivant**.
Un message de confirmation s'affiche.
4. Cliquez sur **OK**.
Le scanner est mis à jour.

Informations connexes

➔ [« Comment exécuter Web Config dans un navigateur Web » à la page 39](#)

➔ [« Configuration d'un Certificat signé CA » à la page 97](#)

➔ « Configuration d'un Certificat CA » à la page 101

Communication chiffrée par filtrage IPsec/IP

À propos d'IPsec/filtrage IP

Vous pouvez filtrer le trafic en fonction des adresses IP, des services et du port à l'aide de la fonction de filtrage IPsec/IP. En associant les filtres, vous pouvez configurer le scanner de manière à ce qu'il accepte ou bloque certains clients et certaines données. Vous pouvez également améliorer le niveau de sécurité en utilisant un filtrage IPsec.

Remarque:

Les ordinateurs sous Windows Vista ou plus, ou sous Windows Server 2008 ou plus, gèrent l'IPsec.

Configuration de la politique par défaut

Pour filtrer le trafic, configurez la politique par défaut. La politique par défaut s'applique à tous les utilisateurs ou groupes qui se connectent au scanner. Pour un meilleur contrôle des utilisateurs et des groupes d'utilisateurs, configurez des politiques de groupes.

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité réseau > IPsec/filtrage IP > De base**.
2. Saisissez une valeur pour chaque élément.
3. Cliquez sur **Suivant**.
Un message de confirmation s'affiche.
4. Cliquez sur **OK**.
Le scanner est mis à jour.

Informations connexes

➔ « Comment exécuter Web Config dans un navigateur Web » à la page 39

Éléments de paramétrage Politique par défaut

Politique par défaut

| Éléments | Paramètres et explication |
|-------------------|--|
| IPsec/filtrage IP | Vous pouvez activer ou désactiver une fonction de filtrage IPsec/IP. |

Contrôle des accès

Configurez la méthode de contrôle pour le trafic de paquets IP.

| Éléments | Paramètres et explication |
|-------------------|---|
| Autoriser l'accès | Sélectionnez cette option pour autoriser le passage des paquets IP configurés. |
| Refuser l'accès | Sélectionnez cette option pour refuser le passage des paquets IP configurés. |
| IPsec | Sélectionnez cette option pour autoriser le passage des paquets IPsec configurés. |

Version IKE

Sélectionnez **IKEv1** ou **IKEv2** pour **Version IKE**. Effectuez votre choix en fonction du périphérique auquel le scanner est connecté.

IKEv1

Les éléments suivants sont affichés lorsque vous sélectionnez **IKEv1** pour **Version IKE**.

| Éléments | Paramètres et explication |
|-------------------------------|--|
| Méthode d'authentification | Pour sélectionner l'option Certificat , vous devez préalablement obtenir et importer un certificat signé par une autorité de certification. |
| Clé pré-partagée | Si vous sélectionnez l'option Clé pré-partagée pour le paramètre Méthode d'authentification , saisissez une clé prépartagée faisant de 1 à 127 caractères. |
| Confirmer la clé pré-partagée | Saisissez la clé configurée pour confirmation. |

IKEv2

Les éléments suivants sont affichés lorsque vous sélectionnez **IKEv2** pour **Version IKE**.

| Éléments | Paramètres et explication | |
|----------|-------------------------------|--|
| Local | Méthode d'authentification | Pour sélectionner l'option Certificat , vous devez préalablement obtenir et importer un certificat signé par une autorité de certification. |
| | Type ID | Si vous sélectionnez Clé pré-partagée pour Méthode d'authentification , sélectionnez le type d'identifiant du scanner. |
| | ID | Saisissez l'identifiant du scanner correspondant au type sélectionné. Le premier caractère ne doit pas être « @ », « # » et « = ». Nom distinctif : saisissez de 1 à 255 caractères ASCII sur 1 octet (0x20 à 0x7E). Vous devez inclure « = ». Adresse IP : effectuez la saisie au format IPv4 ou IPv6. FQDN : saisissez entre 1 et 255 caractères (A-Z, a-z, 0-9, - et .). Adresse de la messagerie : saisissez de 1 à 255 caractères ASCII sur 1 octet (0x20 à 0x7E). Vous devez inclure « @ ». ID clé : saisissez de 1 à 255 caractères ASCII sur 1 octet (0x20 à 0x7E). |
| | Clé pré-partagée | Si vous sélectionnez l'option Clé pré-partagée pour le paramètre Méthode d'authentification , saisissez une clé prépartagée faisant de 1 à 127 caractères. |
| | Confirmer la clé pré-partagée | Saisissez la clé configurée pour confirmation. |

| Éléments | | Paramètres et explication |
|----------|-------------------------------|--|
| Distante | Méthode d'authentification | Pour sélectionner l'option Certificat , vous devez préalablement obtenir et importer un certificat signé par une autorité de certification. |
| | Type ID | Si vous sélectionnez Clé pré-partagée pour Méthode d'authentification , sélectionnez le type d'identifiant du périphérique que vous souhaitez authentifier. |
| | ID | Saisissez l'identifiant du scanner correspondant au type sélectionné. Le premier caractère ne doit pas être « @ », « # » et « = ». Nom distinctif : saisissez de 1 à 255 caractères ASCII sur 1 octet (0x20 à 0x7E). Vous devez inclure « = ». Adresse IP : effectuez la saisie au format IPv4 ou IPv6. FQDN : saisissez entre 1 et 255 caractères (A–Z, a–z, 0–9, - et .). Adresse de la messagerie : saisissez de 1 à 255 caractères ASCII sur 1 octet (0x20 à 0x7E). Vous devez inclure « @ ». ID clé : saisissez de 1 à 255 caractères ASCII sur 1 octet (0x20 à 0x7E). |
| | Clé pré-partagée | Si vous sélectionnez l'option Clé pré-partagée pour le paramètre Méthode d'authentification , saisissez une clé prépartagée faisant de 1 à 127 caractères. |
| | Confirmer la clé pré-partagée | Saisissez la clé configurée pour confirmation. |

Encapsulation

Si vous sélectionnez l'option **IPsec** pour le paramètre **Contrôle des accès**, vous devez configurer un mode d'encapsulation.

| Éléments | Paramètres et explication |
|-------------------|---|
| Mode de transport | Sélectionnez cette option si vous utilisez uniquement le scanner dans un même réseau local. Les paquets IP de couche 4 ou supérieure sont chiffrés. |
| Mode de tunnel | Si vous utilisez le scanner sur un réseau Internet, tel que IPsec-VPN, sélectionnez cette option. L'en-tête et les données des paquets IP sont chiffrés. Adresse de la passerelle à distance : si vous sélectionnez l'option Mode de tunnel pour le paramètre Encapsulation , saisissez une adresse de passerelle faisant de 1 à 39 caractères. |

Protocole de sécurité

Si vous sélectionnez l'option **IPsec** pour le paramètre **Contrôle des accès**, vous devez sélectionner une option.

| Éléments | Paramètres et explication |
|----------|---|
| ESP | Sélectionnez cette option pour garantir l'intégrité de l'authentification et des données, et chiffrer les données. |
| AH | Sélectionnez cette option pour garantir l'intégrité de l'authentification et des données. Vous pouvez utiliser le protocole IPsec, même si le chiffrement des données est interdit. |

❑ Paramètres algorithme

Il vous est recommandé de sélectionner **N'importe lequel** pour tous les paramètres ou sélectionnez autre chose que **N'importe lequel** pour chaque paramètre. Si vous sélectionnez **N'importe lequel** pour certains des paramètres, mais autre chose que **N'importe lequel** pour d'autres paramètres, l'appareil peut ne pas parvenir à communiquer en fonction de l'autre appareil que vous souhaitez authentifier.

| Éléments | | Paramètres et explication |
|----------|------------------|--|
| IKE | Cryptage | Sélectionnez l'algorithme de chiffrement pour IKE. Les éléments varient en fonction de la version de IKE. |
| | Authentification | Sélectionnez l'algorithme d'authentification pour IKE. |
| | Échange clé | Sélectionnez l'algorithme d'échange de clé pour IKE. Les éléments varient en fonction de la version de IKE. |
| ESP | Cryptage | Sélectionnez l'algorithme de chiffrement pour ESP. Disponible lorsque l'option ESP est réglée sur Protocole de sécurité . |
| | Authentification | Sélectionnez l'algorithme d'authentification pour ESP. Disponible lorsque l'option ESP est réglée sur Protocole de sécurité . |
| AH | Authentification | Sélectionnez l'algorithme de chiffrement pour AH. Disponible lorsque l'option AH est réglée sur Protocole de sécurité . |

Configuration de la politique de groupe

Une politique de groupe est composée d'une ou plusieurs règles qui s'appliquent à un utilisateur ou à un groupe d'utilisateurs. Le scanner contrôle les paquets IP qui correspondent aux politiques définies. Les paquets IP sont authentifiés dans l'ordre des politiques de groupes, de 1 à 10, puis en fonction de la politique par défaut.

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité réseau > IPsec/filtrage IP > De base**.
2. Cliquez sur un onglet numéroté à configurer.
3. Saisissez une valeur pour chaque élément.
4. Cliquez sur **Suivant**.
Un message de confirmation s'affiche.
5. Cliquez sur **OK**.
Le scanner est mis à jour.

Éléments de paramétrage Politique de groupe

| Éléments | Paramètres et explication |
|-----------------------------------|--|
| Activer cette politique de groupe | Vous pouvez activer ou désactiver une politique de groupe. |

Contrôle des accès

Configurez la méthode de contrôle pour le trafic de paquets IP.

| Éléments | Paramètres et explication |
|-------------------|---|
| Autoriser l'accès | Sélectionnez cette option pour autoriser le passage des paquets IP configurés. |
| Refuser l'accès | Sélectionnez cette option pour refuser le passage des paquets IP configurés. |
| IPsec | Sélectionnez cette option pour autoriser le passage des paquets IPsec configurés. |

Adresse locale (scanner)

Sélectionnez une adresse IPv4 ou IPv6 correspondant à votre environnement réseau. Si une adresse IP est affectée automatiquement, vous pouvez sélectionner **Utiliser l'adresse IPv4 obtenue automatiquement**.

Remarque:

Si une adresse IPv6 est automatiquement attribuée, il est possible que la connexion ne soit pas disponible. Configurez une adresse IPv6 statique.

Adresse distante (hôte)

Saisissez l'adresse IP d'un périphérique pour contrôler l'accès. L'adresse IP doit contenir de 43 caractères maximum. Si vous ne saisissez aucune adresse IP, toutes les adresses sont contrôlées.

Remarque:

Si une adresse IP est automatiquement attribuée (attribuée par le serveur DHCP, par exemple), il est possible que la connexion ne soit pas disponible. Configurez une adresse IP statique.

Mode de sélection du port

Sélectionnez une méthode de désignation des ports.

- Nom du service

Si vous sélectionnez l'option **Nom du service** pour le paramètre **Mode de sélection du port**, vous devez sélectionner une option.

- Protocole de transport

Si vous sélectionnez l'option **Numéro de port** pour le paramètre **Mode de sélection du port**, vous devez configurer un mode d'encapsulation.

| Éléments | Paramètres et explication |
|--------------------------|--|
| N'importe quel protocole | Sélectionnez cette option pour contrôler tous les types de protocoles. |
| TCP | Sélectionnez cette option pour contrôler les données pour l'envoi individuel. |
| UDP | Sélectionnez cette option pour contrôler les données pour la diffusion et la multidiffusion. |
| ICMPv4 | Sélectionnez cette option pour contrôler la commande ping. |

- Port local

Si vous sélectionnez **Numéro de port** pour **Mode de sélection du port** et si vous sélectionnez **TCP** ou **UDP** pour **Protocole de transport**, saisissez des numéros de port pour contrôler les paquets reçus en les séparant par des virgules. Vous pouvez saisir un maximum de dix numéros de ports.

Exemple : 20,80,119,5220

Si vous ne saisissez aucun numéro de port, tous les ports sont contrôlés.

Port distant

Si vous sélectionnez **Numéro de port** pour **Mode de sélection du port** et si vous sélectionnez **TCP** ou **UDP** pour **Protocole de transport**, saisissez des numéros de port pour contrôler les paquets envoyés en les séparant par des virgules. Vous pouvez saisir un maximum de dix numéros de ports.

Exemple : 25,80,143,5220

Si vous ne saisissez aucun numéro de port, tous les ports sont contrôlés.

Version IKE

Sélectionnez **IKEv1** ou **IKEv2** pour **Version IKE**. Effectuez votre choix en fonction du périphérique auquel le scanner est connecté.

IKEv1

Les éléments suivants sont affichés lorsque vous sélectionnez **IKEv1** pour **Version IKE**.

| Éléments | Paramètres et explication |
|-------------------------------|--|
| Méthode d'authentification | Si vous sélectionnez l'option IPsec pour le paramètre Contrôle des accès , vous devez sélectionner une option. Le certificat utilisé est le même que celui de la politique par défaut. |
| Clé pré-partagée | Si vous sélectionnez l'option Clé pré-partagée pour le paramètre Méthode d'authentification , saisissez une clé prépartagée faisant de 1 à 127 caractères. |
| Confirmer la clé pré-partagée | Saisissez la clé configurée pour confirmation. |

❑ IKEv2

Les éléments suivants sont affichés lorsque vous sélectionnez **IKEv2** pour **Version IKE**.

| Éléments | | Paramètres et explication |
|----------|-------------------------------|--|
| Local | Méthode d'authentification | Si vous sélectionnez l'option IPsec pour le paramètre Contrôle des accès , vous devez sélectionner une option. Le certificat utilisé est le même que celui de la politique par défaut. |
| | Type ID | Si vous sélectionnez Clé pré-partagée pour Méthode d'authentification , sélectionnez le type d'identifiant du scanner. |
| | ID | Saisissez l'identifiant du scanner correspondant au type sélectionné. Le premier caractère ne doit pas être « @ », « # » et « = ». Nom distinctif : saisissez de 1 à 255 caractères ASCII sur 1 octet (0x20 à 0x7E). Vous devez inclure « = ». Adresse IP : effectuez la saisie au format IPv4 ou IPv6. FQDN : saisissez entre 1 et 255 caractères (A–Z, a–z, 0–9, - et .). Adresse de la messagerie : saisissez de 1 à 255 caractères ASCII sur 1 octet (0x20 à 0x7E). Vous devez inclure « @ ». ID clé : saisissez de 1 à 255 caractères ASCII sur 1 octet (0x20 à 0x7E). |
| | Clé pré-partagée | Si vous sélectionnez l'option Clé pré-partagée pour le paramètre Méthode d'authentification , saisissez une clé prépartagée faisant de 1 à 127 caractères. |
| | Confirmer la clé pré-partagée | Saisissez la clé configurée pour confirmation. |
| Distante | Méthode d'authentification | Si vous sélectionnez l'option IPsec pour le paramètre Contrôle des accès , vous devez sélectionner une option. Le certificat utilisé est le même que celui de la politique par défaut. |
| | Type ID | Si vous sélectionnez Clé pré-partagée pour Méthode d'authentification , sélectionnez le type d'identifiant du périphérique que vous souhaitez authentifier. |
| | ID | Saisissez l'identifiant du scanner correspondant au type sélectionné. Le premier caractère ne doit pas être « @ », « # » et « = ». Nom distinctif : saisissez de 1 à 255 caractères ASCII sur 1 octet (0x20 à 0x7E). Vous devez inclure « = ». Adresse IP : effectuez la saisie au format IPv4 ou IPv6. FQDN : saisissez entre 1 et 255 caractères (A–Z, a–z, 0–9, - et .). Adresse de la messagerie : saisissez de 1 à 255 caractères ASCII sur 1 octet (0x20 à 0x7E). Vous devez inclure « @ ». ID clé : saisissez de 1 à 255 caractères ASCII sur 1 octet (0x20 à 0x7E). |
| | Clé pré-partagée | Si vous sélectionnez l'option Clé pré-partagée pour le paramètre Méthode d'authentification , saisissez une clé prépartagée faisant de 1 à 127 caractères. |
| | Confirmer la clé pré-partagée | Saisissez la clé configurée pour confirmation. |

Encapsulation

Si vous sélectionnez l'option **IPsec** pour le paramètre **Contrôle des accès**, vous devez configurer un mode d'encapsulation.

| Éléments | Paramètres et explication |
|-------------------|---|
| Mode de transport | Sélectionnez cette option si vous utilisez uniquement le scanner dans un même réseau local. Les paquets IP de couche 4 ou supérieure sont chiffrés. |
| Mode de tunnel | Si vous utilisez le scanner sur un réseau Internet, tel que IPsec-VPN, sélectionnez cette option. L'en-tête et les données des paquets IP sont chiffrés. Adresse de la passerelle à distance : Si vous sélectionnez l'option Mode de tunnel pour le paramètre Encapsulation , saisissez une adresse de passerelle faisant de 1 à 39 caractères. |

Protocole de sécurité

Si vous sélectionnez l'option **IPsec** pour le paramètre **Contrôle des accès**, vous devez sélectionner une option.

| Éléments | Paramètres et explication |
|----------|---|
| ESP | Sélectionnez cette option pour garantir l'intégrité de l'authentification et des données, et chiffrer les données. |
| AH | Sélectionnez cette option pour garantir l'intégrité de l'authentification et des données. Vous pouvez utiliser le protocole IPsec, même si le chiffrement des données est interdit. |

Paramètres algorithme

Il vous est recommandé de sélectionner **N'importe lequel** pour tous les paramètres ou sélectionnez autre chose que **N'importe lequel** pour chaque paramètre. Si vous sélectionnez **N'importe lequel** pour certains des paramètres, mais autre chose que **N'importe lequel** pour d'autres paramètres, l'appareil peut ne pas parvenir à communiquer en fonction de l'autre appareil que vous souhaitez authentifier.

| Éléments | | Paramètres et explication |
|----------|------------------|--|
| IKE | Cryptage | Sélectionnez l'algorithme de chiffrement pour IKE. Les éléments varient en fonction de la version de IKE. |
| | Authentification | Sélectionnez l'algorithme d'authentification pour IKE. |
| | Échange clé | Sélectionnez l'algorithme d'échange de clé pour IKE. Les éléments varient en fonction de la version de IKE. |
| ESP | Cryptage | Sélectionnez l'algorithme de chiffrement pour ESP. Disponible lorsque l'option ESP est réglée sur Protocole de sécurité . |
| | Authentification | Sélectionnez l'algorithme d'authentification pour ESP. Disponible lorsque l'option ESP est réglée sur Protocole de sécurité . |
| AH | Authentification | Sélectionnez l'algorithme de chiffrement pour AH. Disponible lorsque l'option AH est réglée sur Protocole de sécurité . |

Combinaison de Adresse locale (scanner) et Adresse distante (hôte) sur une Politique de groupe

| | | Paramétrage de Adresse locale (scanner) | | |
|--|-------------------------------------|---|--------------------|--|
| | | IPv4 | IPv6* ² | N'importe quelle adresse* ³ |
| Paramétrage de Adresse distante (hôte) | IPv4* ¹ | ✓ | – | ✓ |
| | IPv6* ¹ , * ² | – | ✓ | ✓ |
| | Vide | ✓ | ✓ | ✓ |

*1 Si IPsec est sélectionné pour **Contrôle des accès**, vous ne pouvez pas préciser la longueur du préfixe.

*2 Si IPsec est sélectionné pour **Contrôle des accès**, vous pouvez sélectionner une adresse de lien local (fe80::) mais la politique de groupe sera désactivée.

*3 À l'exception des adresses de lien local IPv6.

Informations connexes

➔ [« Comment exécuter Web Config dans un navigateur Web » à la page 39](#)

Références du nom de service sur la politique de groupe

Remarque:

Des services indisponibles s'affichent mais ne peuvent pas être sélectionnés.

| Nom du service | Type de protocole | Numéro du port local | Numéro du port à distance | Fonctions contrôlées |
|-----------------------------|-------------------|----------------------|---------------------------|---|
| N'importe lequel | – | – | – | Tous les services |
| ENPC | UDP | 3289 | Tous les ports | En recherchant un scanner dans des applications telles que Epson Device Admin et le pilote d'un scanner |
| SNMP | UDP | 161 | Tous les ports | Acquisition et configuration de MIB depuis des applications telles que Epson Device Admin et le pilote de scanner Epson |
| WSD | TCP | Tous les ports | 5357 | Contrôle de WSD |
| WS-Discovery | UDP | 3702 | Tous les ports | Recherche de scanners WSD |
| Network Scan | TCP | 1865 | Tous les ports | Transmission des données numérisées depuis Document Capture Pro |
| Network Push Scan | TCP | Tous les ports | 2968 | Acquisition d'informations relatives à un travail de tâche de numérisation poussée depuis Document Capture Pro |
| Network Push Scan Discovery | UDP | 2968 | Tous les ports | Recherche d'un ordinateur depuis le scanner |

| Nom du service | Type de protocole | Numéro du port local | Numéro du port à distance | Fonctions contrôlées |
|------------------------------------|-------------------|----------------------|---------------------------|--|
| Données FTP (distant) | TCP | Tous les ports | 20 | Client FTP (transmission de données numérisées) Cependant, cela permet seulement de contrôler un serveur FTP qui utilise le numéro de port à distance 20. |
| Contrôle FTP (distant) | TCP | Tous les ports | 21 | Client FTP (contrôler les données de numérisation transmises) |
| CIFS (distant) | TCP | Tous les ports | 445 | Client CIFS (transmission des données numérisées vers un dossier) |
| NetBIOS Name Service (distant) | UDP | Tous les ports | 137 | Client CIFS (transmission des données numérisées vers un dossier) |
| NetBIOS Datagram Service (distant) | UDP | Tous les ports | 138 | |
| NetBIOS Session Service (distant) | TCP | Tous les ports | 139 | |
| HTTP (local) | TCP | 80 | Tous les ports | Serveur HTTP(S) (transmission de données de Web Config et WSD) |
| HTTPS (local) | TCP | 443 | Tous les ports | |
| HTTP (distant) | TCP | Tous les ports | 80 | Client HTTP(S) (mise à jour du firmware et du certificat racine) |
| HTTPS (distant) | TCP | Tous les ports | 443 | |

Exemples de configuration de IPsec/filtrage IP

Réception de paquets IPsec uniquement

Cet exemple concerne uniquement la configuration d'une police par défaut.

Politique par défaut :

- IPsec/filtrage IP: Activer
- Contrôle des accès: IPsec
- Méthode d'authentification: Clé pré-partagée
- Clé pré-partagée : saisir jusqu'à 127 caractères.

Politique de groupe : ne pas configurer.

Réception des données de numérisation et des paramètres de scanner

Cet exemple permet les communications de données de numérisation et la configuration du scanner depuis des services spécifiés.

Politique par défaut :

- IPsec/filtrage IP: Activer
- Contrôle des accès: Refuser l'accès

Politique de groupe :

- Activer cette politique de groupe : cocher la case.
- Contrôle des accès: Autoriser l'accès
- Adresse distante (hôte) : adresse IP d'un client
- Mode de sélection du port: Nom du service
- Nom du service : cocher la case de ENPC, SNMP, HTTP (local), HTTPS (local) et Network Scan.

Recevoir un accès depuis une adresse IP spécifique uniquement

Cet exemple permet à une adresse IP spécifiée d'accéder au scanner.

Politique par défaut :

- IPsec/filtrage IP: Activer
- Contrôle des accès: Refuser l'accès

Politique de groupe :

- Activer cette politique de groupe : cocher la case.
- Contrôle des accès: Autoriser l'accès
- Adresse distante (hôte) : adresse IP d'un client d'un administrateur

Remarque:

Indépendamment de la configuration de la politique, le client sera en mesure d'accéder au scanner et de le configurer.

Configuration d'un certificat pour IPsec/filtrage IP

Configurer le certificat client pour IPsec/filtrage IP. Lorsque vous le définissez, vous pouvez utiliser le certificat en tant que méthode d'authentification pour IPsec/filtrage IP. Si vous souhaitez configurer l'autorité de certification, rendez-vous sur **Certificat CA**.

1. Accédez à Web Config puis sélectionnez l'onglet **Sécurité réseau > IPsec/filtrage IP > Certificat client**.
2. Importez le certificat dans **Certificat client**.

Si vous avez déjà importé un certificat publié par une Autorité de Certification, vous pouvez copier le certificat et l'utiliser dans IPsec/filtrage IP. Pour effectuer une copie, sélectionnez le certificat dans **Copier de**, puis cliquez sur **Copie**.

Informations connexes

- ➔ « Comment exécuter Web Config dans un navigateur Web » à la page 39
- ➔ « Configuration d'un Certificat signé CA » à la page 97
- ➔ « Configuration d'un Certificat CA » à la page 101

Connexion du scanner à un réseau IEEE802.1X

Configuration d'un réseau IEEE 802.1X

Lorsque vous configurez l'IEEE 802.1X sur le scanner, vous pouvez l'utiliser sur le réseau connecté à un serveur RADIUS, un commutateur LAN disposant d'une fonction d'authentification, ou un point d'accès.

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité réseau > IEEE802.1X > De base**.

2. Saisissez une valeur pour chaque élément.

Si vous voulez utiliser le scanner sur un réseau Wi-Fi, cliquez sur **Configuration du Wi-Fi** et sélectionnez ou saisissez un SSID.

Remarque:

Vous pouvez partager les paramètres entre Ethernet et Wi-Fi.

3. Cliquez sur **Suivant**.

Un message de confirmation s'affiche.

4. Cliquez sur **OK**.

Le scanner est mis à jour.

Informations connexes

➔ [« Comment exécuter Web Config dans un navigateur Web » à la page 39](#)

Éléments de paramétrage du réseau IEEE 802.1X

| Éléments | Paramètres et explication | |
|-------------------------|---|---|
| IEEE802.1X (LAN câblé) | Vous pouvez activer ou désactiver les paramètres de la page (IEEE802.1X > De base) pour IEEE802.1X (LAN filaire). | |
| IEEE802.1X (Wi-Fi) | L'état de connexion IEEE802.1X (Wi-Fi) s'affiche. | |
| Méthode de connexion | Le mode de connexion du réseau sélectionné s'affiche. | |
| Type EAP | Sélectionnez une option pour le mode d'authentification entre le scanner et le serveur RADIUS. | |
| | EAP-TLS | Vous devez obtenir et importer un certificat signé par une autorité de certification. |
| | PEAP-TLS | |
| | PEAP/MSCHAPv2 | Vous devez configurer un mot de passe. |
| EAP-TTLS | | |
| Identifiant utilisateur | Configurez un identifiant à utiliser pour l'authentification du serveur RADIUS. Saisissez de 0 à 128 caractères ASCII sur 1 octet (0x20 à 0x7E). | |

| Éléments | Paramètres et explication | |
|--|--|------------------------|
| Mot de passe | Configurez un mot de passe pour l'authentification du scanner. Saisissez de 0 à 128 caractères ASCII sur 1 octet (0x20 à 0x7E). Si vous utilisez un serveur Windows en guise de serveur RADIUS, vous pouvez saisir jusqu'à 127 caractères. | |
| Confirmer le mot de passe | Saisissez le mot de passe que vous avez configuré pour le confirmer. | |
| Identifiant serveur | Vous pouvez configurer un identifiant pour l'authentification du serveur RADIUS indiqué. L'authentifiant détermine si un identifiant de serveur est inclus dans le champ subject/subjectAltName du certificat de serveur, envoyé ou non depuis un serveur RADIUS. Saisissez de 0 à 128 caractères ASCII sur 1 octet (0x20 à 0x7E). | |
| Validation certificat (Réseau local câblé) | Si vous souhaitez effectuer Validation certificat à l'aide de IEEE802.1X (LAN câblé) , sélectionnez Activer . Si vous sélectionnez Activer, consultez les informations liées et importez le Certificat CA . Veuillez remarquer que Validation certificat est toujours activé dans IEEE802.1X (Wi-Fi). Assurez-vous d'importer le Certificat CA. | |
| Nom anonyme | Si vous sélectionnez l'option PEAP-TLS ou PEAP/MSCHAPv2 pour Type EAP , vous pouvez utiliser un nom anonyme au lieu d'un identifiant utilisateur pour la phase 1 d'une authentification PEAP. Saisissez de 0 à 128 caractères ASCII sur 1 octet (0x20 à 0x7E). | |
| Force du cryptage | Vous pouvez sélectionner une des valeurs suivantes. | |
| | Haut | AES256/3DES |
| | Moyen | AES256/3DES/AES128/RC4 |

Informations connexes

➔ « Configuration d'un Certificat CA » à la page 101

Configuration d'un certificat pour IEEE 802.1X

Configurer le certificat du client pour IEEE802.1X. Lorsque vous le définissez, vous pouvez utiliser **EAP-TLS** et **PEAP-TLS** en tant que méthode d'authentification pour IEEE 802.1X. Si vous souhaitez configurer le certificat d'autorité de certification, rendez-vous sur **Certificat CA**.

1. Accédez à Web Config puis sélectionnez l'onglet **Sécurité réseau** > **IEEE802.1X** > **Certificat client**.
2. Saisissez un certificat dans le **Certificat client**.

Si vous avez déjà importé un certificat publié par une Autorité de Certification, vous pouvez copier le certificat et l'utiliser dans IEEE802.1X. Pour effectuer une copie, sélectionnez le certificat dans **Copier de**, puis cliquez sur **Copie**.

Informations connexes

➔ « Comment exécuter Web Config dans un navigateur Web » à la page 39

Résolution des problèmes pour la sécurité avancée

Restauration des paramètres de sécurité

Lorsque vous mettez en place un environnement hautement sécurisé tel que le filtrage IPsec/IP, il est possible que vous ne puissiez pas communiquer avec les périphériques en raison de paramètres incorrects ou d'un problème au niveau du périphérique ou du serveur. Dans ce cas, rétablissez les paramètres de sécurité pour redéfinir les paramètres du périphérique ou autoriser une utilisation temporaire.

Désactivation de la fonction de sécurité à l'aide de Web Config

Vous pouvez désactiver IPsec/filtrage IP à l'aide de Web Config.

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité réseau > IPsec/filtrage IP > De base**.
2. Désactivez le **IPsec/filtrage IP**.

Problèmes lors de l'utilisation des fonctionnalités de sécurité réseau

Oubli de clé prépartagée

Reconfigurez une clé prépartagée.

Pour modifier la clé, accédez à Web Config et sélectionnez l'onglet **Sécurité réseau > IPsec/filtrage IP > De base > Politique par défaut** ou **Politique de groupe**.

Lorsque vous modifiez la clé pré-partagée, configurez cette dernière pour les ordinateurs.

Informations connexes

- ➔ « [Comment exécuter Web Config dans un navigateur Web](#) » à la page 39
- ➔ « [Communication chiffrée par filtrage IPsec/IP](#) » à la page 103

Communication avec le protocole IPsec impossible

Spécifiez l'algorithme que le scanner ou l'ordinateur ne prend pas en charge.

Le scanner prend en charge les algorithmes suivants. Vérifiez les paramètres de l'ordinateur.

| Modes de sécurité | Algorithmes |
|-----------------------------------|---|
| Algorithme de chiffrement IKE | AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES |
| Algorithme d'authentification IKE | SHA-1, SHA-256, SHA-384, SHA-512, MD5 |

| Modes de sécurité | Algorithmes |
|-----------------------------------|---|
| Algorithme d'échange de clé IKE | DH Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30* |
| Algorithme de chiffrement ESP | AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES |
| Algorithme d'authentification ESP | SHA-1, SHA-256, SHA-384, SHA-512, MD5 |
| Algorithme d'authentification AH | SHA-1, SHA-256, SHA-384, SHA-512, MD5 |

* disponible pour IKEv2 uniquement

Informations connexes

➔ [« Communication chiffrée par filtrage IPsec/IP » à la page 103](#)

Communication soudainement impossible

L'adresse IP du scanner a été modifiée ou ne peut être utilisée.

Lorsque l'adresse IP enregistrée à l'adresse locale de Politique de groupe a été modifiée ou ne peut pas être utilisée, la communication IPsec ne peut être réalisée. Désactivez le protocole IPsec à l'aide du panneau de commande du scanner.

Si le DHCP n'est pas à jour, redémarre, ou si l'adresse IPv6 n'est pas à jour ou impossible à obtenir, il est possible que l'adresse IP enregistrée du scanner dans l'onglet Web Config (**Sécurité réseau > IPsec/filtrage IP > De base > Politique de groupe > Adresse locale (scanner)**) soit introuvable.

Utilisez une adresse IP statique.

L'adresse IP de l'ordinateur a été modifiée ou ne peut être utilisée.

Lorsque l'adresse IP enregistrée à l'adresse distante de Politique de groupe a été modifiée ou ne peut pas être utilisée, la communication IPsec ne peut être réalisée.

Désactivez le protocole IPsec à l'aide du panneau de commande du scanner.

Si le DHCP n'est pas à jour, redémarre, ou si l'adresse IPv6 n'est pas à jour ou impossible à obtenir, il est possible que l'adresse IP enregistrée du scanner dans l'onglet Web Config (**Sécurité réseau > IPsec/filtrage IP > De base > Politique de groupe > Adresse distante (hôte)**) soit introuvable.

Utilisez une adresse IP statique.

Informations connexes

➔ [« Comment exécuter Web Config dans un navigateur Web » à la page 39](#)

➔ [« Communication chiffrée par filtrage IPsec/IP » à la page 103](#)

Impossible de se connecter après la configuration du filtrage IPsec/IP

Les paramètres d'IPsec/IP Filtering sont incorrects.

Désactivez le filtrage IPsec/IP depuis le panneau de commande du scanner. Connectez le scanner et l'ordinateur et effectuez à nouveau les réglages pour le filtrage IPsec/IP.

Informations connexes

➔ « [Communication chiffrée par filtrage IPsec/IP](#) » à la page 103

Impossible d'accéder à l'appareil après avoir configuré IEEE 802.1X

Les paramètres de IEEE 802.1X sont incorrects.

Désactivez IEEE 802.1X et le Wi-Fi à partir du panneau de commande du scanner. Connectez le scanner et l'ordinateur, puis configurez à nouveau IEEE 802.1X.

Informations connexes

➔ « [Configuration d'un réseau IEEE 802.1X](#) » à la page 115

Problèmes lors de l'utilisation d'un certificat numérique

Impossible d'importer un Certificat signé CA

Le Certificat signé CA et les informations sur le CSR ne correspondent pas.

Si les informations du Certificat signé CA et de la demande de signature du certificat ne sont pas les mêmes, le certificat ne peut être importé. Vérifiez les éléments suivants :

- Importez-vous le certificat sur un périphérique ne disposant pas des mêmes informations ?
Vérifiez les informations de la demande de signature de certificat et importez le certificat sur un périphérique disposant des mêmes informations.
- Avez-vous écrasé la demande de signature de certificat enregistrée sur le scanner après avoir envoyé la demande à l'autorité de certification ?
Obtenez un nouveau certificat signé par l'autorité de certification à l'aide de la demande de signature de certificat.

La taille du Certificat signé CA est supérieure à 5 Ko.

Vous ne pouvez pas importer un Certificat signé CA dont la taille est supérieure à 5 Ko.

Le mot de passe d'importation du certificat est incorrect.

Saisissez le mot de passe correct. Vous ne pouvez pas importer le certificat en cas d'oubli du mot de passe. Obtenez à nouveau le Certificat signé CA.

Informations connexes

➔ « [Importation d'un certificat signé par une autorité de certification](#) » à la page 98

Mise à jour d'un certificat à signature automatique impossible

Le Nom commun n'a pas été saisi.

Le paramètre **Nom commun** doit être défini.

Les caractères non pris en charge ont été saisis dans Nom commun.

Saisissez entre 1 et 128 caractères ASCII (0x20–0x7E) au format IPv4, IPv6, nom d'hôte ou FQDN.

Une virgule ou un espace est inclut dans le nom commun.

Si la valeur inclut une virgule, le paramètre **Nom commun** est divisé à cet emplacement. Si un espace a été ajouté avant ou après la virgule, une erreur survient.

Informations connexes

➔ « [Mise à jour d'un certificat à signature automatique](#) » à la page 100

Création d'une demande de signature de certificat impossible

Le Nom commun n'a pas été saisi.

Le paramètre **Nom commun** doit être défini.

Les caractères non pris en charge ont été saisis Nom commun, Organisation, Unité organisationnelle, Localité et État / Province.

Saisissez des caractères ASCII (0x20–0x7E) au format IPv4, IPv6, nom d'hôte ou FQDN.

Une virgule ou un espace est inclut dans le paramètre Nom commun.

Si la valeur inclut une virgule, le paramètre **Nom commun** est divisé à cet emplacement. Si un espace a été ajouté avant ou après la virgule, une erreur survient.

Informations connexes

➔ « [Obtention d'un certificat signé par une autorité de certification](#) » à la page 97

Un avertissement relatif à un certificat numérique s'affiche

| Messages | Cause/procédure à suivre |
|----------------------------------|--|
| Entrez un certificat de serveur. | Cause : Vous n'avez sélectionné aucun fichier à importer. Procédure à suivre : Sélectionnez un fichier et cliquez sur Importer . |

| Messages | Cause/procédure à suivre |
|----------------------------------|--|
| Certificat CA 1 n'est pas entré. | <p>Cause : Le certificat de l'autorité de certification 1 n'est pas saisi, seul le certificat de l'autorité de certification 2 est saisi.</p> <p>Procédure à suivre : Commencez par importer le certificat de l'autorité de certification 1.</p> |
| Valeur invalide ci-dessous. | <p>Cause : Le chemin d'accès au fichier et/ou le mot de passe incluent des caractères non pris en charge.</p> <p>Procédure à suivre : Vérifiez que les caractères sont correctement saisis pour l'élément.</p> |
| Date et heure non valides. | <p>Cause : La date et l'heure du scanner n'ont pas été définies.</p> <p>Procédure à suivre : Définissez la date et l'heure à l'aide du logiciel Web Config ou EpsonNet Config.</p> |
| MdPasse non valide. | <p>Cause : Le mot de passe défini pour le certificat de l'autorité de certification et le mot de passe saisi ne correspondent pas.</p> <p>Procédure à suivre : Saisissez le mot de passe correct.</p> |
| Fichier non valide. | <p>Cause : Le fichier de certificat que vous importez n'est pas au format X509.</p> <p>Procédure à suivre : Veillez à sélectionner le certificat correct, envoyé par une autorité de certification digne de confiance.</p> |
| | <p>Cause : Le fichier importé est trop volumineux. La taille du fichier ne doit pas dépasser 5 Ko.</p> <p>Procédure à suivre : Si vous avez sélectionné le fichier correct, il est possible que le certificat soit corrompu ou contrefait.</p> |
| | <p>Cause : La chaîne incluse dans le certificat est incorrecte.</p> <p>Procédure à suivre : Pour plus d'informations au sujet du certificat, reportez-vous au site Web de l'autorité de certification.</p> |

| Messages | Cause/procédure à suivre |
|---|--|
| Impossible d'utiliser les certificats de serveur qui incluent plus de trois certificats CA. | <p>Cause :</p> <p>Le fichier de certificat au format PKCS#12 comprend plus de trois certificats d'autorités de certification.</p> <p>Procédure à suivre :</p> <p>Importez chaque certificat en convertissant le format PKCS#12 au format PEM ou importez un fichier de certificat au format PKCS#12 contenant au maximum deux certificats d'autorités de certification.</p> |
| Le certificat a expiré. Vérifiez que le certificat est valide ou vérifiez les date et heure sur le produit. | <p>Cause :</p> <p>Le certificat n'est plus à jour.</p> <p>Procédure à suivre :</p> <ul style="list-style-type: none"> <input type="checkbox"/> Si le certificat n'est plus à jour, vous devez obtenir et importer un nouveau certificat. <input type="checkbox"/> Si le certificat est à jour, vérifiez que la date et l'heure du scanner sont correctement réglées. |
| La clé privée est nécessaire. | <p>Cause :</p> <p>Aucune clé privée n'est associée au certificat.</p> <p>Procédure à suivre :</p> <ul style="list-style-type: none"> <input type="checkbox"/> Sélectionnez le fichier de la clé privée si le certificat est au format PEM/DER et que vous l'avez obtenu à partir d'une demande de signature de certificat à l'aide d'un ordinateur. <input type="checkbox"/> Créez un fichier contenant la clé privée si le certificat est au format PKCS#12 et que vous l'avez obtenu à partir d'une demande de signature de certificat à l'aide d'un ordinateur. |
| | <p>Cause :</p> <p>Vous avez réimporté le certificat PEM/DER obtenu à partir d'une demande de signature de certificat à l'aide du logiciel Web Config.</p> <p>Procédure à suivre :</p> <p>Si le certificat est au format PEM/DER et que vous l'avez obtenu à partir d'une demande de signature de certificat à l'aide du logiciel Web Config, vous ne pouvez l'importer qu'une fois.</p> |
| Échec de la configuration. | <p>Cause :</p> <p>Impossible de terminer la configuration : échec de la communication entre le scanner et l'ordinateur ou lecture du fichier impossible en raison de certaines erreurs.</p> <p>Procédure à suivre :</p> <p>Une fois le fichier sélectionné et la communication vérifiés, importez de nouveau le fichier.</p> |

Informations connexes

➔ [« À propos de la certification numérique » à la page 96](#)

Suppression accidentelle d'un certificat signé par une autorité de certification

Il n'existe aucun fichier de sauvegarde pour le certificat signé par une autorité de certification.

Si vous disposez d'un fichier de sauvegarde, importez de nouveau le certificat.

Si vous obtenez un certificat à l'aide d'une demande de signature de certificat créée à partir du logiciel Web Config, vous ne pouvez importer de nouveau un certificat supprimé. Créez une demande de signature de certificat et obtenez un nouveau certificat.

Informations connexes

- ➔ [« Importation d'un certificat signé par une autorité de certification » à la page 98](#)
- ➔ [« Suppression d'un certificat signé par une autorité de certification » à la page 99](#)

Utilisation d'Epson Open Platform

| | |
|---|-----|
| Présentation d'Epson Open Platform. | 125 |
| Configuration de Epson Open Platform. | 125 |
| Validation d'Epson Open Platform. | 125 |

Présentation d'Epson Open Platform

Epson Open Platform est une plateforme qui vous permet d'utiliser les systèmes d'authentification avec ce scanner.

Elle peut être utilisée avec Epson Print Admin (Epson Authentication System) ou un système d'authentification tiers. Vous pouvez obtenir des journaux par périphérique et utilisateur, configurer les périphériques que les utilisateurs et les groupes peuvent utiliser, définir des limites pour les fonctions, etc.

Si vous connectez un périphérique d'authentification, vous pouvez également effectuer l'authentification d'utilisateur à l'aide de la carte d'identité.

Configuration de Epson Open Platform

Activez Epson Open Platform afin de pouvoir utiliser le périphérique à partir du système d'authentification.

1. Obtenir une clé produit depuis le site Web dédié.

Consultez le manuel Epson Open Platform pour plus d'informations sur la manière d'obtenir la clé du produit.

2. Rendez-vous dans Web Config, puis sélectionnez l'onglet **Epson Open Platform > Clé produit ou Clé de licence**.

3. Vérifiez et définissez chaque élément.

- Numéro de série

Le numéro de série du périphérique s'affiche.

- Version Epson Open Platform

Sélectionnez la version d'Epson Open Platform. La version correspondante varie en fonction du système d'authentification.

- Clé produit ou Clé de licence

Saisissez la clé de produit que vous avez obtenue.

4. Cliquez sur **Suivant**.

L'écran de confirmation du paramètre s'affiche.

5. Cliquez sur **OK**.

Les paramètres sont appliqués au scanner.

Remarque:

Vous ne pouvez pas utiliser Epson Print Admin Serverless lorsque le système est synchronisé avec Epson Open Platform.

Validation d'Epson Open Platform

Vous pouvez vérifier la validité de la Epson Open Platform en suivant l'une des méthodes ci-dessous.

- Web Config

Une clé de produit a été saisie dans l'onglet **Epson Open Platform > Clé produit ou Clé de licence > Clé produit ou Clé de licence**, et l'onglet **Epson Open Platform > Système d'authentification** s'affiche à gauche dans l'arborescence de menu.

- Panneau de commande du scanner

Vérifiez que la clé produit s'affiche dans **Param.** > **Informations sur l'appareil** > **Informations Epson Open Platform.**

Montage d'un dispositif d'authentification

| | |
|--|-----|
| Connexion du périphérique d'authentification. | 128 |
| Vérification de l'utilisation du périphérique d'authentification. | 128 |
| Vérification de la reconnaissance de la carte d'authentification. | 128 |
| Résolution des problèmes rencontrés avec le dispositif d'authentification. | 129 |

Connexion du périphérique d'authentification

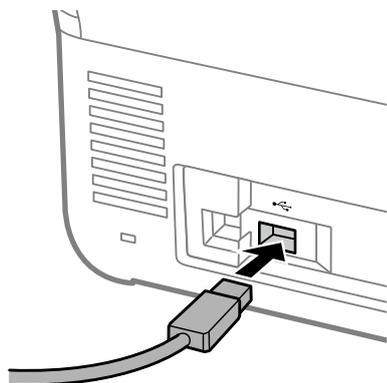
Remarque:

Vous pouvez utiliser un dispositif d'authentification avec un système d'authentification.

! **Important:**

Lorsque vous connectez le périphérique d'authentification à plusieurs scanners, utilisez un produit comportant le même numéro de modèle.

Connectez le câble USB du lecteur de carte au port USB d'interface externe sur le scanner.



Vérification de l'utilisation du périphérique d'authentification

Vous pouvez vérifier l'état de la connexion et la reconnaissance de la carte d'authentification pour le périphérique d'authentification depuis le panneau de commande du scanner.

Des informations sont affichées si vous sélectionnez **Param.** > **Informations sur l'appareil** > **État du dispositif d'authentification**.

Vérification de la reconnaissance de la carte d'authentification

Vous pouvez vérifier que la carte d'authentification est bien reconnue à l'aide de Web Config.

1. Rendez-vous dans Web Config, puis sélectionnez l'onglet **Gestion des périphériques** > **Lecteur de carte**.
2. Maintenez la carte d'authentification sur le lecteur de carte d'authentification.
3. Cliquez sur **Contrôler**.
Le résultat s'affiche.

Résolution des problèmes rencontrés avec le dispositif d'authentification

Impossible de lire la carte d'authentification

Vérifiez les éléments suivants.

- Vérifiez que le périphérique d'authentification est bien connecté au scanner.
Connectez le périphérique d'authentification au port USB d'interface externe à l'arrière du scanner.
- Vérifiez que le périphérique d'authentification et la carte d'authentification sont certifiés.
Contactez votre revendeur pour plus d'informations sur les périphériques et cartes d'authentification pris en charge.

Entretien

| | |
|---|-----|
| Nettoyage de l'extérieur du scanner. | 131 |
| Nettoyage de l'intérieur du scanner. | 131 |
| Remplacement du jeu de rouleaux. | 135 |
| Réinitialiser le nombre de numérisations après avoir remplacé les rouleaux. | 141 |
| Économie d'énergie. | 142 |
| Transport du scanner. | 142 |
| Sauvegarde des paramètres. | 143 |
| Rest param défaut. | 144 |
| Mise à jour des applications et du micrologiciel. | 145 |

Nettoyage de l'extérieur du scanner

Essuyez toute tache présente sur l'extérieur du boîtier avec un chiffon sec ou humecté d'un mélange de détergent doux et d'eau.



Important:

- N'utilisez jamais d'alcool, de diluant ou de solvant corrosif pour nettoyer le scanner. Ceci pourrait entraîner une déformation ou une décoloration.
- Assurez-vous que de l'eau ne pénètre pas dans le produit. Ceci pourrait entraîner un dysfonctionnement.
- N'ouvrez jamais le boîtier du scanner.

1. Appuyez sur la touche  pour éteindre le scanner.
2. Débranchez l'adaptateur secteur du scanner.
3. Nettoyez l'extérieur du boîtier avec un chiffon humecté d'un mélange de détergent doux et d'eau.

Remarque:

Essuyez l'écran tactile à l'aide d'un chiffon doux et sec.

Nettoyage de l'intérieur du scanner

Avec le temps, la poussière du papier et de la pièce se dépose sur le rouleau et sur la vitre à l'intérieur du scanner, ce qui peut provoquer des problèmes d'entraînement du papier ou de qualité de l'image numérisée. Nettoyez l'intérieur du scanner toutes les 5,000 numérisations.

Le nombre de numérisations effectuées est indiqué sur le panneau de commande ou dans Epson Scan 2 Utility.

Si une surface a été tachée par substance difficile à enlever, utilisez un kit de nettoyage Epson authentique pour retirer les taches. Déposez une petite quantité de produit nettoyant sur un chiffon.

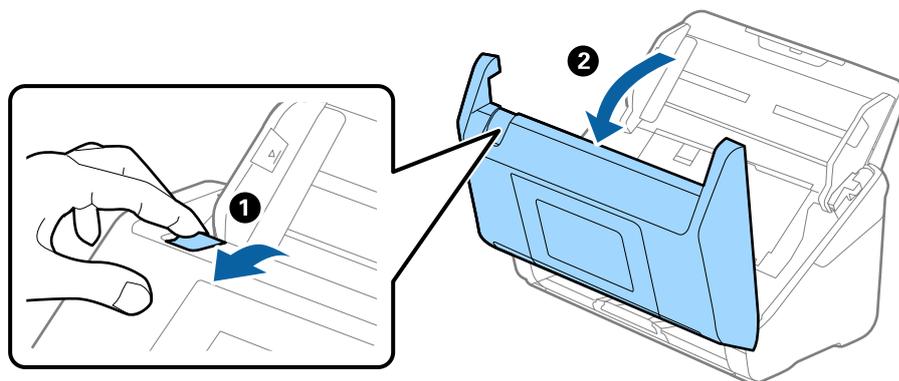


Important:

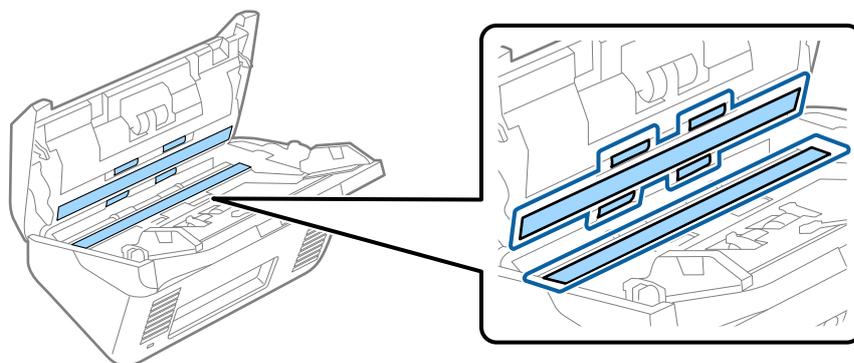
- N'utilisez jamais d'alcool, de diluant ou de solvant corrosif pour nettoyer le scanner. Ceci pourrait entraîner une déformation ou une décoloration.
- Ne vaporisez jamais de liquide ou de lubrifiant sur le scanner. Tout dommage porté à l'équipement ou aux circuits pourrait provoquer un fonctionnement anormal.
- N'ouvrez jamais le boîtier du scanner.

1. Appuyez sur la touche  pour éteindre le scanner.
2. Débranchez l'adaptateur secteur du scanner.

3. Tirez le levier pour ouvrir le capot du scanner.



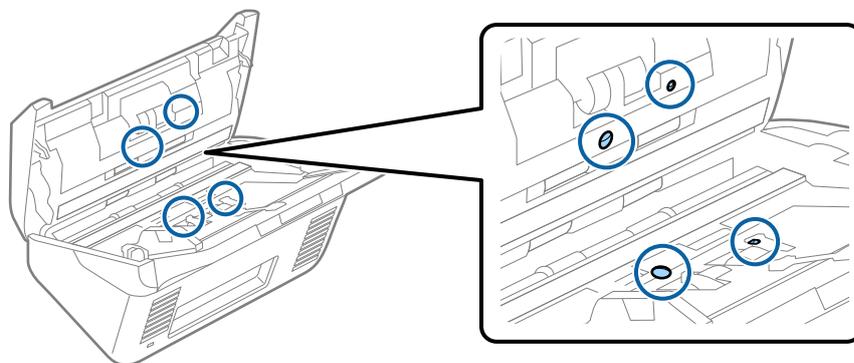
4. Essuyez toute tache présente sur le rouleau en plastique (4 emplacements) ou sur la vitre d'exposition de la face interne du capot du scanner. Nettoyez-le à l'aide d'un chiffon doux et non pelucheux imbibé d'un peu de nettoyant adapté ou d'eau.



! Important:

- N'appuyez pas trop sur la surface vitrée.
- N'utilisez pas de brosse ni un outil dur. Toute rayure du verre peut affecter la qualité de la numérisation.
- Ne pulvérisez pas de nettoyant directement sur la surface vitrée.

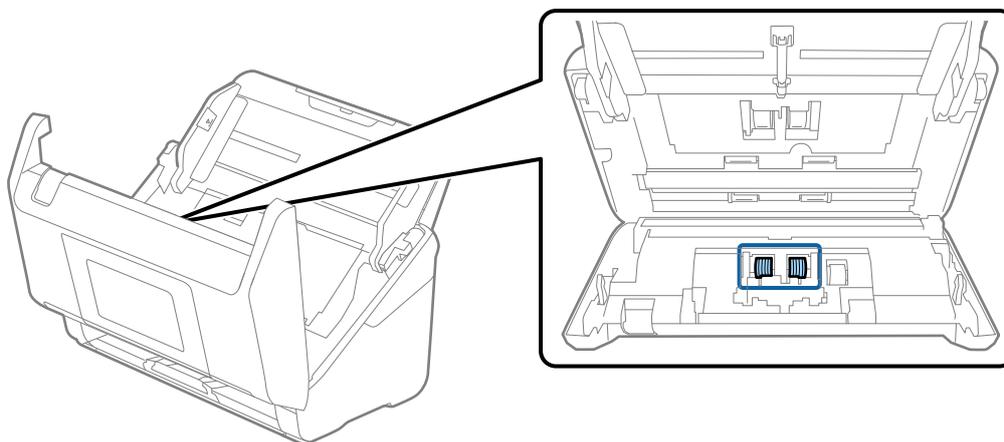
5. Essuyez toute tache présente sur les capteurs avec un coton-tige.



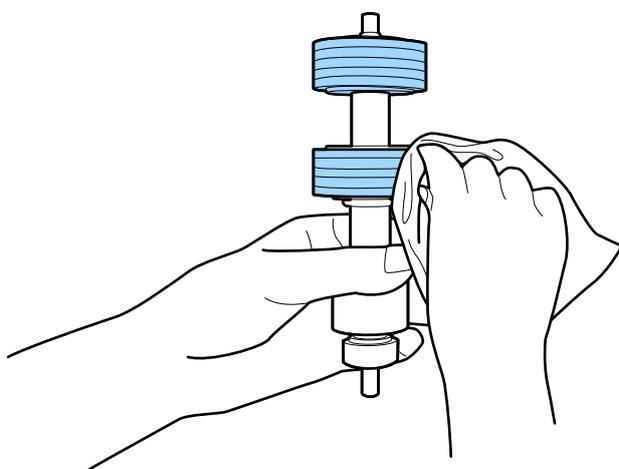
! *Important:*

N'utilisez pas de produit nettoyant sur un coton-tige.

- Ouvrez le capot du scanner et retirez le rouleau de séparation.
Pour plus d'informations, voir « Remplacement du jeu de rouleaux ».



- Nettoyez le rouleau de séparation. Nettoyez-le à l'aide d'un chiffon doux et non pelucheux imbibé d'un peu de nettoyant adapté ou d'eau.

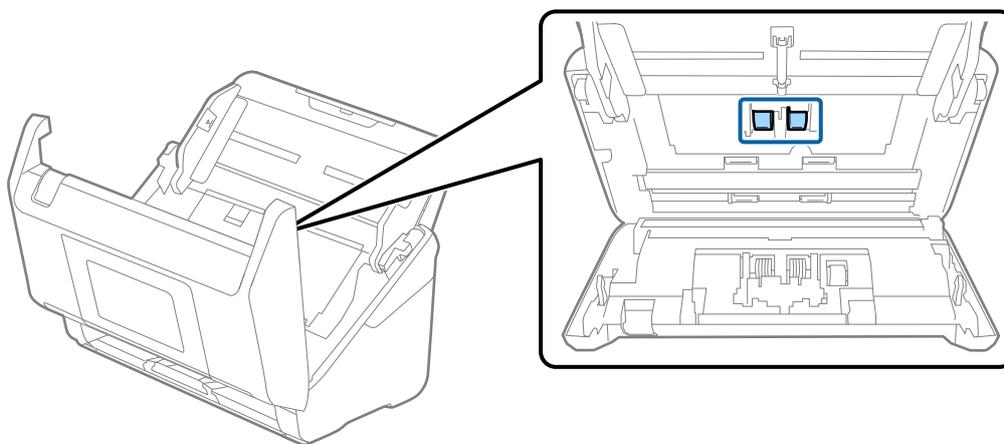


! *Important:*

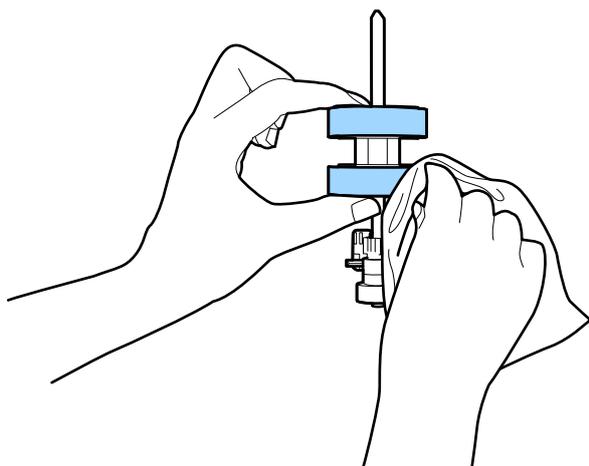
Veillez à n'utiliser qu'un kit de nettoyage Epson authentique ou un chiffon doux et humide pour nettoyer le rouleau. L'utilisation d'un chiffon sec peut endommager la surface du rouleau.

- Ouvrez le capot et retirez le rouleau d'entraînement.

Pour plus d'informations, voir « Remplacement du jeu de rouleaux ».



- Nettoyez le rouleau de saisie. Nettoyez-le à l'aide d'un chiffon doux et non pelucheux imbibé d'un peu de nettoyant adapté ou d'eau.

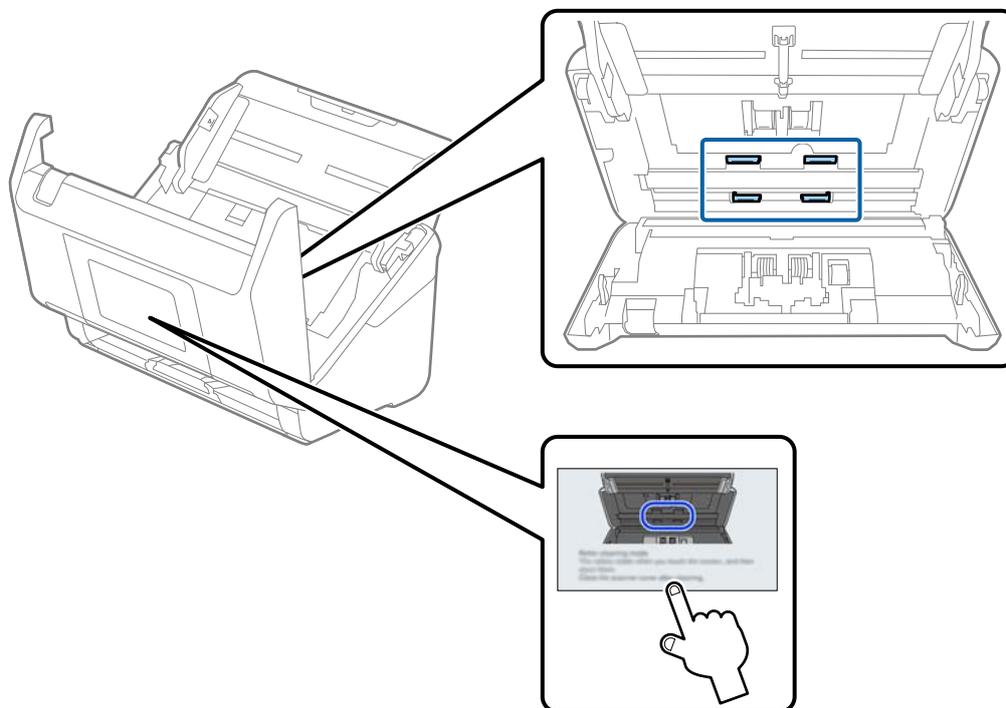


! *Important:*

Veillez à n'utiliser qu'un kit de nettoyage Epson authentique ou un chiffon doux et humide pour nettoyer le rouleau. L'utilisation d'un chiffon sec peut endommager la surface du rouleau.

- Fermez le capot du scanner.
- Branchez l'adaptateur secteur et mettez le scanner sous tension.
- Sélectionnez **Entretien du scanner** sur l'écran d'accueil.
- Sur l'écran **Entretien du scanner**, sélectionnez **Nettoyage des rouleaux**.
- Tirez le levier pour ouvrir le capot du scanner.
Le scanner entre en mode de nettoyage du rouleau.

15. Touchez n'importe quel endroit de l'écran LCD pour tourner lentement les rouleaux du fond. Essayez la surface des rouleaux à l'aide d'un kit de nettoyage Epson authentique ou un chiffon doux humidifié. Répétez l'opération jusqu'à ce que les rouleaux soient propres.



⚠ Attention:

Veillez à ce que vos mains ou vos cheveux ne se prennent pas dans le mécanisme lorsque vous actionnez le rouleau. Vous pourriez être blessé.

16. Fermez le capot du scanner.
Le scanner quitte le mode de nettoyage de rouleau.

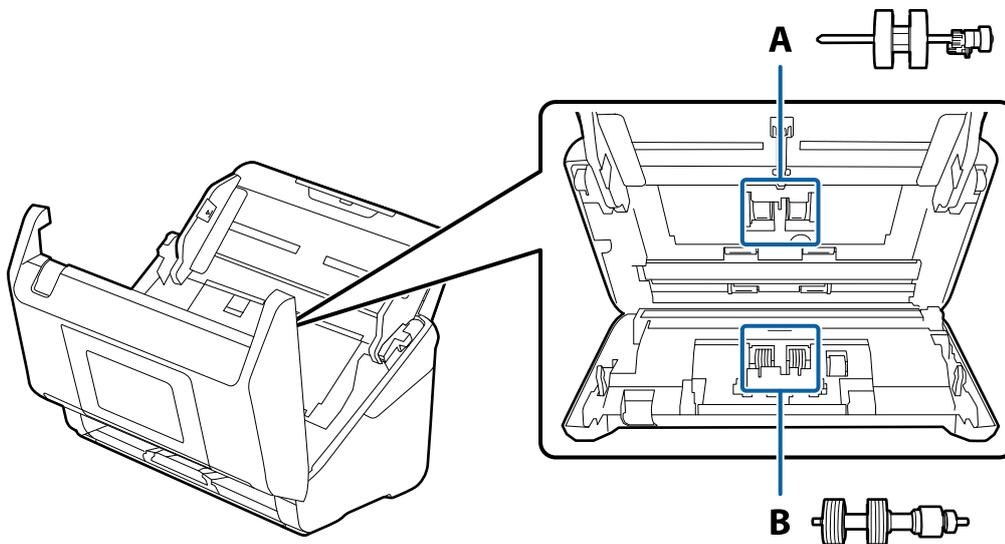
Informations connexes

➔ « Remplacement du jeu de rouleaux » à la page 135

Remplacement du jeu de rouleaux

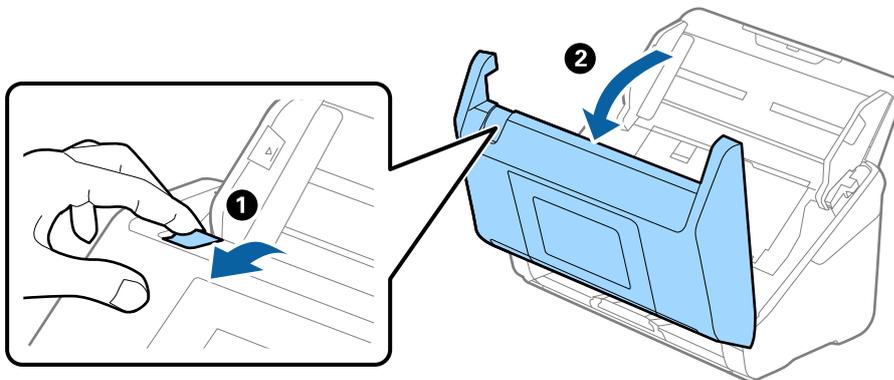
Le kit d'ensemble de rouleau (rouleau de saisie et rouleau de séparation) doit être remplacé lorsque le nombre de numérisations est supérieur au nombre prévu dans le Cycle de vie des rouleaux. Lorsqu'un message de

remplacement s'affiche sur le panneau de commande ou votre écran d'ordinateur, procédez comme suit pour le remplacement.

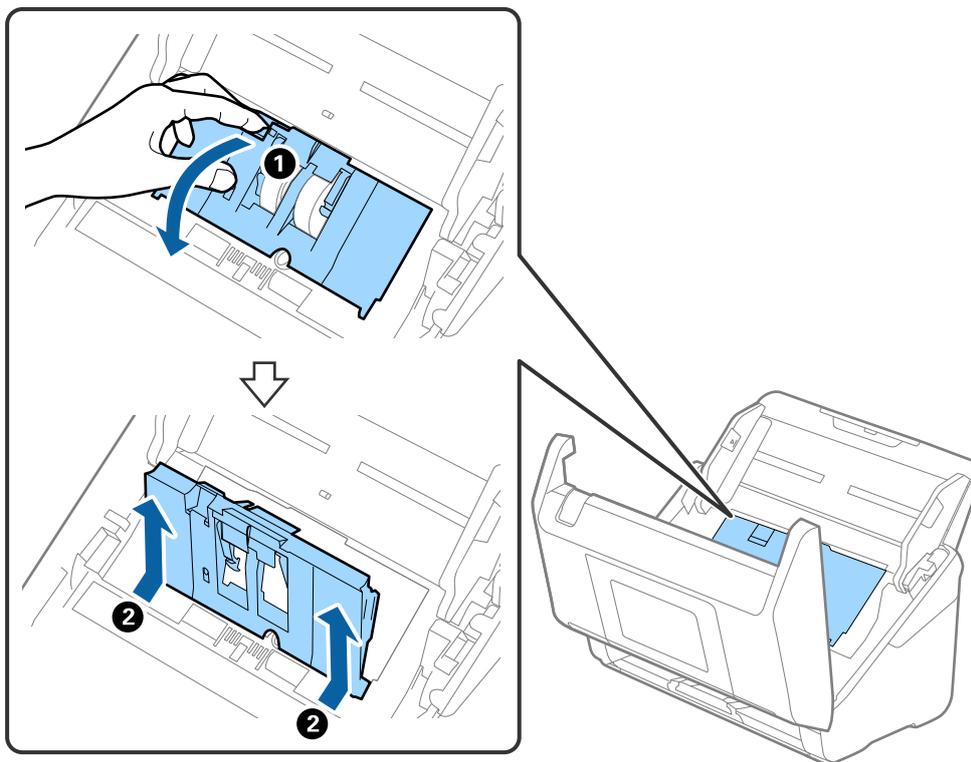


A : rouleau de saisie, B : rouleau de séparation

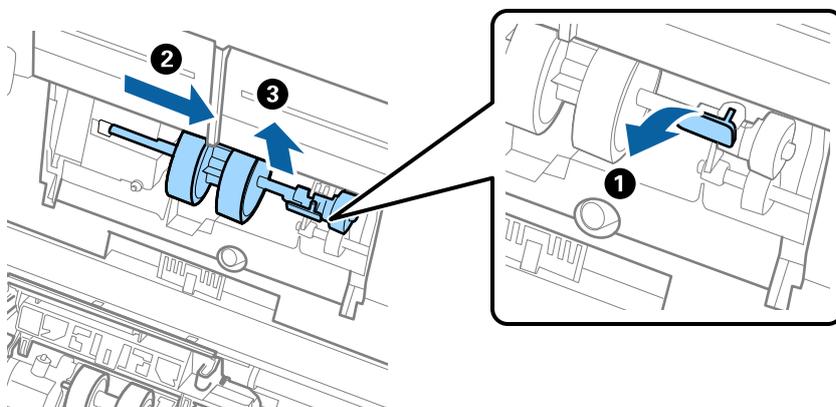
1. Appuyez sur la touche  pour éteindre le scanner.
2. Débranchez l'adaptateur secteur du scanner.
3. Tirez le levier et ouvrez le capot du scanner.



4. Ouvrez le capot du rouleau de saisie, faites-le coulisser et retirez-le.



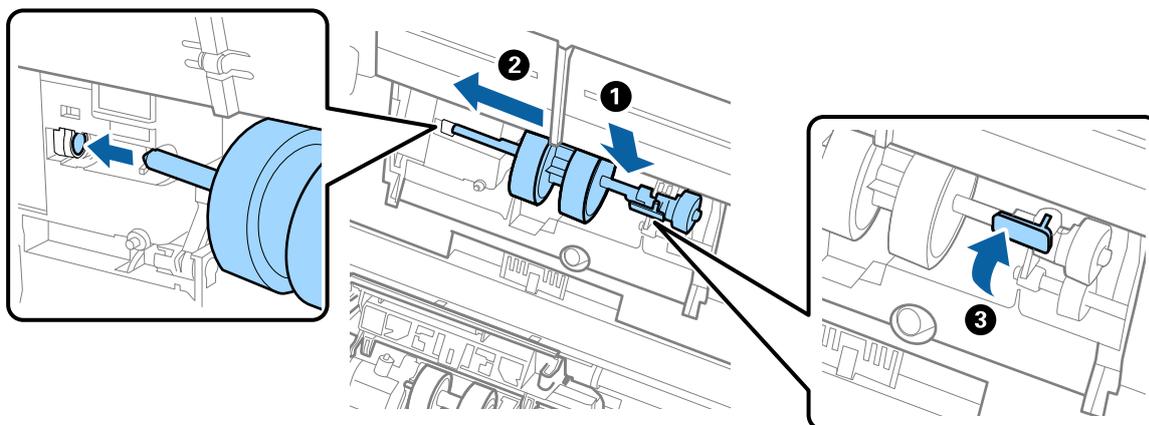
5. Abaissez la patte de l'axe du rouleau, puis faites coulisser et retirez les rouleaux d'entraînement.



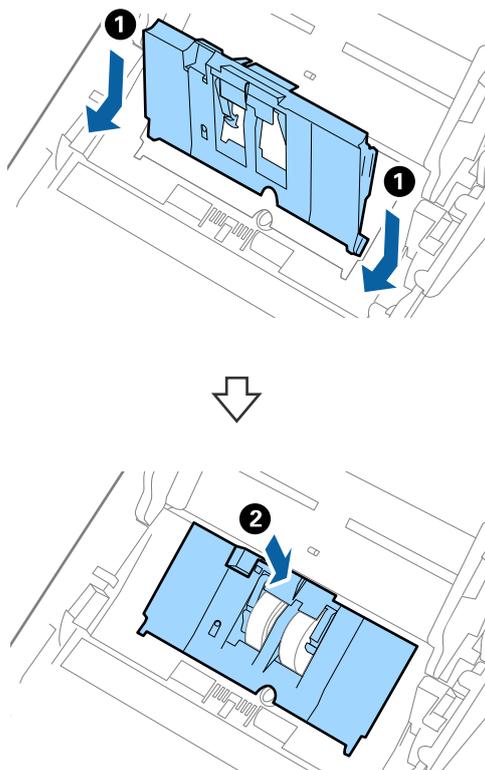
Important:

Ne forcez pas lorsque vous retirez le rouleau de saisie. Vous pourriez endommager l'intérieur du scanner.

6. Tout en maintenant la patte abaissée, insérez le nouveau rouleau de saisie en le faisant glisser vers la gauche et insérez-le dans l'orifice du scanner. Appuyez sur la patte pour le fixer.

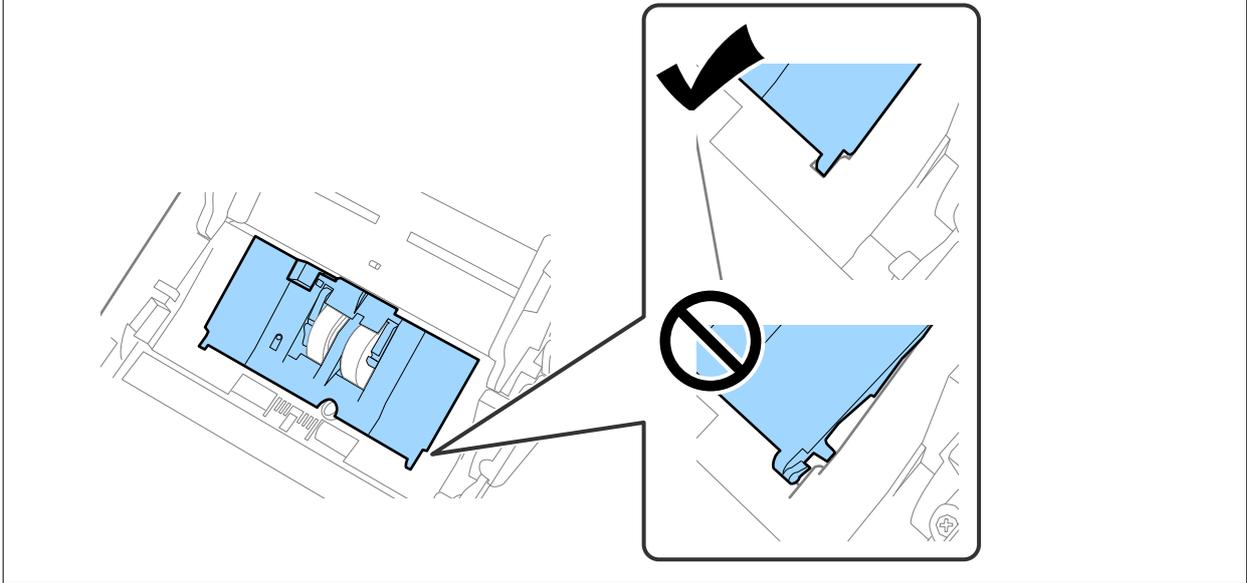


7. Placez le bord du capot du rouleau de saisie dans la rainure et faites-le coulisser. Enclenchez bien le capot.

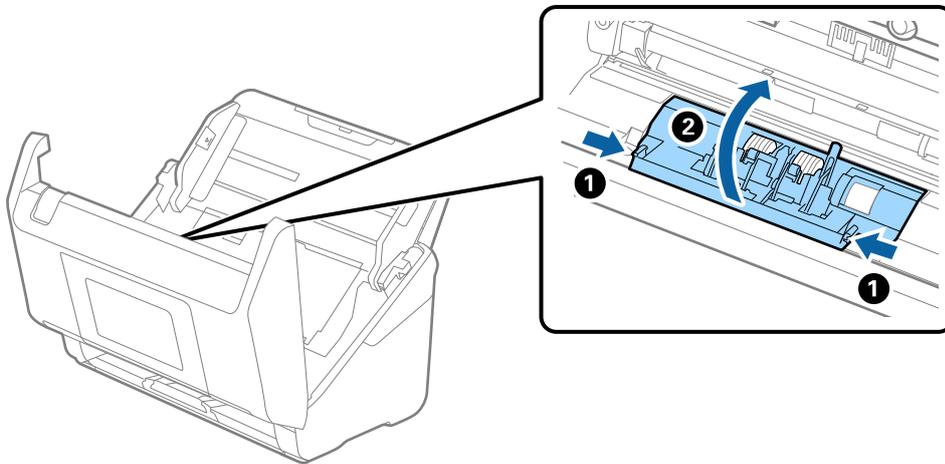


! Important:

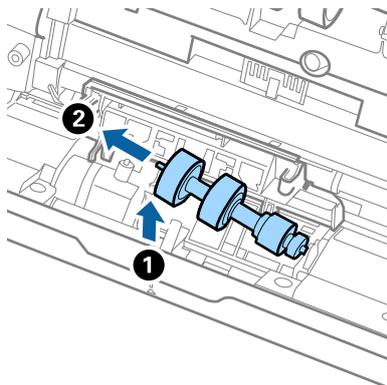
- ❑ Vérifiez que le capot de saisie est bien fermé.
- ❑ Si vous avez du mal à fermer le capot, assurez-vous que les rouleaux de prise sont correctement positionnés.
- ❑ N'installez pas le capot en position relevée.



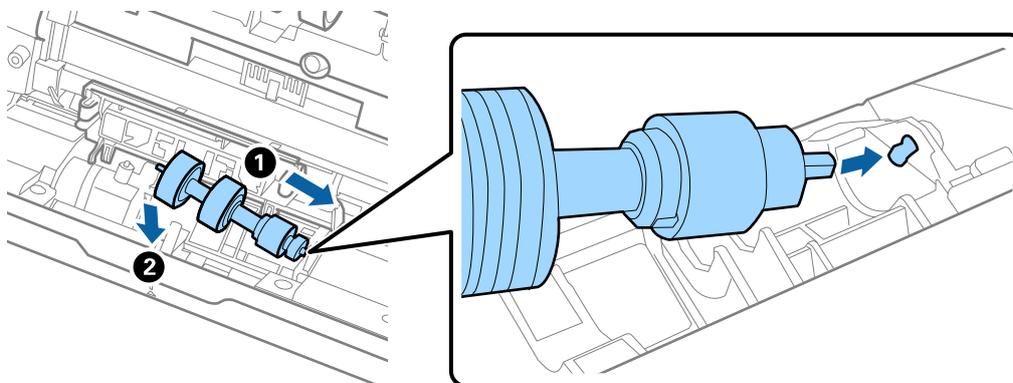
8. Pour ouvrir le capot, poussez les crochets situés aux deux extrémités du capot du rouleau de séparation.



9. Soulevez l'extrémité gauche du rouleau de séparation, puis faites coulisser et retirez les rouleaux de séparation.



10. Insérez le nouvel axe de rouleau de séparation dans l'orifice du côté droit et abaissez le rouleau.



11. Fermez le capot du rouleau de séparation.



Important:

Si le couvercle est difficile à fermer, assurez-vous que les rouleaux de séparation sont correctement installés.

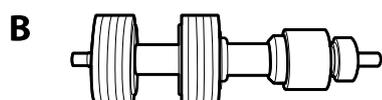
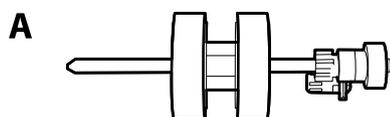
12. Fermez le capot du scanner.
13. Branchez l'adaptateur secteur et mettez le scanner sous tension.
14. Réinitialisez le nombre de numérisations sur le panneau de commande.

Remarque:

Jetez le rouleau de saisie et le rouleau de séparation en respectant les réglementations locales. Ne les démontez pas.

Codes de jeu de rouleaux

Les éléments (rouleau d'entraînement et rouleau de remplacement) doivent être remplacés lorsque le nombre de numérisations est supérieur au seuil de maintenance. Le nombre de numérisations effectuées est indiqué sur le panneau de commande ou dans Epson Scan 2 Utility.



A : rouleau de saisie, B : rouleau de séparation

| Nom de la pièce | Codes | Cycle de vie |
|-------------------|--|--------------|
| Jeu de rouleaux 2 | B12B819711 B12B819721 (Inde uniquement) | 200,000* |

* Ce nombre a été atteint suite aux numérisations successives avec les documents originaux de test Epson et sert de référence pour définir le cycle de remplacement. Le cycle de remplacement peut varier en fonction des types de papiers, selon que le papier génère une grande quantité de poussières ou que sa rugosité de surface raccourcit le cycle de vie.

Réinitialiser le nombre de numérisations après avoir remplacé les rouleaux

Après avoir remplacé le jeu de rouleaux, réinitialisez le nombre de numérisations depuis le panneau de commande ou à l'aide de Epson Scan 2 Utility.

Cette section explique comment effectuer cette réinitialisation depuis le panneau de commande.

1. Appuyez sur **Entretien du scanner** à l'écran d'accueil.
2. Appuyez sur **Remplacement du rouleau**.
3. Appuyez sur **Réinitialiser le nombre de numérisations**.
4. Sélectionnez **Nb de nums ap remplacement du rouleau**, puis appuyez sur **Oui**.

Remarque:

Pour réinitialiser à l'aide de Epson Scan 2 Utility, lancez Epson Scan 2 Utility, cliquez sur l'onglet **Compteur**, puis cliquez sur **Réinitialiser dans Kit de rouleaux d'entraînement des originaux**.

Informations connexes

➔ « Remplacement du jeu de rouleaux » à la page 135

Économie d'énergie

Vous pouvez économiser de l'électricité en utilisant le mode veille ou le mode d'extinction automatique lorsque le scanner est inactif. Vous pouvez définir le délai au bout duquel le scanner passe en mode veille et s'éteint automatiquement. Toute augmentation se répercutera sur la consommation d'énergie du produit. Prenez en compte l'environnement avant d'apporter une modification.

1. Sélectionnez **Param.** à l'écran d'accueil.
2. Sélectionnez **Param de base**.
3. Sélectionnez **Minut. veille** ou **Réglages d'arrêt**, puis définissez les paramètres.

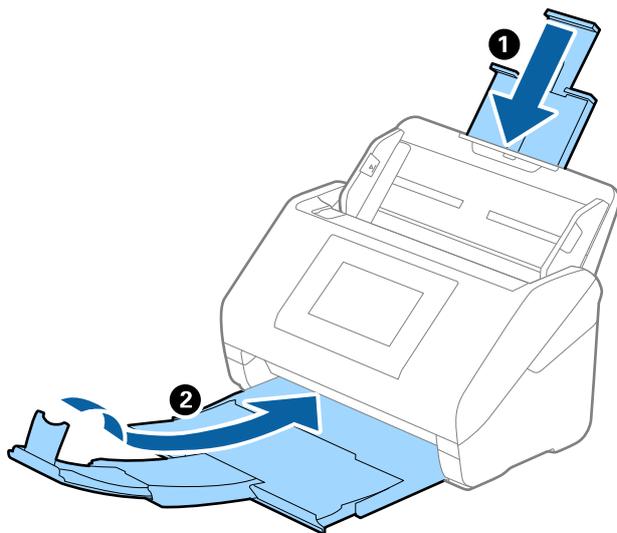
Remarque:

Les fonctions disponibles peuvent varier en fonction du lieu de l'achat.

Transport du scanner

Lorsque vous devez transporter votre scanner pour un déménagement ou une réparation, suivez les étapes ci-dessous pour l'emballer.

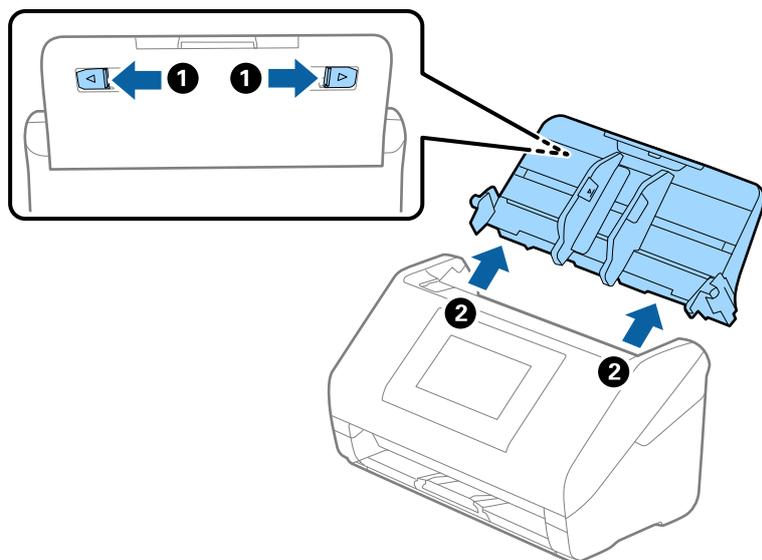
1. Appuyez sur la touche  pour éteindre le scanner.
2. Débranchez l'adaptateur secteur.
3. Retirez les câbles et les périphériques.
Retirez la Paper Alignment Plate en option ou fournie si elle est attachée.
4. Fermez l'extension du bac d'insertion et le bac de sortie.



Important:

Enclenchez bien le bac de sortie sinon il pourrait être endommagé pendant le transport.

5. Retirez le bac d'insertion.



6. Installez les matériaux d'emballage accompagnant le scanner, puis emballez le scanner dans son carton d'origine ou dans un carton de même type.

Sauvegarde des paramètres

Vous pouvez exporter l'ensemble des valeurs de paramètre de Web Config vers le fichier. Vous pouvez l'utiliser pour sauvegarder les contacts, définir des valeurs, remplacer le scanner, etc.

Le fichier exporté ne peut être modifié, car il est exporté en tant que fichier binaire.

Exporter les paramètres

Exportez le paramètre du scanner.

1. Accédez à Web Config, puis sélectionnez l'onglet **Gestion des périphériques > Exporter et importer valeur de paramètre > Exporter**.

2. Sélectionnez les paramètres que vous souhaitez exporter.

Sélectionnez les paramètres que vous souhaitez exporter. Si vous sélectionnez la catégorie parente, les sous-catégories sont également sélectionnées. Cependant, les sous-catégories pouvant causer des erreurs de duplication sur un même réseau (adresses IP et ainsi de suite) ne peuvent pas être sélectionnées.

3. Saisissez un mot de passe pour déchiffrer le fichier exporté.

Vous avez besoin du mot de passe pour importer le fichier. Laissez le champ vide si vous ne souhaitez pas chiffrer le fichier.

4. Cliquez sur **Exporter**.

 **Important:**

*Si vous voulez exporter les paramètres réseau du scanner, comme le nom du périphérique et l'adresse IPv6, sélectionnez **Activez pour sélectionner les paramètres individuels de l'appareil** et sélectionnez plus d'éléments. Utilisez uniquement les valeurs sélectionnées pour le scanner de remplacement.*

Informations connexes

➔ [« Comment exécuter Web Config dans un navigateur Web » à la page 39](#)

Importer les paramètres

Importez le fichier Web Config exporté vers le scanner.

 **Important:**

Lors de l'importation de valeurs qui incluent des informations individuelles telles que le nom d'un scanner ou une adresse IP, assurez-vous qu'une adresse IP similaire n'existe pas sur le même réseau.

1. Accédez à Web Config, puis sélectionnez l'onglet **Gestion des périphériques > Exporter et importer valeur de paramètre > Importer**.
2. Sélectionnez le fichier exporté, puis saisissez le mot de passe chiffré.
3. Cliquez sur **Suivant**.
4. Sélectionnez les paramètres que vous souhaitez importer, puis cliquez sur **Suivant**.
5. Cliquez sur **OK**.

Les paramètres sont appliqués au scanner.

Informations connexes

➔ [« Comment exécuter Web Config dans un navigateur Web » à la page 39](#)

Rest param défaut

Sur le panneau de commande, sélectionnez **Param. > Administration système > Rest param défaut**, puis sélectionnez les éléments que vous souhaitez restaurer sur leur valeur par défaut.

- Paramètres réseau : restaure la valeur initiale des paramètres liés au réseau.
- Tous sauf les Paramètres réseau : restaure la valeur initiale des autres paramètres, à l'exception des paramètres liés au réseau.
- Tous les paramètres : restaure tous les paramètres à leur valeur initiale au moment de l'achat.

 **Important:**

Si vous sélectionnez **Tous les paramètres** et l'exécutez, tous les paramètres enregistrés dans le scanner, dont les contacts, seront supprimés. Les paramètres supprimés ne peuvent pas être restaurés.

Remarque:

Vous pouvez également effectuer des réglages sur Web Config.

Onglet **Gestion des périphériques** > **Restaurer param. par défaut**

Mise à jour des applications et du micrologiciel

Vous pouvez régler certains problèmes et améliorer ou ajouter des fonctions en mettant à jour les applications et le micrologiciel. Assurez-vous que vous utilisez la dernière version des applications et du micrologiciel.

 **Important:**

N'éteignez pas l'ordinateur ou le scanner pendant la mise à jour.

Remarque:

Si le scanner ne peut pas se connecter à Internet, vous pouvez mettre à jour le micrologiciel depuis Web Config. Sélectionnez l'onglet **Gestion des périphériques** > **Mise à jour du micrologiciel**, vérifiez le message qui s'affiche, puis cliquez sur **Démarrer**.

1. Assurez-vous que le scanner et l'ordinateur sont raccordés et que l'ordinateur est connecté à Internet.
2. Lancez EPSON Software Updater et mettez à jour les applications ou le micrologiciel.

Remarque:

Les systèmes d'exploitation Windows Server ne sont pas pris en charge.

Windows 11

Cliquez sur le bouton Démarrer, puis sélectionnez **Toutes les applications** > **Epson Software** > **EPSON Software Updater**.

Windows 10

Cliquez sur le bouton Démarrer, puis sélectionnez **Epson Software** > **EPSON Software Updater**.

Windows 8.1/Windows 8

Saisissez le nom de l'application dans la vignette de recherche, puis sélectionnez l'icône qui s'affiche.

Windows 7

Cliquez sur le bouton Démarrer, puis sélectionnez **Tous les programmes** ou **Programmes** > **Epson Software** > **EPSON Software Updater**.

Mac OS

Sélectionnez **Finder** > **Aller** > **Applications** > **Epson Software** > **EPSON Software Updater**.

Remarque:

Si vous ne trouvez pas l'application que vous voulez mettre à jour dans la liste, vous ne pouvez pas procéder à sa mise à jour à l'aide d'EPSON Software Updater. Recherchez les dernières versions des applications sur votre site Web Epson local.

<http://www.epson.com>

Mise à jour du micrologiciel du scanner à l'aide du panneau de commande

Si le scanner peut être connecté à Internet, vous pouvez mettre à jour son micrologiciel à l'aide du panneau de commande. Vous pouvez également configurer le scanner de manière à ce qu'il vérifie régulièrement les mises à jour du micrologiciel et vous informe lorsque de telles mises à jour sont disponibles.

1. Sélectionnez **Param.** à l'écran d'accueil.
2. Sélectionnez **Administration système > Mise à jour firmware > Mise à jour.**

Remarque:

Sélectionnez **Notification > Activé** de manière à ce que le scanner vérifie régulièrement les mises à jour du micrologiciel disponibles.

3. Lisez le message affiché à l'écran et lancez la recherche des mises à jour disponibles.
4. Si un message vous indiquant qu'une mise à jour du micrologiciel est disponible s'affiche sur l'écran LCD, suivez les instructions affichées à l'écran pour lancer la mise à jour.



Important:

- ❑ *N'éteignez pas le scanner et ne le débranchez pas avant la fin de la mise à jour, faute de quoi le scanner risque de ne pas fonctionner correctement.*
- ❑ *Si la procédure de mise à jour du micrologiciel n'est pas terminée ou échoue, le scanner ne redémarrera pas normalement et le message Recovery Mode s'affichera sur l'écran LCD lors du prochain allumage du scanner. Vous devrez alors procéder de nouveau à la mise à jour du micrologiciel à l'aide d'un ordinateur. Branchez le scanner à l'ordinateur à l'aide d'un câble USB. Vous ne pouvez pas mettre à jour le micrologiciel via une connexion réseau tant que le message Recovery Mode s'affiche sur le scanner. Sur l'ordinateur, rendez-vous sur le site Web Epson dans votre langue, puis téléchargez le micrologiciel du scanner le plus récent. Reportez-vous aux instructions du site Web pour connaître les étapes suivantes.*

Mettre à jour le micrologiciel à l'aide de Web Config

Lorsque le scanner ne peut pas se connecter à Internet, vous pouvez mettre à jour le micrologiciel depuis Web Config.

1. Accédez à Web Config et sélectionnez l'onglet **Gestion des périphériques > Mise à jour du micrologiciel.**
2. Cliquez sur **Démarrer**, puis suivez les instructions qui s'affichent à l'écran.

La confirmation du micrologiciel démarre, et les informations sur le micrologiciel s'affichent si le micrologiciel mis à jour existe.

Remarque:

Vous pouvez également mettre à jour le micrologiciel à l'aide de Epson Device Admin. Vous pouvez confirmer visuellement les informations du micrologiciel sur la liste du périphérique. Cela est utile lorsque vous souhaitez mettre à jour le micrologiciel de plusieurs périphériques. Voir le guide Epson Device Admin ou l'aide pour plus de détails.

Informations connexes

➔ [« Comment exécuter Web Config dans un navigateur Web » à la page 39](#)

Mise à jour du micrologiciel sans connexion à Internet

Vous pouvez télécharger sur votre ordinateur le micrologiciel de l'appareil depuis le site Web d'Epson, puis relier l'appareil à l'ordinateur à l'aide d'un câble USB pour mettre à jour le micrologiciel. If you cannot update over the network, try this method.

Remarque:

Avant de procéder à la mise à jour, vérifiez que le pilote du scanner Epson Scan 2 est installé sur votre ordinateur. Si l'application Epson Scan 2 n'est pas installée, réinstallez-la.

1. Consultez le site Web d'Epson pour connaître les dernières mises à jour du micrologiciel.
<http://www.epson.com>
 - Si un micrologiciel est disponible pour votre scanner, téléchargez-le et passez à l'étape suivante.
 - Si aucun micrologiciel n'est disponible sur le site Web, alors vous utilisez déjà le micrologiciel le plus récent.
2. Utilisez un câble USB pour relier le scanner à l'ordinateur qui contient le micrologiciel téléchargé.
3. Double-cliquez sur le fichier .exe téléchargé.
Le Epson Firmware Updater démarre.
4. Suivez les instructions à l'écran.