EPSON
EXCEED YOUR VISION

Guide de l'administrateur

NPD5668-00 FR

Table des matières

Annexe

Paramètres de sécurité avancés pour les entreprises

Copyright

Marques commerciales

- ❏ EPSON® est une marque commerciale déposée et EPSON EXCEED YOUR VISION ou EXCEED YOUR VISION est une marque commerciale de Seiko Epson Corporation.
- ❏ Epson Scan 2 software is based in part on the work of the Independent JPEG Group.
- ❏ Google Cloud Print™, Chrome™, Chrome OS™, and Android™ are trademarks of Google Inc.
- ❏ Microsoft®, Windows®, Windows Server®, and Windows Vista® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Macintosh, Mac OS, OS X, AirMac, Bonjour, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint is a trademark of Apple Inc.
- ❏ Avis général : les autres noms de produit utilisés dans ce manuel sont donnés uniquement à titre d'identification et peuvent être des noms de marque de leur détenteur respectif. Epson dénie toute responsabilité vis-à-vis de ces marques.

À propos du présent manuel

Marques et symboles

> ***Attention:***
> *Instructions à suivre à la lettre pour éviter des blessures corporelles.*

> ***Important:***
> *Instructions à respecter pour éviter d'endommager votre équipement.*

Remarque:
Conseils utiles et limitations portant sur le fonctionnement du scanner.

Informations connexes

➡ Cliquez sur cette icône pour obtenir des informations connexes.

Descriptions utilisées dans ce manuel

❏ Les captures d'écran du pilote du scanner et les écrans d'Epson Scan 2 (pilote du scanner) proviennent de Windows 10 ou OS X El Capitan. Le contenu affiché sur les écrans dépend du modèle et de la situation.

❏ Les illustrations utilisées dans ce manuel sont fournies à titre d'exemple seulement. Bien qu'il puisse y avoir de légères différences selon le modèle, la méthode de fonctionnement est identique.

❏ Certaines options de menu affichées sur l'écran LCD varient selon le modèle et les paramètres.

Références du système d'exploitation

Windows

Dans ce manuel, des termes tels que « Windows 10 », « Windows 8.1 », « Windows 8 », « Windows 7 », « Windows Vista », « Windows XP », « Windows Server 2016 », « Windows Server 2012 R2 », « Windows Server 2012 », « Windows Server 2008 R2 », « Windows Server 2008 », « Windows Server 2003 R2 », et « Windows Server 2003 » sont utilisés pour faire référence aux systèmes d'exploitation suivants. De plus, « Windows » est utilisé pour faire référence à toutes les versions.

❏ 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 Vista®

❏ Système d'exploitation Microsoft® Windows® XP

- ❏ Système d'exploitation Microsoft® Windows® XP Professional x64 Edition
- ❏ 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
- ❏ Système d'exploitation Microsoft® Windows Server® 2003 R2
- ❏ Système d'exploitation Microsoft® Windows Server® 2003

Mac OS

Dans ce manuel, « Mac OS » est utilisé pour faire référence à « macOS Sierra », « OS X El Capitan », « OS X Yosemite », « OS X Mavericks », « OS X Mountain Lion », « Mac OS X v10.7.x », et « Mac OS X v10.6.8 ».

Introduction

Composition du manuel

Ce manuel s'adresse à l'administrateur de périphérique chargé de connecter l'imprimante ou le scanner au réseau. Il explique comment définir les paramètres nécessaires à l'utilisation des fonctions.

Pour des informations sur l'utilisation des fonctions, voir le *Guide d'utilisation*.

Préparation

Présente les tâches de l'administrateur, comment paramétrer les périphériques et le logiciel de gestion.

Connexion

Explique comment connecter un périphérique au réseau ou à une ligne téléphonique. Présente également l'environnement réseau, notamment l'utilisation d'un port pour le périphérique et apporte des informations sur le serveur DNS et proxy.

Paramètres des fonctions

Explique les paramètres de chaque fonction du périphérique.

Paramètres de sécurité de base

Présente les paramètres de chaque fonction, notamment pour l'impression, la numérisation et la télécopie.

Paramètres d'utilisation et de gestion

Présente les opérations à effectuer lorsque l'utilisation des périphériques a commencé, comme la consultation des informations et la maintenance.

Résolution des problèmes

Explique l'initialisation des paramètres et le dépannage du réseau.

Paramètres de sécurité avancés pour les entreprises

Explique comment paramétrer le périphérique pour renforcer sa sécurité, notamment comment utiliser un certificat d'autorité de certification, la communication SSL/TLS et le filtrage IPsec/IP.

Selon le modèle, certaines des fonctions indiquées dans ce chapitre peuvent ne pas être disponibles.

Définitions des termes utilisés dans le présent guide

Les termes suivants sont utilisés dans le présent guide.

Administrateur

Personne chargée d'installer et configurer le périphérique ou le réseau d'un bureau ou d'une organisation. Dans les petites organisations, cette personne peut être chargée de l'administration du périphérique et de celle du réseau. Dans les grandes organisations, les administrateurs sont responsables du réseau ou des périphériques d'un groupe

d'un service ou d'une division, tandis que les administrateurs réseau sont responsables des paramètres de communication à l'extérieur de l'organisation, notamment sur Internet.

Administrateur réseau

Personne chargée de contrôler les communications réseau. Elle doit paramétrer le routeur, le serveur proxy, le serveur DNS et le serveur de messagerie pour contrôler les communications par Internet ou par le réseau.

Utilisateur

Personne qui utilise des périphériques tels qu'imprimantes et scanners.

Web Config (page web du périphérique)

Serveur Web intégré au périphérique. Il est appelé Web Config. Il permet de contrôler et modifier l'état du périphérique à l'aide du navigateur.

Outil

Terme générique désignant un logiciel servant à installer ou gérer un périphérique, tel que Epson Device Admin, EpsonNet Config, EpsonNet SetupManager, etc.

Numérisation poussée

Terme générique désignant la numérisation depuis le panneau de commande du périphérique.

ASCII (American Standard Code for Information Interchange)

Un des codes de caractères standard. 128 caractères sont définis, tels que ceux de l'alphabet (a–z, A–Z), chiffres arabes (0–9), symboles, caractères d'espacement et caractères de contrôle. Lorsqu'il est mentionné dans ce guide, « ASCII » désigne les caractères 0x20–0x7E (nombres hexadécimaux) indiqués ci-dessous et ne comprend pas les caractères de contrôle.

SP*	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	

* Caractère espace.

Unicode (UTF-8)

Code standard international couvrant les principales langues du monde. Lorsqu'il est mentionné dans ce guide, « UTF-8 » désigne les caractères de codage au format UTF-8.

Préparation

Ce chapitre précise le rôle de l'administrateur et la préparation requise avant définition des paramètres.

Flux des paramètres et de la gestion du scanner

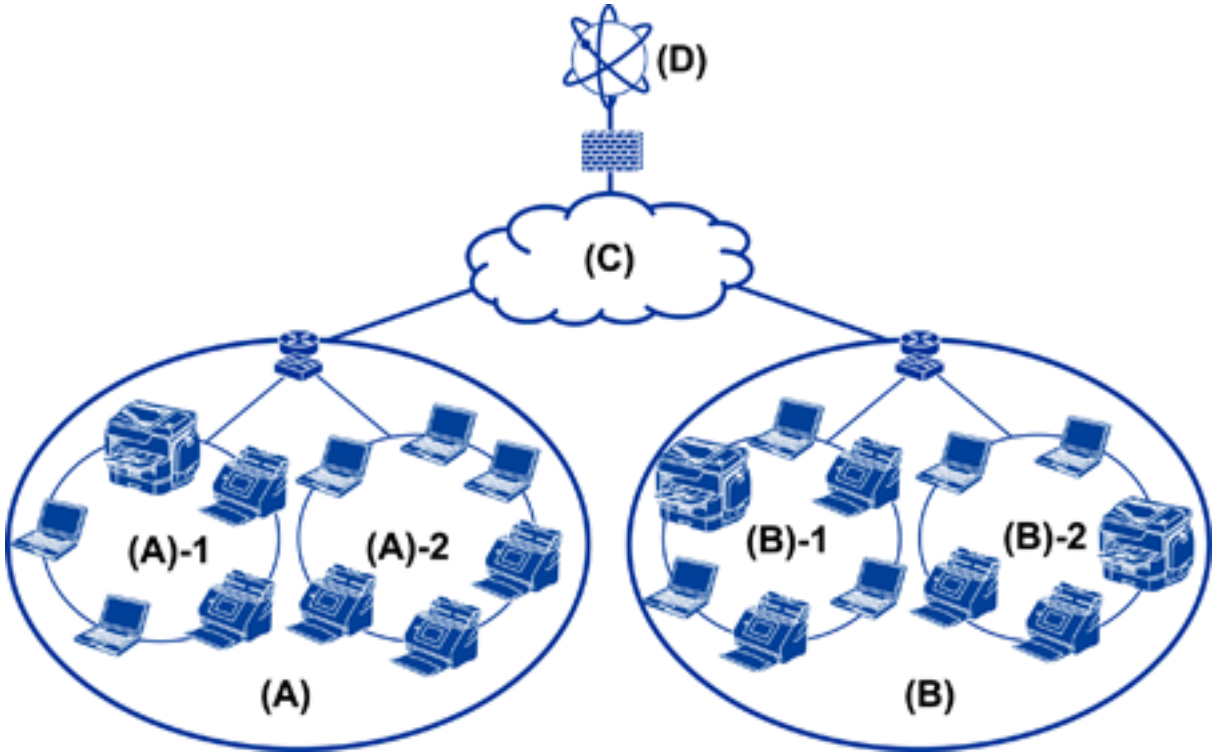
L'administrateur définit les paramètres de la connexion réseau, procède à l'installation initiale et à la maintenance du scanner afin qu'ils soient accessibles aux utilisateurs.

1. Préparation
   - ❏ Collecte des informations de paramétrage de la connexion
   - ❏ Choix de la méthode de connexion
2. Connexion
   - ❏ Connexion réseau à partir du panneau de commande du scanner
3. Paramétrage des fonctions
   - ❏ Paramètres du pilote du scanner
   - ❏ Autres paramètres avancés
4. Paramètres de sécurité
   - ❏ Paramètres administrateur
   - ❏ SSL/TLS
   - ❏ Contrôle de protocole
   - ❏ Paramètres de sécurité avancés (option)
5. Utilisation et gestion
   - ❏ Vérification du statut de l'imprimante
   - ❏ Gestion des évènements
   - ❏ Sauvegarde des paramètres du périphérique

Informations connexes

➡ « Préparation » à la page 10
➡ « Connexion » à la page 15
➡ « Paramètres des fonctions » à la page 22
➡ « Paramètres de sécurité de base » à la page 33
➡ « Paramètres d'utilisation et de gestion » à la page 41

Exemple d'environnement réseau



(A) : bureau 1

❏ (A) – 1 : réseau local 1

❏ (A) – 2 : réseau local 2

(B) : bureau 2

❏ (B) – 1 : réseau local 1

❏ (B) – 2 : réseau local 2

(C) : réseau étendu

(D) : Internet

Introduction d'un exemple de paramètre de connexion du scanner

Il existe deux types de connexion principaux selon l'utilisation du scanner. Les deux utilisent le concentrateur pour connecter le scanner en réseau avec l'ordinateur.

❏ Connexion serveur/client (scanner à l'aide du serveur Windows, gestion des tâches)

❏ Connexion peer-to-peer (connexion directe via l'ordinateur client)

Informations connexes

➡ « Connexion serveur/client » à la page 12

➡ « Connexion peer-to-peer » à la page 12

Connexion serveur/client

Centralisez la gestion du scanner et des tâches avec Document Capture Pro Server installé sur le serveur. Cela est plus adapté à une tâche qui utilise plusieurs scanners afin de numériser un grande nombre de documents dans un format donné.

Informations connexes

➡ « Définitions des termes utilisés dans le présent guide » à la page 8

Connexion peer-to-peer

Utilisez un scanner individuel avec un pilote de scanner installé sur l'ordinateur client, tel que Epson Scan 2. L'installation de Document Capture Pro (Document Capture) sur l'ordinateur client vous permet d'exécuter des tâches sur les ordinateurs clients individuels du scanner.

Informations connexes

➡ « Définitions des termes utilisés dans le présent guide » à la page 8

Préparation de la connexion au réseau

Rassemblement d'informations sur le paramétrage de la connexion

Vous devez avoir une adresse IP, une adresse de passerelle, etc. pour la connexion réseau. Vérifiez ce qui suit à l'avance.

Divisions	Éléments	Remarque
Méthode de connexion du périphérique	❏ Ethernet	Utilisez un câble (paire torsadée blindée) STP de catégorie 5e ou supérieur pour la connexion Ethernet.
Informations sur la connexion au réseau local	❏ Adresse IP ❏ Masque de sous-réseau ❏ Passerelle par défaut	Elle n'est pas obligatoire si vous définissez automatiquement l'adresse IP à l'aide de la fonction DHCP du routeur.
Informations sur le serveur DNS	❏ Adresse IP du DNS principal ❏ Adresse IP du DNS secondaire	Si vous utilisez une adresse IP statique comme adresse IP, configurez le serveur DNS. Configurez quand procéder à une affectation automatique avec la fonction DHCP et quand le serveur DNS ne peut pas être affecté automatiquement.
Informations sur le serveur proxy	❏ Nom du serveur proxy ❏ Numéro de port	Configurez quand utiliser un serveur proxy pour la connexion Internet et quand utiliser le service Epson Connect ou la fonction de mise à jour automatique du microprogramme.

Spécifications du scanner

Pour connaître les spécifications prises en charge par le scanner en mode standard et avec connexion, consultez le *Guide d'utilisation*.

Utilisation du numéro de port

Pour le numéro de port utilisé par le scanner, reportez-vous à l'annexe.

Informations connexes

➡ « Utilisation du port pour le scanner » à la page 61

Type d'attribution d'adresse IP

Il y a deux types d'attribution d'une adresse IP au scanner.

Adresse IP statique :

Attribuer au scanner l'adresse IP unique prédéterminée.

L'adresse IP n'est pas modifiée, même lorsque le scanner ou le routeur sont arrêtés, et vous pouvez donc gérer le périphérique à partir de son adresse IP.

Ce type d'adresse convient pour un réseau où sont gérés un grand nombre de scanners, comme un grand bureau ou une école.

Attribution automatique par la fonction DHCP :

L'adresse IP correcte est automatiquement attribuée lorsque la communication est établie entre le scanner et le routeur prenant en charge la fonction DHCP.

S'il n'est pas pratique de modifier l'adresse IP d'un périphérique particulier, réservez à l'avance l'adresse IP puis attribuez-la.

Serveur DNS et serveur proxy

Si vous utilisez un service de connexion Internet, configurez le serveur DNS. Si vous ne le configurez pas, vous devez indiquer l'adresse IP utilisée pour l'accès sinon la résolution du nom pourrait échouer.

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.

Vous pouvez interdire l'accès à une URL spécifique en utilisant la fonction de filtrage, étant donné que le serveur proxy est capable de contrôler le contenu de la communication.

Méthode de paramétrage de la connexion réseau

Pour les paramètres de connexion de l'adresse IP, du masque de sous-réseau et de la passerelle par défaut du scanner, procédez comme suit.

Depuis le panneau de commande :

Configurez les paramètres depuis le panneau de commande de chaque scanner. Connectez-vous au réseau après avoir configuré les paramètres de connexion du scanner.

À l'aide du programme d'installation :

Si vous utilisez le programme d'installation, le réseau et l'ordinateur client du scanner sont définis automatiquement. Le paramètre est disponible en suivant les instructions du programme d'installation, même si vous n'avez qu'une connaissance superficielle du fonctionnement du réseau.

À l'aide d'un outil :

Utilisez un outil de l'ordinateur de l'administrateur. Vous pouvez rechercher un scanner puis le paramétrer ou créer un fichier SYLK pour appliquer des paramètres par lot aux scanners. Vous pouvez définir un grand nombre de scanners mais ils doivent être connectés physiquement au moyen d'un câble Ethernet avant d'être paramétrés. Cette méthode est donc conseillée si vous pouvez mettre en place un Ethernet pour le paramètre.

Informations connexes

➡ « Connexion au réseau à partir du panneau de commande » à la page 15

➡ « Connexion au réseau via le programme d'installation » à la page 19

➡ « Attribution d'une adresse IP avec EpsonNet Config » à la page 57

Connexion

Ce chapitre présente l'environnement ou la procédure de connexion du scanner au réseau.

Connexion au réseau

Connexion au réseau à partir du panneau de commande

Connectez le scanner au réseau à l'aide du panneau de commande du scanner.

Pour plus d'informations sur le panneau de commande du scanner, voir le *Guide d'utilisation*.

Attribution de l’adresse IP

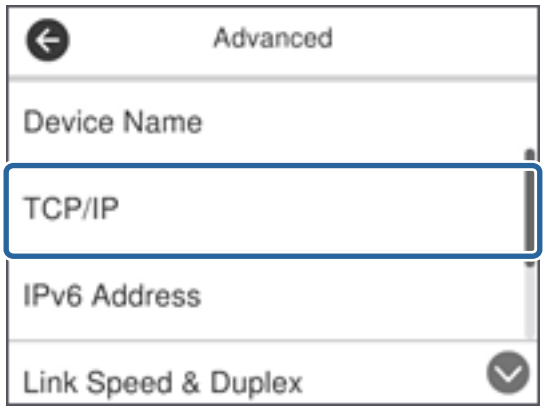
Définissez des éléments de base tels que Adresse IP, Masque de s-réseau, et Passerelle par défaut.

1. Mettez le scanner sous tension.
2. Effleurez l’écran vers la gauche sur le panneau de commande du scanner, puis appuyez sur **Param.**.

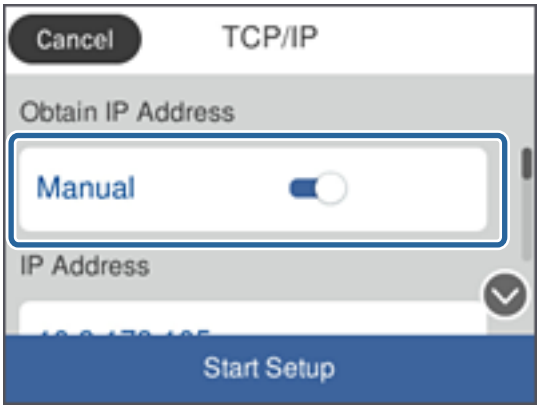
3. Appuyez sur **Paramètres réseau** > **Modifier les param.**.

   Si l’élément ne s’affiche pas, effleurez l’écran vers le haut pour l’afficher.

4. Appuyez sur **TCP/IP**.

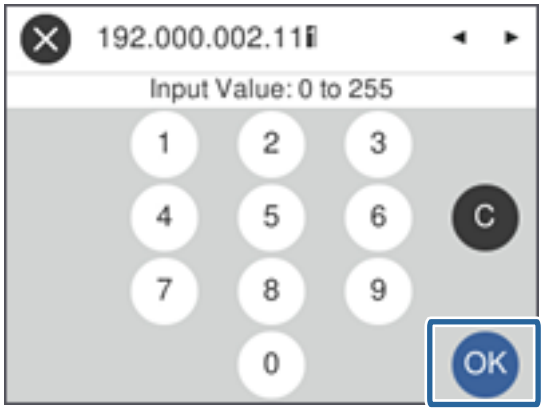


5. Sélectionnez **Manuel** pour **Obtenir l'adresse IP**.



Remarque:
Lorsque vous définissez l'adresse IP automatiquement à l'aide de la fonction DHCP du routeur, sélectionnez ***Auto****. Dans ce cas, les paramètres* ***Adresse IP****,* ***Masque de s-réseau****, et* ***Passerelle par défaut*** *des étapes 6 à 7 sont également définis automatiquement. Passez à l'étape 8.*

6. Appuyez sur le champ **Adresse IP**, saisissez l'adresse IP sur le clavier affiché à l'écran et appuyez sur **OK**.



Vérifiez la valeur indiquée sur l'écran précédent.

7. Définissez les options **Masque de s-réseau** et **Passerelle par défaut**.

   Vérifiez la valeur indiquée sur l'écran précédent.

   Remarque:
   *Si la combinaison de paramètres Adresse IP, Masque de s-réseau et Passerelle par défaut est incorrecte, **Démarrer configuration** est inactif et ne peut pas poursuivre le paramétrage. Vérifiez que vous n'avez fait aucune erreur de saisie.*

8. Appuyez sur le champ **DNS primaire** pour le **Serveur DNS**, saisissez l'adresse IP du serveur DNS principal sur le clavier affiché à l'écran et appuyez sur **OK**.

   Vérifiez la valeur indiquée sur l'écran précédent.

   Remarque:
   *Lorsque vous sélectionnez **Auto** pour les paramètres d'attribution de l'adresse IP, vous pouvez sélectionner les paramètres du serveur DNS dans **Manuel** ou **Auto**. Si vous ne pouvez pas obtenir automatiquement l'adresse du serveur DNS, sélectionnez **Manuel** et saisissez l'adresse du serveur DNS. Ensuite, saisissez directement l'adresse du serveur DNS secondaire. Si vous sélectionnez **Auto**, passez à l'étape 10.*

9. Appuyez sur le champ **DNS secondaire**, saisissez l'adresse IP du serveur DNS secondaire sur le clavier affiché à l'écran et appuyez sur **OK**.

   Vérifiez la valeur indiquée sur l'écran précédent.

10. Appuyez sur **Démarrer configuration**.

11. Sélectionnez **Fermer** sur l'écran de confirmation.

    L'écran se ferme automatiquement après une durée spécifique si vous n'appuyez pas sur **Fermer**.

Connexion à Ethernet

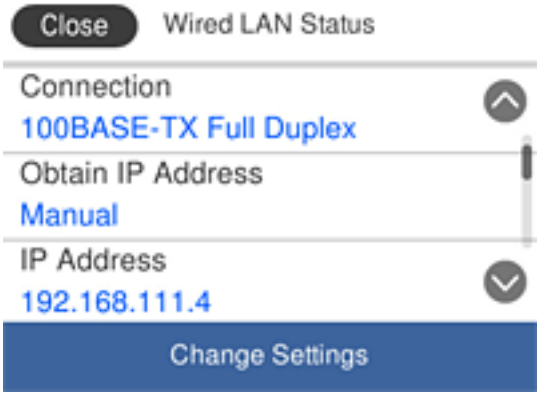
Connectez le scanner au réseau à l'aide du câble Ethernet et vérifiez la connexion.

1. Connectez le scanner et le concentrateur (commutateur L2) à l'aide d'un câble Ethernet.

   L'icône de l'écran d'accueil devient  .

2. Appuyez sur  au niveau de l'écran d'accueil.

3. Penchez l'écran vers le haut, puis vérifiez l'état de la connexion et l'adresse IP.



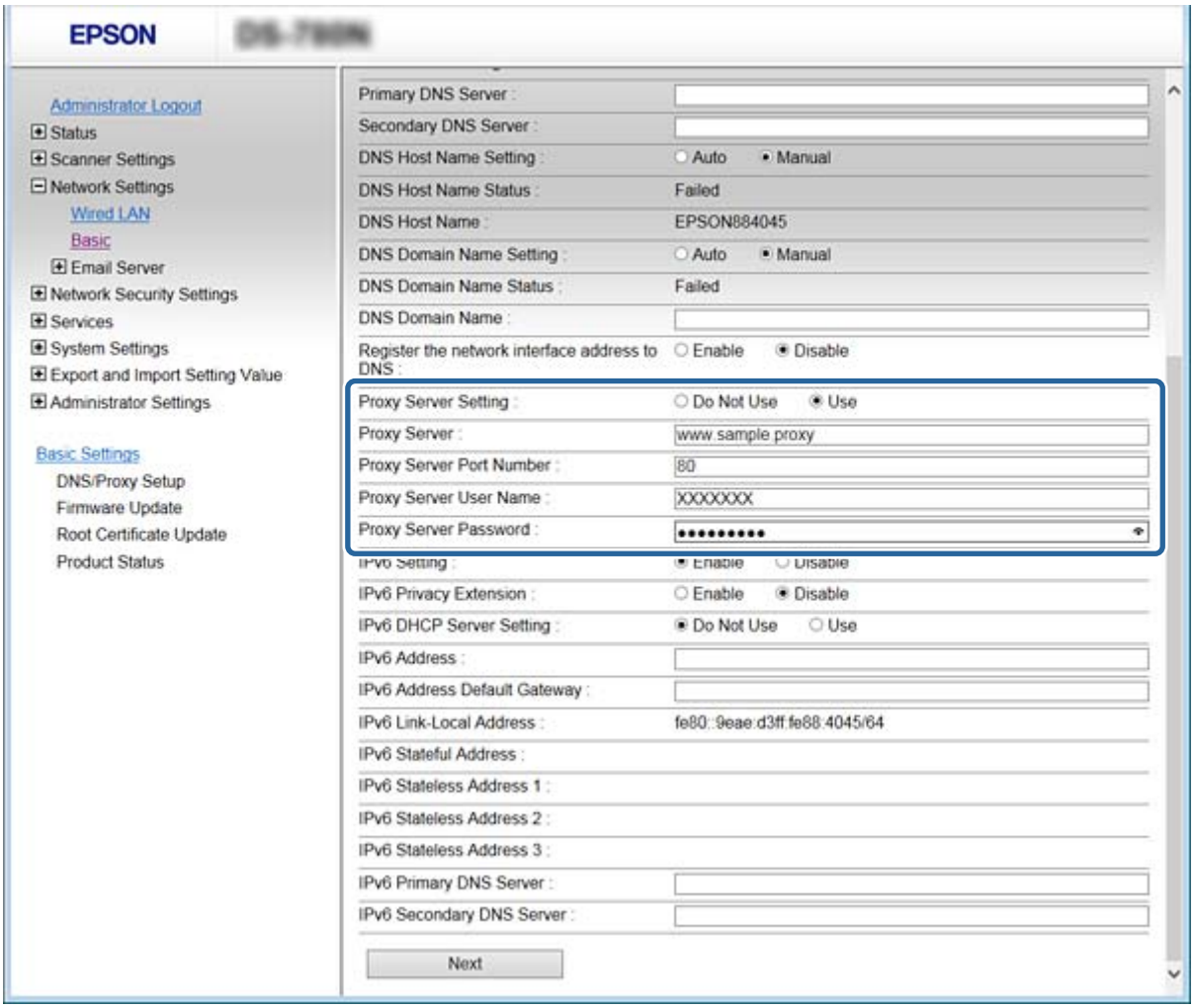
Paramétrage du serveur proxy

Il est impossible de définir le serveur proxy sur le panneau. Configurez à l'aide de Web Config.

1. Accédez à Web Config et sélectionnez **Paramètres réseau** > **De base**.
2. Sélectionnez **Utiliser** dans **Paramètre de Serveur proxy**.
3. Définissez le serveur proxy avec une adresse IPv4 ou au format FQDN **Serveur Proxy**, puis saisissez le numéro de port dans **Num. port serveur Proxy**.

   Pour les serveurs proxy nécessitant une authentification, saisissez le nom d'utilisateur et le mot de passe d'authentification du serveur proxy.

4. Cliquez sur le bouton **Suivant**.



5. Confirmez les paramètres, puis cliquez **Param.**.

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23

Connexion au réseau via le programme d'installation

Nous vous conseillons d'utiliser le programme d'installation pour connecter le scanner à un ordinateur. Vous pouvez exécuter le programme d'installation de l'une des manières suivantes.

❏ Configuration à partir du site Web

Accédez au site web suivant, puis saisissez le nom du produit. Allez dans **Installation**, puis lancez la configuration.

http://epson.sn

❏ Configuration depuis le CD du logiciel (uniquement pour les modèles fournis avec un CD et pour les utilisateurs dont les ordinateurs sont équipés de lecteurs de CD).

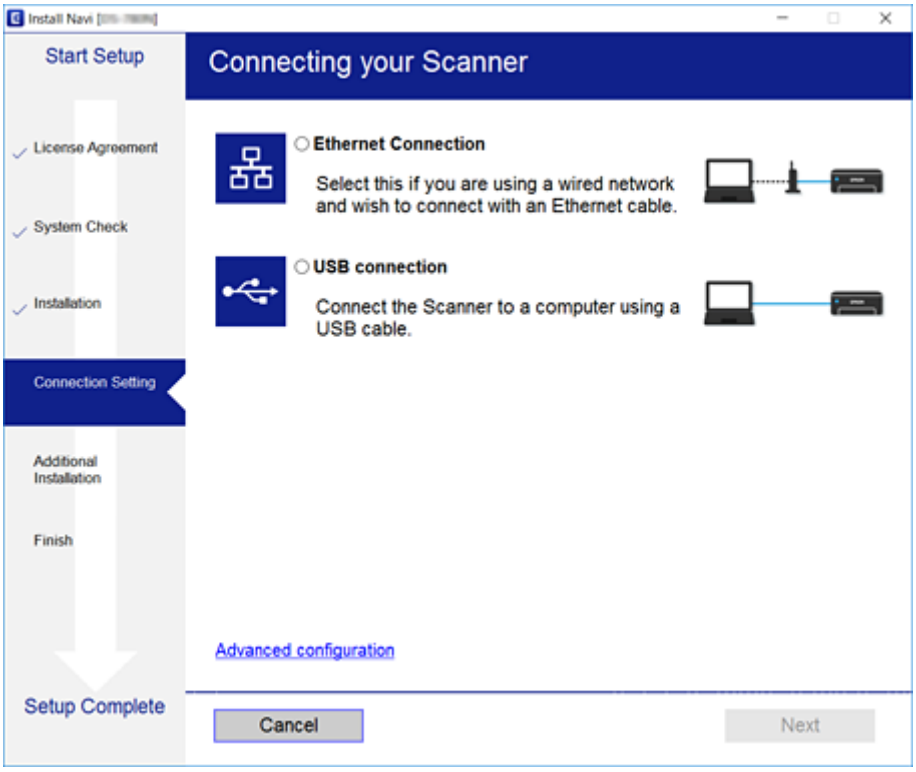
Insérez le CD dans l'ordinateur, puis suivez les instructions affichées à l'écran.

Sélection des méthodes de connexion

Suivez les instructions à l'écran jusqu'à ce que l'écran suivant s'affiche puis sélectionnez la méthode de connexion du scanner à l'ordinateur.

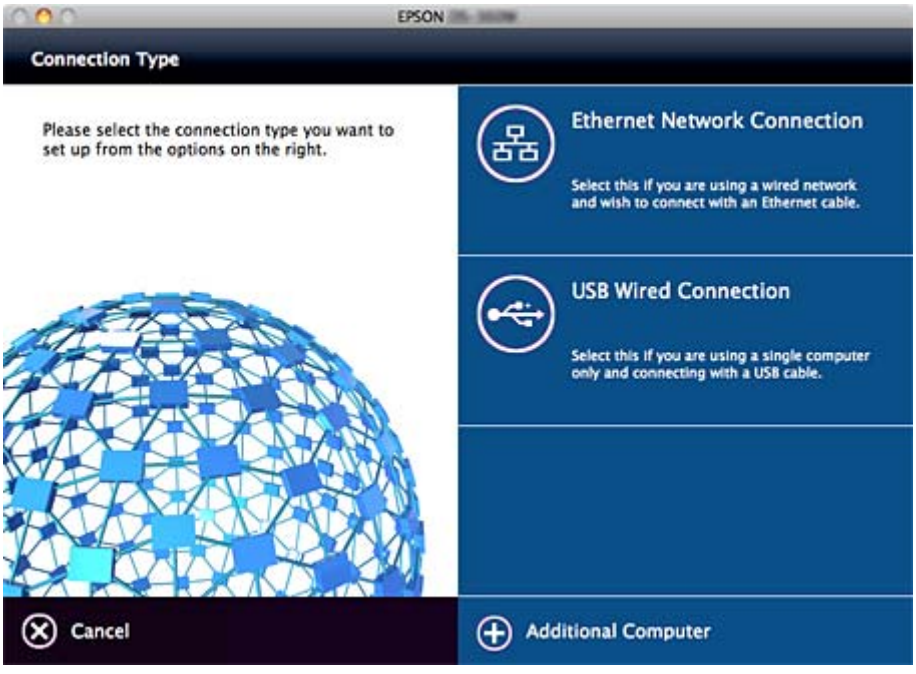
❏ Windows

Sélectionnez le type de connexion puis cliquez sur **Suivant**.



❏ Mac OS

Sélectionnez le type de connexion.



Connexion

Suivez les instructions affichées à l'écran. Le logiciel nécessaire est installé.

Paramètres des fonctions

Ce chapitre présente les premiers paramètres à définir pour utiliser chaque fonction du périphérique.

Logiciel de paramétrage

Cette section explique la procédure à suivre pour effectuer des paramétrages à partir de l'ordinateur de l'administrateur, en utilisant Web Config.

Web Config (Page web pour le périphérique)

À propos d'Web Config

Web Config est une application basée sur un navigateur qui permet de configurer les paramètres du scanner.

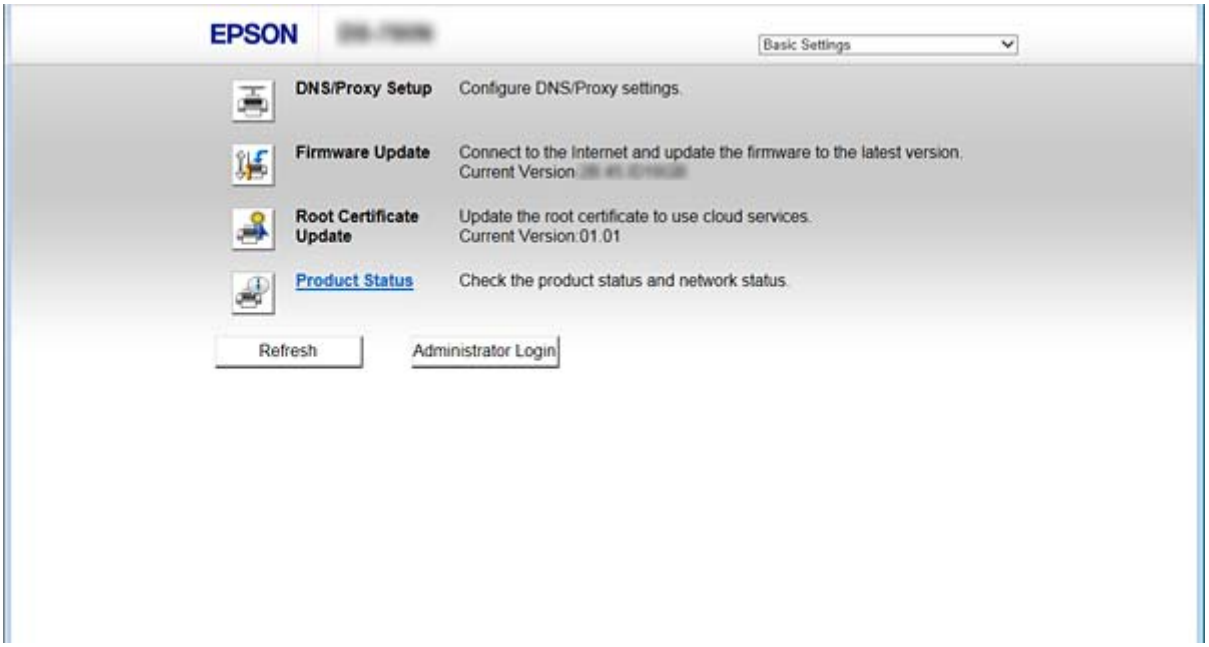
Pour accéder au logiciel Web Config, vous devez d'abord attribuer une adresse IP au scanner.

Remarque:
Vous pouvez verrouiller les paramètres en configurant le mot de passe administrateur du scanner.

Les deux pages de paramétrage suivantes sont disponibles.

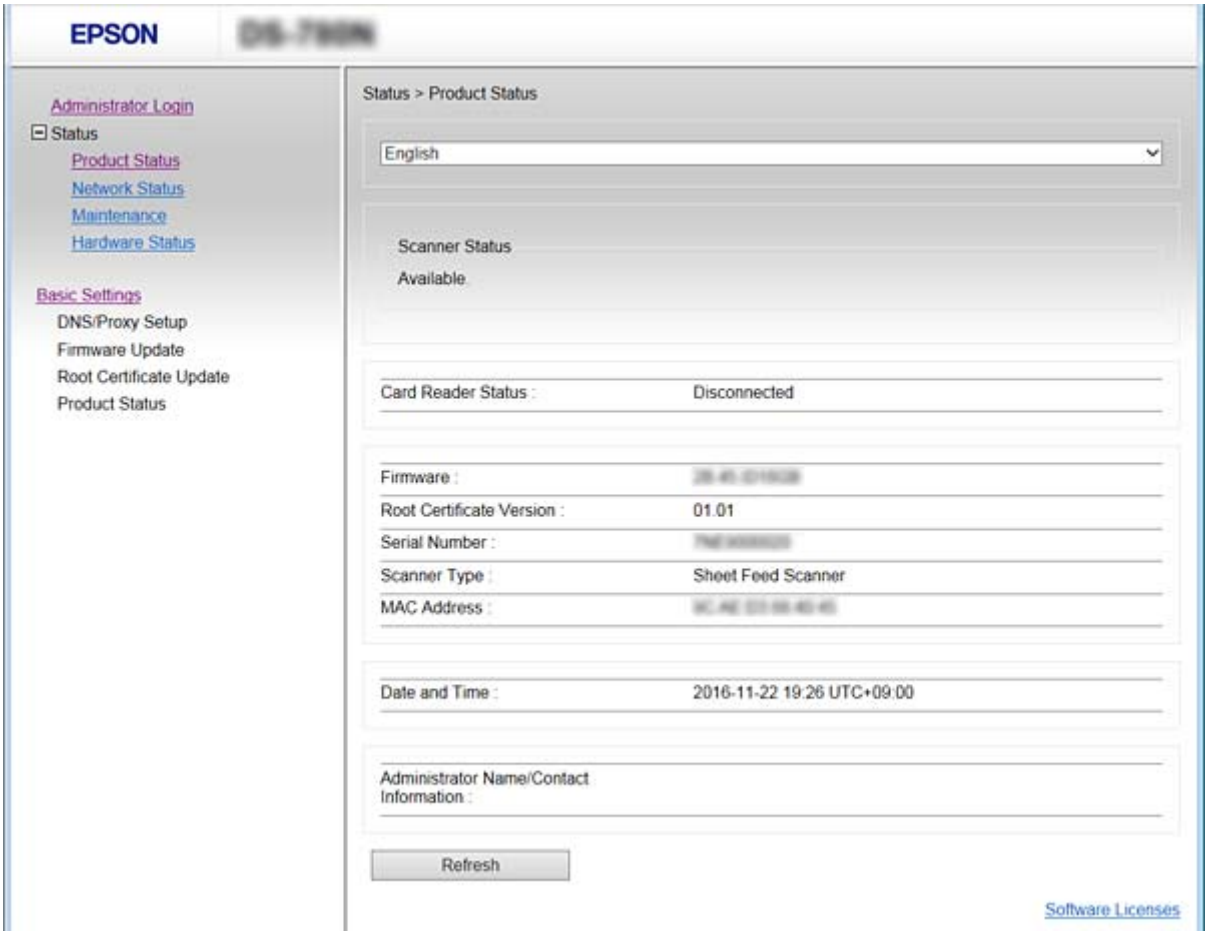
❏ **Paramètres de base**

Vous permet de configurer les paramètres de base du scanner.



❏ **Paramètres avancés**

Vous permet de configurer les paramètres avancés du scanner. Cette page est essentiellement destinée aux administrateurs.



Accès au logiciel Web Config

Saisissez l'adresse IP du scanner dans le navigateur Web. JavaScript doit être activé. Lorsque vous accédez à Web Config via HTTPS, un message d'avertissement s'affiche dans le navigateur du fait qu'un certificat à signature automatique, conservé sur le scanner, est utilisé.

❏ Accès via HTTPS

IPv4 : https://<adresse IP du scanner> (sans les < >)

IPv6 : https://[adresse IP du scanner]/ (sans les [ ])

❏ Accès via HTTP

IPv4 : http://<adresse IP du scanner> (sans les < >)

IPv6 : http://[adresse IP du scanner]/ (sans les [ ])

Remarque:

❏ *Exemples*

IPv4 :

https://192.0.2.111/

http://192.0.2.111/

IPv6 :

https://[2001:db8::1000:1]/

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

❏ *Si le nom du scanner a été enregistré à l'aide du serveur DNS, vous pouvez utiliser ce nom plutôt que l'adresse IP.*

Informations connexes

➡ « Communication SSL/TLS avec le scanner » à la page 64

➡ « À propos de la certification numérique » à la page 64

Utilisation des fonctions de numérisation

Selon la façon dont vous utilisez le scanner, installez les logiciels suivants et définissez les paramètres en conséquence.

❏ **Numériser à partir d'un ordinateur**

- ❏ Confirmez la validité du service de numérisation réseau à l'aide de Web Config (valide à la sortie de l'usine).
- ❏ Installez Epson Scan 2 sur votre ordinateur et définissez l'adresse IP
- ❏ Si vous utilisez des tâches pour numériser, installez Document Capture Pro (Document Capture) et définissez les paramètres des tâches.

❏ **Numériser à partir du panneau de commande**

- ❏ Si vous utilisez Document Capture Pro or Document Capture Pro Server :

  Installez Document Capture Pro ou Document Capture Pro Server

  Paramètre DCP (mode serveur, mode client).
- ❏ Si vous utilisez le protocole WSD :

  Confirmez la validité de WSD sur Web Config ou le panneau de commande (valide à la sortie de l'usine)

  Paramètres de périphérique supplémentaires (ordinateur Windows).

Numérisation à partir d'un ordinateur

Installez le logiciel et vérifiez que le service de numérisation réseau pour numériser depuis un ordinateur via le réseau est activé.

Informations connexes

➡ « Logiciel devant être installé » à la page 25

➡ « Activation de la numérisation réseau » à la page 25

Logiciel devant être installé

❏ Epson Scan 2

Ceci est un pilote de scanner. Si vous utilisez le périphérique depuis un ordinateur, installez le pilote sur chaque ordinateur client. Si Document Capture Pro/Document Capture est installé, vous pouvez réaliser les opérations attribuées aux boutons du périphérique.

Avec EpsonNet SetupManager, les pilotes d'imprimante peuvent également être distribués sous la forme de paquets.

❏ Document Capture Pro (Windows)/Document Capture (Mac OS)

Installez sur l'ordinateur client. Vous pouvez appeler et exécuter des tâches enregistrées sur un ordinateur avec Document Capture Pro/Document Capture installé sur le réseau à partir de l'ordinateur et du panneau de commande du scanner.

Vous pouvez également numériser à partir de l'ordinateur via le réseau. Epson Scan 2 est exigé pour la numérisation.

Informations connexes

➡ « EpsonNet SetupManager » à la page 57

Définissez l'adresse IP du scanner sur Epson Scan 2

Indiquez l'adresse IP du scanner de sorte que ce dernier puisse être utilisé sur le réseau.

1. Démarrez **Epson Scan 2 Utility** à partir de **Start** > **Tous les programmes** > **EPSON** > **Epson Scan 2**.

   Si un autre scanner est déjà enregistré, passez à l'étape 2.

   Si aucun n'est enregistré, passez à l'étape 4.

2. Cliquez sur ▼ on **Scanner**.
3. Cliquez sur **Paramètre**.
4. Cliquez sur **Activer la modification**, puis sur **Ajouter**.
5. Sélectionnez le nom du modèle de scanner **Modèle**.
6. Sélectionnez l'adresse IP du scanner pour être utilisé à **Adresse** in **Rechercher un réseau**.

   Cliquez sur  , puis sur  pour mettre à jour la liste. Si vous ne trouvez pas l'adresse IP du scanner, sélectionnez **Saisir adresse** et saisissez l'adresse IP.

7. Cliquez sur **Ajouter**.
8. Cliquez sur **OK**.

Activation de la numérisation réseau

Vous pouvez définir le service de numérisation réseau lorsque vous numérisez depuis un ordinateur client du réseau. Le paramètre par défaut est activé.

1. Accédez à la configuration Web et sélectionnez **Services** > **Numérisation en réseau**.
2. Assurez-vous que **Activer la numérisation** est sélectionné dans **EPSON Scan**.

   Si ce paramètre est sélectionné, la tâche est terminée. Fermez la configuration Web.

   Si elle est vierge, sélectionnez-la et passez à l'étape suivante.
3. Cliquez sur **Suivant**.
4. Cliquez sur **OK**.

   Le réseau est reconnecté puis les paramètres sont activés.

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23

Numérisation à l'aide du panneau de commande

La fonction de numérisation vers un dossier ou un e-mail utilisée via le panneau de commande du scanner, de même que le transfert de résultats de numérisation vers un e-mail, des dossiers, etc. est réalisée par l'exécution d'une tâche à partir de l'ordinateur.

Si vous transférez des résultats de numérisation, définissez la tâche dans Document Capture Pro Server ou Document Capture Pro.

Pour plus d'informations sur les paramètres et la définition de la tâche, consultez la documentation ou l'aide de Document Capture Pro Server ou Document Capture Pro.

Informations connexes

➡ « Paramètres de Document Capture Pro Server/Document Capture Pro » à la page 27

➡ « Paramétrage des serveurs et dossiers » à la page 27

Logiciel à installer sur l'ordinateur

❏ **Document Capture Pro Server**

Ceci est la version serveur de Document Capture Pro. Installez-le sur un serveur Windows. Plusieurs périphériques et tâches peuvent être gérés de manière centralisée par le serveur. Les tâches peuvent être exécutées simultanément de plusieurs scanners.

L'utilisation de la version certifiée de Document Capture Pro Server vous permet de gérer des tâches et l'historique de numérisations liées aux utilisateurs et aux groupes.

Pour plus d'informations sur Document Capture Pro Server, contactez votre bureau local Epson.

❏ **Document Capture Pro (Windows)/Document Capture (Mac OS)**

De la même manière qu'une numérisation à partir d'un ordinateur, vous pouvez appeler les tâches enregistrées sur l'ordinateur à partir du panneau de commande pour les exécuter. Il est impossible d'exécuter simultanément des tâches d'ordinateur depuis plusieurs scanners.

Paramètres de Document Capture Pro Server/Document Capture Pro

Définissez les paramètres d'utilisation de la fonction de numérisation à partir du panneau de commande du scanner.

1. Accédez à Web Config et sélectionnez **Services** > **Document Capture Pro**.
2. Sélectionnez **Mode Opération**.
   - ❏ Mode serveur :

     Sélectionnez ce mode uniquement si vous utilisez Document Capture Pro Server ou Document Capture Pro pour les tâches définies pour un ordinateur spécifique.
   - ❏ Mode client :

     Sélectionnez ce mode si vous sélectionnez le paramètre de tâche de Document Capture Pro (Document Capture) installé sur chaque ordinateur client du réseau sans spécifier l'ordinateur.
3. Définissez les paramètres suivants en fonction du mode sélectionné.
   - ❏ Mode serveur :

     Dans **Adresse serveur**, spécifiez le serveur sur lequel Document Capture Pro Server est installé. Il peut être compris entre 2 et 252 caractères au format IPv4, IPv6, nom d'hôte ou FQDN. Dans le format FQDN, les lettres US-ASCII, les chiffres, les alphabets et les tirets (à l'exception des tirets de devant ou derrière) peuvent être utilisés.
   - ❏ Mode client :

     Spécifiez **Paramètres de groupe** pour utiliser un groupe de scanners spécifié dans Document Capture Pro (Document Capture).
4. Cliquez sur **Param.**.

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23

Paramétrage des serveurs et dossiers

Document Capture Pro et Document Capture Pro Server enregistrent une fois les données numérisées sur l'ordinateur serveur ou client et utilisent la fonction de transfert pour exécuter les fonctions de numérisation vers un dossier ou e-mail.

Vous devez avoir l'autorisation et les informations nécessaires au transfert depuis l'ordinateur sur lequel Document Capture Pro, Document Capture Pro Server est installé vers l'ordinateur ou le service de cloud.

Préparez les informations de la fonction que vous allez utiliser en vous référant aux instructions suivantes.

Vous pouvez paramétrer ces fonctions à l'aide de Document Capture Pro ou Document Capture Pro Server. Pour plus d'informations sur les paramètres, consultez la documentation ou l'aide de Document Capture Pro Server ou Document Capture Pro.

Paramètres des fonctions

Nom	Paramètres	Condition
Numérisation vers un dossier réseau (SMB)	Créez et paramétrez le partage du dossier d'enregistrement	Le compte administrateur pour l'ordinateur qui crée les dossiers d'enregistrement.
	Destination pour la numérisation vers un dossier réseau (SMB)	Nom d'utilisateur et mot de passe pour s'identifier sur l'ordinateur contenant le dossier d'enregistrement, ainsi que les droits pour mettre à jour ce dernier.
Numérisation vers un dossier réseau (FTP)	Paramétrage de la connexion au serveur FTP	Informations de connexion au serveur FTP et droits pour mettre à jour le dossier d'enregistrement.
Numérisation vers un e-mail	Paramétrage pour le serveur de messagerie	Informations de paramétrage pour le serveur de messagerie
Numérisation vers Document Capture Pro (si utilisation de Document Capture Pro Server)	Configuration de la connexion aux services de cloud	Environnement de connexion Internet Enregistrement du compte des services de cloud

Utilisez la numérisation WSD (Windows uniquement)

Si l'ordinateur utilise Windows Vista ou une version ultérieure, vous pouvez utiliser la numérisation WSD.

Lorsque le protocole WSD peut être utilisé, le menu **Ordi (WSD)** s'affichera sur le panneau de commande du scaner.

1. Accédez à Web Config et sélectionnez **Services** > **Protocole**.
2. Confirmez que **Activer WSD** est coché dans **Paramètres WSD**.

   Si cette case est cochée, votre tâche est terminée et vous pouvez fermer Web Config.

   Si cette case n'est pas cochée, cochez-la et passez à l'étape suivante.
3. Cliquez sur le bouton **Suivant**.
4. Confirmez les paramètres et cliquez sur **Param.**.

Définition des paramètres du système

Configuration des paramètres système à partir du panneau de commande

Définition de la luminosité de l'écran

Définissez la luminosité de l'écran LCD.

1. Appuyez sur **Param.** au niveau de l'écran d'accueil.

2. Appuyez sur **Param. communs** > **Luminosité LCD**.
3. Appuyez sur  ou  pour ajuster la luminosité.
   Vous pouvez l'ajuster de 1 à 9.
4. Appuyez sur **OK**.

Définition du son

Définissez le son et le son d'erreur sur le panneau de commande.

1. Appuyez sur **Param.** au niveau de l'écran d'accueil.
2. Appuyez sur **Param. communs** > **Son**.
3. Définissez les éléments suivants selon les besoins.
   - ❏ Son de fonctionnement
     Définissez le volume du son de fonctionnement sur le panneau de commande.
   - ❏ Son d'erreur
     Définissez le volume du son d'erreur.
4. Appuyez sur **OK**.

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23

Détection d'une double alimentation d'un original

Découvrez la fonction permettant de détecter une double alimentation d'un document à numériser et arrêter la numérisation lorsque cela se produit.

Pour numériser des originaux devant être alimenté en une seule fois, tels que des enveloppes ou du papier à autocollants, désactivez-la.

Remarque:
Elle peut également être définie dans Web Config oy Epson Scan 2.

1. Appuyez sur **Param.** au niveau de l'écran d'accueil.
2. Appuyez sur **Paramètres de numérisation externes** > **Détection par ultrasons de double alim**.
3. Appuyez sur **Détection par ultrasons de double alim** pour l'activer ou le désactiver.
4. Appuyez sur **Fermer**.

Définition du mode de vitesse lente

Définissez le mode de vitesse lente de sorte qu'aucun bourrage papier ne se produise lors de la numérisation de fins documents, tels que des bordereaux.

1. Appuyez sur **Param.** au niveau de l'écran d'accueil.
2. Appuyez sur **Paramètres de numérisation externes** > **Lent**.
3. Appuyez sur **Lent** pour l'activer ou le désactiver.
4. Appuyez sur **Fermer**.

Définition des paramètres système à l'aide de la configuration Web

Paramètres d'économie d'énergie en période d'inactivité

Définissez les paramètres d'économie d'énergie à appliquer lorsque le scanner est inactif. Définissez le délai en fonction de votre environnement d'utilisation.

Remarque:
Vous pouvez également définir les paramètres d'économie d'énergie sur le panneau de commande du scanner.

1. Accédez à Web Config et sélectionnez **Paramètres système** > **Économie d'énergie**.
2. Saisissez le délai du **Minut. veille** au bout duquel basculer en mode économie d'énergie en cas d'inactivité.

   Vous pouvez paramétrer une durée allant jusqu'à 240 minutes à la minute près.
3. Sélectionnez le délai d'extinction du **Minuterie d'arrêt alim**.
4. Cliquez sur **OK**.

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23

Paramétrage du panneau de commande

Paramétrage pour le panneau de commande du scanner. Pour effectuer le paramétrage, vous pouvez procéder comme suit.

1. Accédez à Web Config et sélectionnez **Paramètres système** > **Panneau de commande**.
2. Définissez les éléments suivants selon les besoins.

   ❏ Langue

   Sélectionnez la langue d'affichage sur le panneau de commande.

❏ Verrouillage du panneau

Si vous sélectionnez **MARCHE**, le mot de passe administrateur est demandé si vous effectuez une opération exigeant des droits administrateur. Si le mot de passe administrateur n'est pas défini, le panneau de verrouillage est désactivé.

❏ Expiration opération

Si vous sélectionnez **MARCHE**, lorsque vous vous connectez en tant qu'administrateur, vous serez automatiquement déconnecté et renvoyé à l'écran initial s'il n'y a eu aucune activité pendant un certain laps de temps.

Vous pouvez définir un délai compris entre 10 secondes et 240 minutes.

3. Cliquez sur **OK**.

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23

Définition des limitations d'interface externe

Vous pouvez limiter la connexion USB depuis l'ordinateur. Cela a pour effet de limiter les numérisations hors du réseau.

1. Accédez à Web Config et sélectionnez **Paramètres système** > **Interface externe**.
2. Sélectionnez **Activer** ou **Désactiver**.

   Sélectionnez **Désactiver** pour restreindre.
3. Appuyez sur **OK**.

Synchronisation de la date et de l'heure avec un serveur horaire

Si vous utilisez un certificat d'autorité de certification, vous pouvez éviter les problèmes liés à l'heure.

1. Accédez à Web Config et sélectionnez **Paramètres système** > **Date et heure** > **Serveur d'heure**.
2. Sélectionnez **Utiliser** pour **Utiliser le serveur d'heure**.
3. Saisissez l'adresse du serveur horaire pour **Adresse du serveur d'heure**.

   Vous pouvez utiliser le format IPv4, IPv6 ou FQDN. Saisissez 252 caractères ou moins. Si vous ne donnez pas cette information, laissez la zone vide.
4. Saisissez le paramètre **Intervalle de mise à jour (min)**.

   Vous pouvez paramétrer une durée allant jusqu'à 10 800 minutes à la minute près.
5. Cliquez sur **OK**.

   Remarque:
   *Vous pouvez confirmer l'état de la connexion avec le serveur horaire sur **État du serveur d'heure**.*

Paramètres des fonctions

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23

Paramètres de sécurité de base

Ce chapitre présente les paramètres de sécurité de base qui n'exigent aucun environnement spécial.

Présentation des fonctions de sécurité de base

Voici une présentation des fonctions de fonctions de sécurité de base du périphérique.

Nom de la fonction	Type de fonction	Que définir	Risques à éviter
Paramétrage du mot de passe administrateur	Verrouillez les paramètres liés au système, tels que les paramètres de connexion réseau et USB, de sorte que l'administrateur soit le seul à pouvoir les modifier.	Un administrateur définit un mot de passe sur le périphérique. La configuration ou la mise à jour s'effectue au choix depuis Web Config, le panneau de commande, Epson Device Admin, et EpsonNet Config.	Éviter les lectures et modifications non autorisées des informations conservées dans le périphérique, telles qu'identifiant, mot de passe, paramètres réseau et contacts. Prévenir également de nombreux risques tels que la fuite d'informations pour l'environnement réseau ou la politique de sécurité.
Communications SSL/TLS	Lorsque vous accédez à un serveur Epson sur Internet à partir d'un périphérique, pour communiquer avec un ordinateur via un navigateur ou une mise à jour de micrologicie lpar exemple, le contenu de la communication est cryptée par le biais d'une communication SSL/TLS.	Procurez-vous un certificat signé par une autorité de certification puis importez-le dans le scanner.	L'obtention d'une identification du périphérique par un certificat délivré par une autorité de certification empêche toute usurpation d'identité et les accès non autorisés. De plus, le contenu des communications de SSL/TLS est protégé et empêche toute fuite de contenu des données d'impression et informations de paramétrage.
Protocoles de contrôle	Les protocoles de contrôles sont utilisés pour la communication entre les périphériques et les ordinateurs.	Un protocole ou service appliqué à des fonctionnalités autorisées ou interdites de manière isolée.	Limitez les risques associés à toute utilisation non intentionnée en empêchant les utilisateurs d'utiliser des fonctions dont ils n'ont pas besoin.

Informations connexes

➡ « À propos d'Web Config » à la page 22
➡ « EpsonNet Config » à la page 56
➡ « Epson Device Admin » à la page 56
➡ « Configuration du mot de passe administrateur » à la page 34
➡ « Contrôle des protocoles » à la page 36

Configuration du mot de passe administrateur

Lorsque vous définissez le mot de passe administrateur, les utilisateurs qui ne sont pas administrateurs ne peuvent pas modifier les paramètres d'administration du système. Vous pouvez définir et modifier le mot de passe administrateur en utilisant Web Config, le panneau de commande du scanner ou le logiciel (Epson Device Admin ou EpsonNet Config). Si vous utilisez le logiciel, consultez sa documentation.

Informations connexes

➡ « Configuration du mot de passe administrateur à partir du panneau de commande » à la page 34
➡ « Configuration du mot de passe administrateur avec Web Config » à la page 34
➡ « EpsonNet Config » à la page 56
➡ « Epson Device Admin » à la page 56

Configuration du mot de passe administrateur à partir du panneau de commande

Vous pouvez définir le mot de passe administrateur depuis le panneau de commande du scanner.

1. Appuyez sur **Param.** au niveau de l'écran d'accueil.
2. Appuyez sur **Administration système** > **Param admin**.

   Si l'élément ne s'affiche pas, effleurez l'écran vers le haut pour l'afficher.
3. Appuyez sur **Mot de passe Admin** > **Enreg.**.
4. Saisissez le nouveau mot de passe, puis appuyez sur **OK**.
5. Saisissez de nouveau le mot de passe, puis appuyez sur **OK**.
6. Sélectionnez **OK** sur l'écran de confirmation.

   L'écran des paramètres administrateur s'affiche.
7. Appuyez sur **Verrouiller le réglage**, puis appuyez sur **OK** dans l'écran de confirmation.

   Verrouiller le réglage est défini sur **On**, et le mot de passe administrateur sera demandé lorsque vous utiliserez l'élément de menu verrouillé.

Remarque:

❏ *Si vous définissez **Param.** > **Param. communs** > **Expiration opération** sur **On**, le scanner vous déconnecte au bout d'une période d'inactivité sur le panneau de commande.*

❏ *Vous pouvez modifier ou supprimer le mot de passe administrateur lorsque vous sélectionnez **Changer** ou **Réinitialiser** sur l'écran **Mot de passe Admin** et saisissez le mot de passe administrateur.*

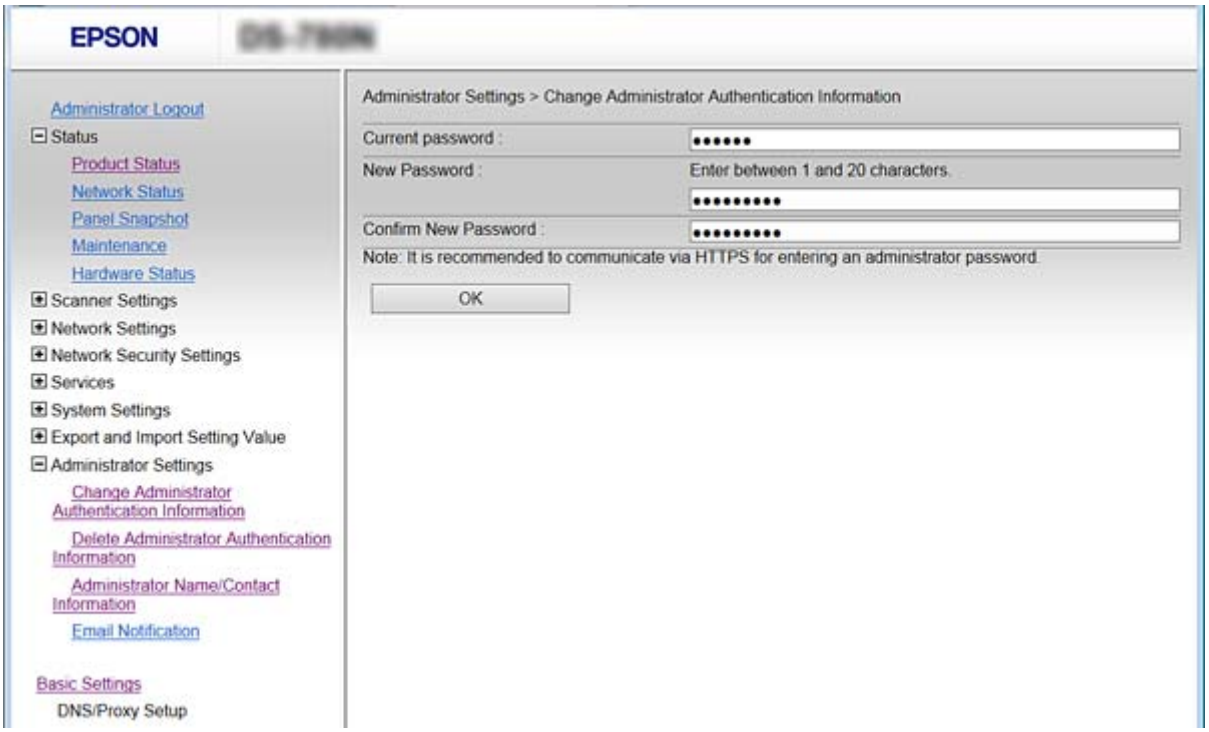
Configuration du mot de passe administrateur avec Web Config

Vous pouvez définir le mot de passe administrateur avec Web Config.

1. Accédez à Web Config et sélectionnez **Paramètres administrateur** > **Modifier les informations d'authentification de l'administrateur**.

2. Saisissez un mot de passe dans les champs **Nouveau MdPasse** et **Confirmez le nouveau MdPasse**. Si nécessaire, saisissez le nom d'utilisateur.

   Si vous voulez changer de mot de passe, saisissez un mot de passe en cours.



3. Sélectionnez **OK**.

   Remarque:

   ❏ *Pour définir ou modifier les éléments de menu verrouillés, cliquez sur* ***Connexion administrateur*** *puis saisissez le mot de passe administrateur.*

   ❏ *Pour supprimer le mot de passe administrateur, cliquez sur* ***Paramètres administrateur*** *>* ***Supprimer les informations d'authentification de l'administrateur****, puis saisissez le mot de passe administrateur.*

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23

Éléments à verrouiller à l'aide d'un mot de passe administrateur

Les administrateurs ont le droit de définir et modifier toutes les fonctions des périphériques.

Si vous définissez le mot de passe administrateur sur le périphérique, vous pouvez également le verrouiller afin que vous ne puissiez pas modifier des éléments liés à la gestion des périphériques.

L'administrateur peut contrôler les éléments suivants.

Élément	Description
Paramétrage du scanner	Définition de la double alimentation et du mode de vitesse lente.

Élément	Description
Paramètres de connexion Ethernet	Modification du nom des périphériques et de l'adresse IP, paramétrage du serveur DNS ou proxy et modifications des paramètres liées aux connexions réseau.
Paramétrage des services utilisateur	Paramétrage utilisé pour contrôler les protocoles de communication Network scan, numérisation réseau et les services Document Capture Pro.
Paramétrage du serveur de messagerie	Configuration d'un serveur de messagerie avec lequel les périphériques communiquent directement.
Paramètres de sécurité	Paramètres de sécurité du réseau, tels que la communication SSL/TLS, le filtrage IPsec/IP et IEEE802.1X.
Mise à jour d'un certificate raci	Mise à jour des certificats racine nécessaire pour l'authentification et la mise à jour du micrologiciel de Document Capture Pro Server à partir de Web Config.
Mise à jour du microprogramme	Contrôle et mise à jour du microprogramme des appareils.
Paramétrage de l'heure et des délais	Délai de passage en veille, extinction automatique, délai d'inactivité et autres paramètres de temporisation.
Restauration des paramètres par défaut	Rétablissement des paramètres usine du scanner.
Paramètres administrateur	Paramétrage du verrouillage administrateur ou d'un mot de passe administrateur.
Paramétrage de périphérique certifié	Paramétrage de l'identifiant du périphérique d'authentification. Paramétrage à définir en cas d'utilisation du scanner sur un système d'authentification prenant en charge des périphériques d'authentification.

Contrôle 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. L'utilisation de voies et de protocoles pour numériser est autorisée, par exemple. Vous pouvez réduire les risques pour la sécurité en limitant la numérisation à certains chemins ou en contrôlant les fonctions disponibles.

Configurez les paramètres de protocole.

1. Accédez à Web Config et sélectionnez **Services** > **Protocole**.
2. Configurez chaque élément.
3. Cliquez sur **Suivant**.
4. Cliquez sur **OK**.

   Les paramètres sont appliqués au scanner.

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23
➡ « Les protocoles que vous pouvez activer ou désactiver » à la page 37
➡ « Éléments de paramétrage du protocole » à la page 38

Les protocoles que vous pouvez activer ou désactiver

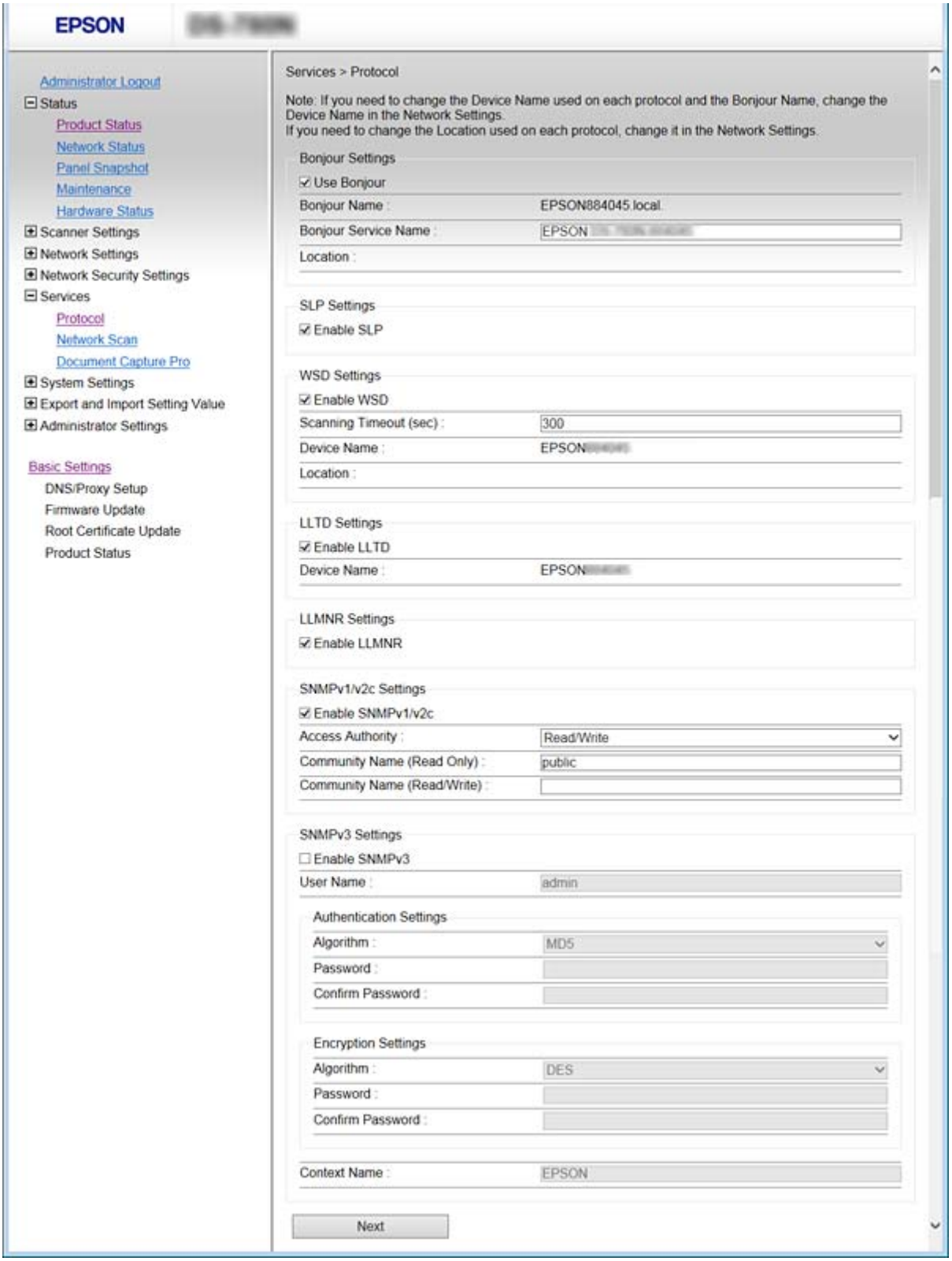
Protocole	Description
Réglages Bonjour	Vous pouvez choisir d'utiliser ou non Bonjour. Bonjour permet de rechercher des appareils, numériser avec et ainsi de suite.
Paramètres SLP	Vous pouvez activer ou désactiver la fonction SLP. SLP est utilisé pour Epson Scan 2 et l'analyse du réseau dans EpsonNet Config.
Paramètres WSD	Vous pouvez activer ou désactiver la fonction WSD. Si vous l'activez, vous pouvez ajouter des périphériques WSD ou numériser à partir du port WSD.
Paramètres LLTD	Vous pouvez activer ou désactiver la fonction LLTD. Si vous l'activez, elle s'affiche sur la carte réseau de Windows.
Paramètres LLMNR	Vous pouvez activer ou désactiver la fonction LLMNR. Si vous l'activez, vous pouvez utiliser la résolution de noms sans NetBIOS même si vous ne pouvez pas utiliser DNS.
Param SNMPv1/v2c	Vous pouvez choisir d'autoriser ou non SNMPv1/v2c. Cela permet de configurer les périphériques, la surveillance et ainsi de suite.
Param SNMPv3	Vous pouvez choisir d'autoriser ou non SNMPv3. Cela permet de configurer les périphériques chiffrés, la surveillance, etc.

Informations connexes

➡ « Contrôle des protocoles » à la page 36

➡ « Éléments de paramétrage du protocole » à la page 38

Éléments de paramétrage du protocole



Éléments	Valeur et description des paramètres
Réglages Bonjour	

Paramètres de sécurité de base

Éléments	Valeur et description des paramètres
Utiliser Bonjour	Sélectionnez cette option pour rechercher ou utiliser des périphériques via Bonjour.
Nom Bonjour	Affiche le nom Bonjour.
Nom du service Bonjour	Vous pouvez afficher et définir le nom du service Bonjour.
Emplacement	Affiche le nom d'emplacement Bonjour.
Paramètres SLP	
Activer SLP	Sélectionnez cette option pour activer la fonction SLP. Il utilisé pour découvrir le réseau dans Epson Scan 2 et EpsonNet Config.
Paramètres WSD	
Activer WSD	Sélectionnez cette option pour activer l'ajout de périphériques avec WSD et pour imprimer et numériser à partir du port WSD.
Expiration numérisation (sec)	Saisissez la valeur d'expiration de communication pour la numérisation WSD de 3 à 3600 secondes.
Nom de l'appareil	Affiche le nom de périphérique WSD.
Emplacement	Affiche le nom d'emplacement WSD.
Paramètres LLTD	
Activer LLTD	Sélectionnez cette option pour activer LLTD. Le scanner s'affiche sur la carte réseau Windows.
Nom de l'appareil	Affiche le nom de périphérique LLTD.
Paramètres LLMNR	
Activer LLMNR	Sélectionnez cette option pour activer LLMNR. Vous pouvez utiliser la résolution de noms sans NetBIOS même si vous ne pouvez pas utiliser DNS.
Param SNMPv1/v2c	
Activer SNMPv1/v2c	Sélectionnez cette option pour activer SNMPv1/v2c. Seules les scanners qui prennent en charge SNMPv3 s'affichent.
Autorité accès	Définissez l'autorité d'accès lorsque SNMPv1/v2c est activé. Sélectionnez **En lecture seule** ou **Lecture/écriture**.
Nom communauté (lecture seult)	Saisissez de 0 à 32 caractères ASCII (0x20 à 0x7E).
Nom communauté (lecture/écriture)	Saisissez de 0 à 32 caractères ASCII (0x20 à 0x7E).
Param SNMPv3	
Activer SNMPv3	SNMPv3 est activé lorsque la case est cochée.
Nom d'utilisateur	Saisissez de 1 à 32 caractères en utilisant des caractères sur un seul bit.
Param authentification	

Paramètres de sécurité de base

Éléments	Valeur et description des paramètres
Algorithme	Sélectionnez un algorithme d'authentification pour SNMPv3.
Mot de passe	Sélectionnez le mot de passe d'authentification pour SNMPv3. Saisissez entre 8 et 32 caractères au format ASCII (0x20–0x7E). Si vous ne donnez pas cette information, laissez la zone vide.
Confirmer le mot de passe	Saisissez le mot de passe configuré pour confirmation.
Param cryptage	
Algorithme	Sélectionnez un algorithme de chiffrement pour SNMPv3.
Mot de passe	Sélectionnez le mot de passe de chiffrement pour SNMPv3. Saisissez entre 8 et 32 caractères au format ASCII (0x20–0x7E). Si vous ne donnez pas cette information, laissez la zone vide.
Confirmer le mot de passe	Saisissez le mot de passe configuré pour confirmation.
Nom contexte	Saisissez 32 caractères maximum au format Unicode (UTF-8). Si vous ne donnez pas cette information, laissez la zone vide. Le nombre de caractères pouvant être saisis varie selon la langue.

Informations connexes

➡ « Contrôle des protocoles » à la page 36
➡ « Les protocoles que vous pouvez activer ou désactiver » à la page 37

Paramètres d'utilisation et de gestion

Ce chapitre présente les éléments liés aux opérations quotidiennes et à la gestion du périphérique.

Vérification des informations d'un périphérique

Vous pouvez vérifier les informations suivantes du périphérique depuis **État**, en utilisant Web Config.

❏ État du produit

Vérifiez la langue, le statut, le numéro de produit, l'adresse MAC, etc.

❏ État réseau

Vérifiez les informations sur le statut de la connexion du réseau, l'adresse IP, le serveur DNS, etc.

❏ Cliché panneau

Affichez un instantané de l'écran qui apparaît sur le panneau de commande du périphérique.

❏ Entretien

Vérifiez la date de début, les informations de numérisation, etc.

❏ État matériel

Vérifiez l'état du scanner.

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23

Gestion des périphériques (Epson Device Admin)

Vous pouvez gérer et piloter plusieurs périphériques depuis Epson Device Admin. Epson Device Admin permet de gérer des périphériques appartenant à des réseaux différents. Les fonctionnalités de gestion sont présentées ci-dessous.

Pour plus d'informations sur les fonctions et l'utilisation du logiciel, consultez la documentation ou l'aide de Epson Device Admin.

❏ Recherche de périphériques

Vous pouvez rechercher des périphériques sur le réseau et les enregistrer dans une liste. Si des périphériques Epson tels que des imprimantes ou des scanners sont connectés au même segment de réseau que l'ordinateur de l'administrateur, vous pouvez les trouver, même s'ils n'ont pas d'adresse IP.

Vous pouvez également rechercher des périphériques connectés à des ordinateurs du réseau au moyen de câbles USB. Vous devez installer Epson Device USB Agent sur l'ordinateur.

❏ Paramétrage des périphériques

Vous pouvez créer un modèle contenant les options de paramètres, tels que l'interface réseau et le source de papier, puis l'appliquer aux autres périphériques en tant que paramètres partagés. Lorsque le périphérique est connecté au réseau, vous pouvez lui attribuer une adresse IP s'il n'en a pas encore.

❏ Surveillance des périphériques

Vous pouvez obtenir des informations détaillées et le statut des périphériques du réseau. Vous pouvez également surveiller des périphériques connectés à des ordinateurs du réseau au moyen de câbles USB et les périphériques d'autres entreprises enregistrés dans la liste des périphériques. Pour surveiller ces appareils connectés par USB, vous devez installer Epson Device USB Agent.

❏ Gestion des alertes

Vous pouvez surveiller les alertes sur le statut des périphériques et consommables. Le système envoie automatiquement des e-mails de notification à l'administrateur en fonction des conditions définies.

❏ Gestion des rapports

Vous pouvez créer des rapports au fur et à mesure que le système accumule des données sur l'utilisation des appareils et sur les consommables. Vous pouvez ensuite enregistrer les rapports créés et les envoyer par e-mail.

Informations connexes

➡ « Epson Device Admin » à la page 56

Réception de notifications par courrier électronique en cas d'événements

À propos des notifications par e-mail

Vous pouvez utiliser cette fonction pour recevoir des alertes par e-mail lorsque des événements se produisent. Vous pouvez enregistrer jusqu'à 5 adresses e-mail et choisir les événements dont vous voulez être averti.

Le serveur de messagerie doit être configuré de manière à utiliser cette fonction.

Informations connexes

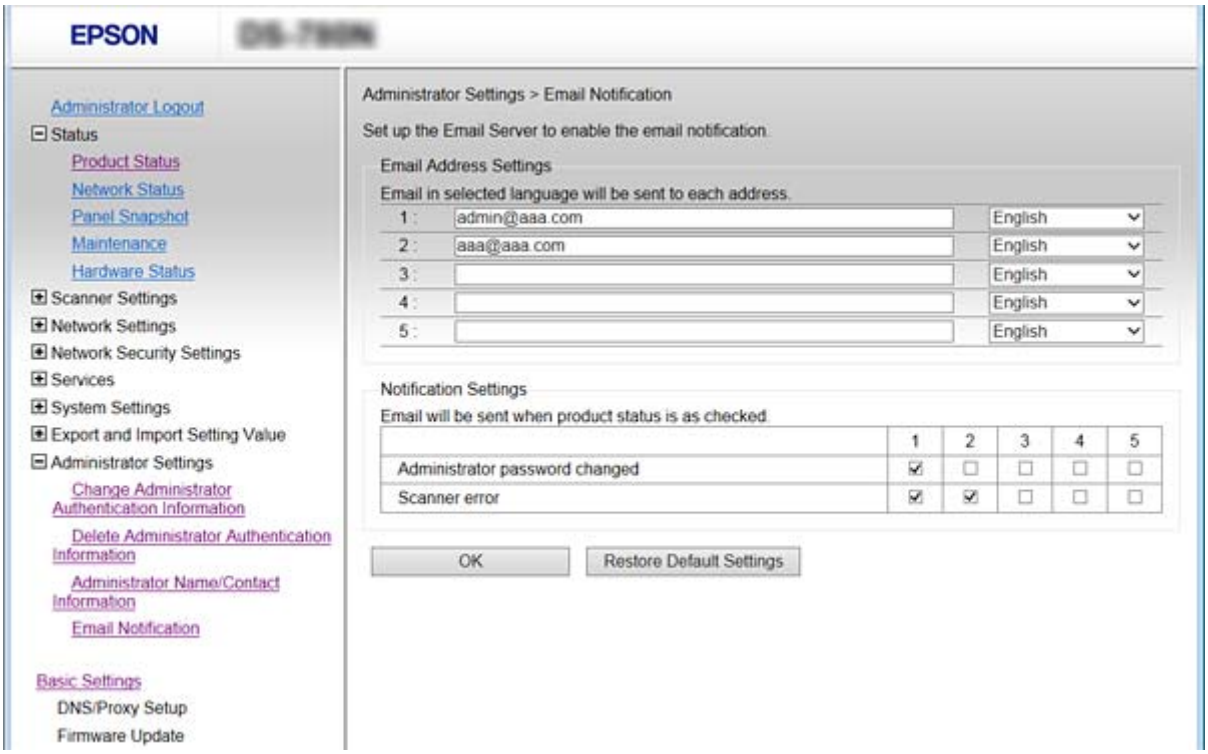
➡ « Configuration d'un serveur de messagerie » à la page 43

Configuration des notifications par e-mail

Pour utiliser la fonctionnalité, vous devez configurer un serveur de messagerie.

1. Accédez à Web Config et sélectionnez **Paramètres administrateur** > **Notification par email**.
2. Saisissez l'adresse e-mail à laquelle vous souhaitez recevoir les notifications.
3. Sélectionnez la langue des notifications par e-mail.

4. Cochez les cases des notifications que vous souhaitez recevoir.



5. Cliquez sur **OK**.

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23
➡ « Configuration d'un serveur de messagerie » à la page 43

Configuration d'un serveur de messagerie

Vérifiez ce qui suit avant la configuration.

❏ Le scanner est connecté à un réseau.

❏ Les informations du serveur de messagerie de l'ordinateur.

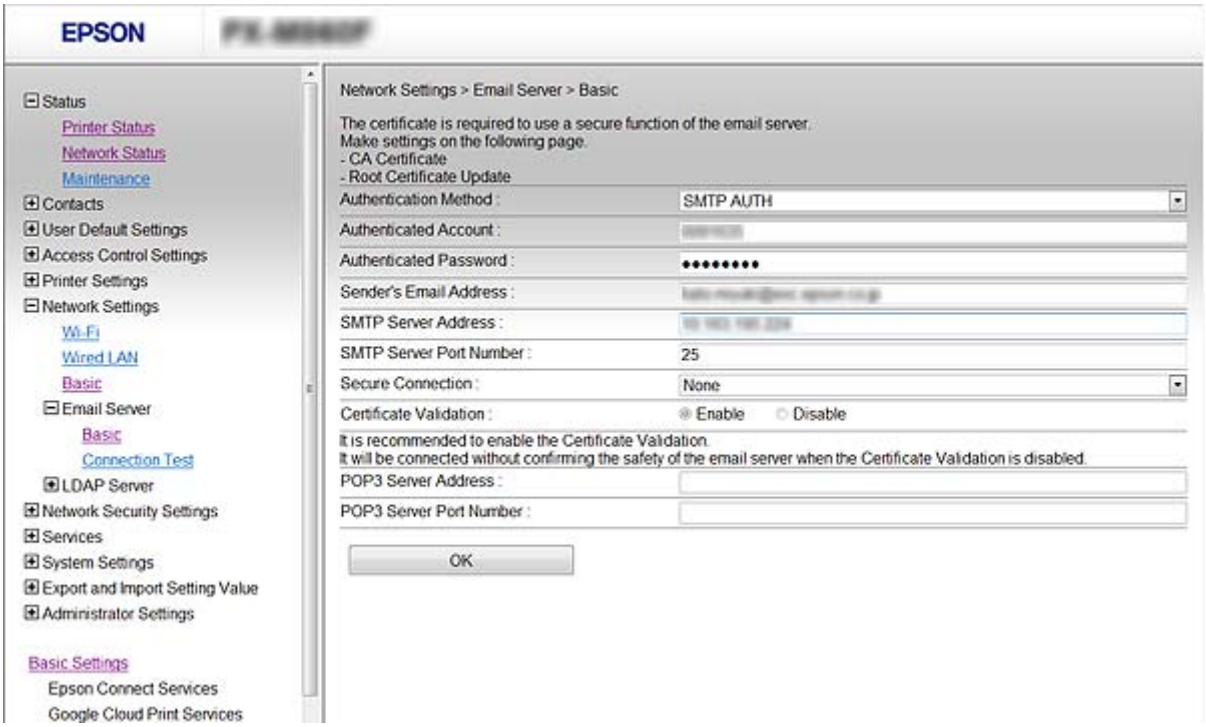
1. Accédez à Web Config et sélectionnez **Paramètres réseau** > **Serveur d'email** > **De base**.
2. Saisissez une valeur pour chaque élément.
3. Sélectionnez **OK**.

   Les paramètres sélectionnés sont affichés.

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23
➡ « Éléments de paramétrage du serveur de messagerie » à la page 44

Éléments de paramétrage du serveur de messagerie



Éléments	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	Exige qu'un serveur de messagerie prenne en charge l'authentification SMTP.
	POP avant SMTP	Si vous sélectionnez ce mode, vous devez configurer le serveur POP3.
Compte authentifié	Si vous sélectionnez **SMTP-AUTH** ou **POP avant SMTP** en tant que **Méthode d'authentification**, saisissez le nom du compte authentifié contenant de 0 à 255 caractères ASCII (0x20–0x7E).	
Mot de passe authentifié	Si vous sélectionnez **SMTP-AUTH** ou **POP avant SMTP** en tant que **Méthode d'authentification**, saisissez le mot de passe authentifié contenant de 0 à 20 caractères, A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.	
Adr. messagerie expéditeur	Saisissez l'adresse électronique de l'expéditeur. Saisissez de 0 à 255 caractères au format ASCII (0x20–0x7E), sauf : ( ) < > [ ] ; ¥. Le premier caractère ne peut être un point (.).	
Adresse du serveur SMTP	Saisissez de 0 à 255 caractères, A–Z a–z 0–9 . - . Vous pouvez utiliser le format IPv4 ou FQDN.	
Numéro port serveur SMTP	Saisissez un nombre de 1 à 65 535.	

Éléments	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	Le certificat est validé lorsque cette option est activée. Nous vous recommandons de sélectionner la valeur **Activer**.	
Adresse du serveur POP3	Si vous sélectionnez **POP avant SMTP** en tant que **Méthode d'authentification**, saisissez l'adresse de serveur POP3 contenant de 0 à 255 caractères, A–Z a–z 0–9 . - . Vous pouvez utiliser le format IPv4 ou FQDN.	
Numéro port serveur POP3	Si vous sélectionnez l'option **POP avant SMTP** pour le paramètre **Méthode d'authentification**, saisissez un nombre de 1 à 65535.	

Informations connexes

➡ « Configuration d'un serveur de messagerie » à la page 43

Vérification de la connexion au serveur de messagerie

1. Accédez à Web Config et sélectionnez **Paramètres réseau** > **Serveur d'email** > **Test de connexion**.
2. Sélectionnez **Démarrer**.

   Le test de connexion au serveur de messagerie est lancé. Le rapport de vérification s'affiche une fois le test terminé.

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23
➡ « Références du test de connexion au serveur de messagerie » à la page 45

Références du test de connexion au serveur de messagerie

Messages	Explications
Le test de connexion a réussi.	Ce message s'affiche une fois la connexion au serveur correctement établie.

Paramètres d'utilisation et de gestion

Messages	Explications
Erreur de communication avec le serveur SMTP. Vérifiez l'élément suivant. - Paramètres réseau	Ce message s'affiche lorsque ❏ Le scanner n'est pas connecté à un réseau ❏ Le serveur SMTP est indisponible ❏ La connexion réseau est interrompue lors de la communication ❏ Des données incomplètes sont reçues
Erreur de communication avec le serveur POP3. Vérifiez l'élément suivant. - Paramètres réseau	Ce message s'affiche lorsque ❏ Le scanner n'est pas connecté à un réseau ❏ Le serveur POP3 est indisponible ❏ La connexion réseau est interrompue lors de la communication ❏ Des données incomplètes sont reçues
Une erreur est survenue lors de la connexion au serveur SMTP. Vérifiez les éléments suivants. - Adresse du serveur SMTP - Serveur DNS	Ce message s'affiche lorsque ❏ La connexion à un serveur DNS a échoué ❏ La résolution de noms pour 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	Ce message s'affiche lorsque ❏ La connexion à un serveur DNS a échoué ❏ La résolution de noms pour un serveur POP3 a échoué
Erreur authentification sur serveur SMTP. Vérifiez les éléments suivants. - Méthode d'authentification - Compte authentifié - Mot de passe authentifié	Ce message s'affiche en cas d'échec de l'authentification du serveur SMTP.
Erreur authentification sur serveur POP3. Vérifiez les éléments suivants. - Méthode d'authentification - Compte authentifié - Mot de passe authentifié	Ce message s'affiche en cas d'échec de l'authentification du serveur POP3.
Méthode de communication non prise en charge. Vérifiez ce qui suit. - Adresse du serveur SMTP - Numéro port serveur SMTP	Ce message s'affiche lorsque vous essayez de communiquer avec des protocoles non pris en charge.
La connexion au serveur SMTP a échoué. Remplacez Connexion sécurisée par Aucun.	Ce message s'affiche lorsqu'une incompatibilité SMTP se produit entre un serveur et un client, ou lorsque le serveur ne prend pas en charge les connexions SMTP sécurisées (connexion SSL).
La connexion au serveur SMTP a échoué. Remplacez Connexion sécurisée par SSL/TLS.	Ce message s'affiche lorsqu'une incompatibilité SMTP se produit entre un serveur et un client, ou lorsque le serveur demande à utiliser une connexion SSL/TLS pour une connexion sécurisée SMTP.
La connexion au serveur SMTP a échoué. Remplacez Connexion sécurisée par STARTTLS.	Ce message s'affiche lorsqu'une incompatibilité SMTP se produit entre un serveur et un client, ou lorsque le serveur demande à utiliser une connexion STARTTLS pour une connexion sécurisée SMTP.
La connexion n'est pas de confiance. Vérifiez ce qui suit. - Date et heure	Ce message s'affiche lorsque la date et l'heure du scanner sont incorrectes ou que le certificat a expiré.
La connexion n'est pas de confiance. Vérifiez ce qui suit. - Certificat CA	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.
La connexion n'est pas de confiance.	Ce message s'affiche lorsque le certificat obtenu est endommagé.

Messages	Explications
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 spécifié est incorrecte.
Impossible d'accéder au produit tant que le traitement n'est pas terminé.	Ce message s'affiche lorsque le scanner est occupé.

Informations connexes

➡ « Vérification de la connexion au serveur de messagerie » à la page 45

Mise à jour du microprogramme

Mise à jour du microprogramme en utilisant Web Config

Met à jour le microprogramme en utilisant Web Config. Le périphérique doit être connecté à Internet.

1. Accédez à Web Config et sélectionnez **Paramètres de base** > **Mise à jour du micrologiciel**.
2. Cliquez sur **Démarrer**.

   La confirmation du microprogramme démarre, et les informations du microprogramme sont affichées s'il existe une mise à jour du microprogramme.
3. Cliquez sur **Démarrer**, puis suivez les instructions affichées à l'écran.

Remarque:
Vous pouvez également mettre à jour le microprogramme en utilisant Epson Device Admin. Vous pouvez consulter visuellement les informations de microprogramme sur la liste des périphériques. Cela est utile lorsque vous voulez mettre à jour le microprogramme de plusieurs périphériques. Pour plus de détails, reportez-vous au guide ou à l'aide d'Epson Device Admin.

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23
➡ « Epson Device Admin » à la page 56

Mettre à jour le microprogramme en utilisant Epson Firmware Updater

Vous pouvez télécharger sur l'ordinateur le microprogramme du périphérique à partir du site web d'Epson, puis connecter le périphérique et l'ordinateur avec un câble USB afin de mettre à jour le microprogramme. Essayez cette méthode si vous ne parvenez pas à effectuer la mise à jour à partir du réseau.

1. Accédez au site web d'Epson et téléchargez le microprogramme.
2. Utilisez un câble USB pour connecter le périphérique à l'ordinateur sur lequel vous avez téléchargé le microgramme.
3. Double-cliquez sur le fichier .exe téléchargé.

   Epson Firmware Updater démarre.
4. Suivez les instructions affichées à l'écran.

Sauvegarde des paramètres

En exportant les paramètres de Web Config, vous pouvez les copier sur d'autres scanners.

Exporter les paramètres

Exportez chaque paramètre du scanner.

1. Accédez à Web Config et sélectionnez **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 le mot de passe pour chiffrer le fichier exporté.

   Vous devrez disposer du mot de passe pour importer le fichier. Laissez cette option vide si vous ne souhaitez pas chiffrer le fichier.
4. Cliquez sur **Exporter**.

> ***Important:***
>
> *Si vous voulez exporter les paramètres réseau du scanner, comme son nom et son adresse IP, 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

➡ « Accès au logiciel Web Config » à la page 23

Importer les paramètres

Importez sur le scanner le fichier Web Config exporté.

> ***Important:***
> *Lors de l'importation de valeurs qui comprennent des informations individuelles, comme un nom du scanner ou une adresse IP, assurez-vous que la même adresse IP n'existe pas sur le même réseau. Si l'adresse IP existe déjà, le scanner ne reflète pas la valeur.*

1. Accédez à Web Config et sélectionnez **Exporter et importer valeur de paramètre** > **Importer**.
2. Sélectionnez le fichier exporté et saisissez le mot de passe du chiffrement.
3. Cliquez sur **Suivant**.
4. Sélectionnez les paramètres à importer, puis cliquez sur **Suivant**.
5. Cliquez sur **OK**.

Les paramètres sont appliqués au scanner.

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23

Dépannage

Conseils de dépannage

Vous trouverez de plus amples informations dans le manuel suivant.

❏ Guide d'utilisation

Fournit des instructions pour l'utilisation du scanner, l'entretien et le dépannage.

Vérification du journal du serveur et des périphériques réseau

En cas de problème avec une connexion réseau, il peut être possible d'identifier la cause en consultant le journal du serveur de messagerie, serveur LDAP, etc. et en vérifiant le journal réseau des commandes et journaux de l'équipement du système (des routeurs, par exemple).

Initialisation des paramètres réseau

Rétablissement des paramètres réseau à partir du panneau de commande

Vous pouvez réinitialiser tous les paramètres réseau.

1. Appuyez sur **Param.** au niveau de l'écran d'accueil.
2. Appuyez sur **Administration système** > **Rest param défaut** > **Paramètres réseau**.
3. Consultez le message, puis appuyez sur **Oui**.
4. Lorsqu'un message de finalisation s'affiche, appuyez sur **Fermer**.

   L'écran se ferme automatiquement après une durée spécifique si vous n'appuyez pas sur **Fermer**.

Vérification de la communication entre les périphériques et ordinateurs

Vérification de la connexion à l'aide d'une commande Ping — Windows

Vous pouvez utiliser une commande Ping pour vous assurer que l'ordinateur est bien connecté au scanner. Procédez comme suit pour vérifier la connexion à l'aide d'une commande Ping.

1. Vérifiez l'adresse IP du scanner pour la connexion que vous voulez contrôler.

   Vous pouvez la vérifier à l'aide d'Epson Scan 2.

2. Affichez l'écran d'invite de commandes de l'ordinateur.

   ❏ Windows 10

   Faites un clic droit sur le bouton Démarrer ou appuyez dessus de manière prolongée et sélectionnez **Invite de commandes**.

   ❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012

   Affichez l'écran de l'application et sélectionnez **Invite de commandes**.

   ❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 ou versions antérieures

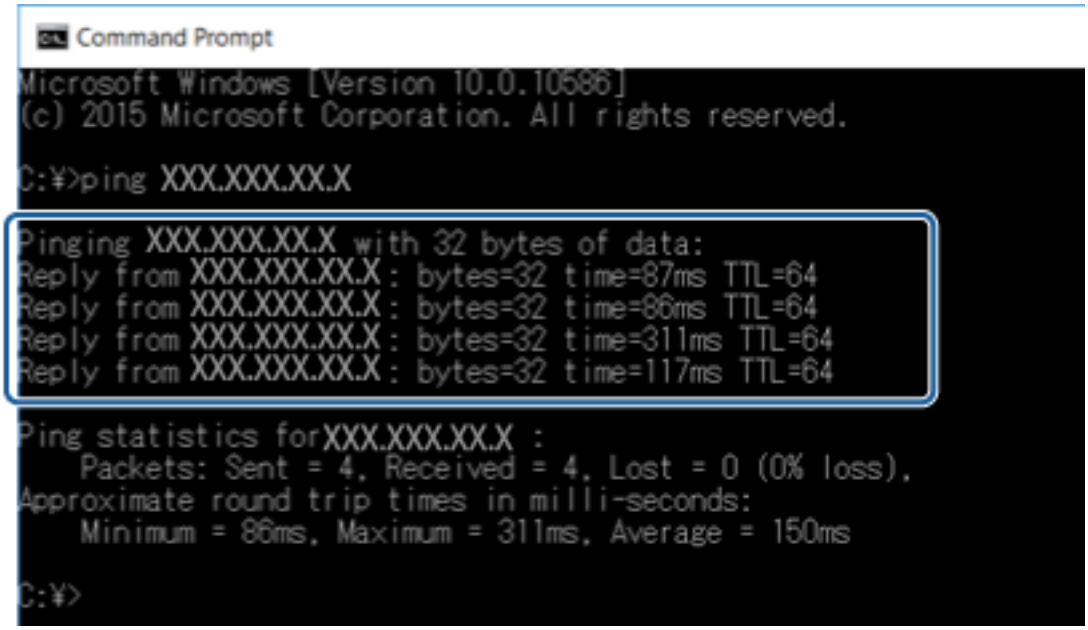
   Cliquez sur le bouton Démarrer, sélectionnez **Tous les programmes** ou **Programmes** > **Accessoires** > **Invite de commandes**.

3. Saisissez la chaîne de caractères ping xxx.xxx.xxx.xxx et appuyez sur la touche Entrée.

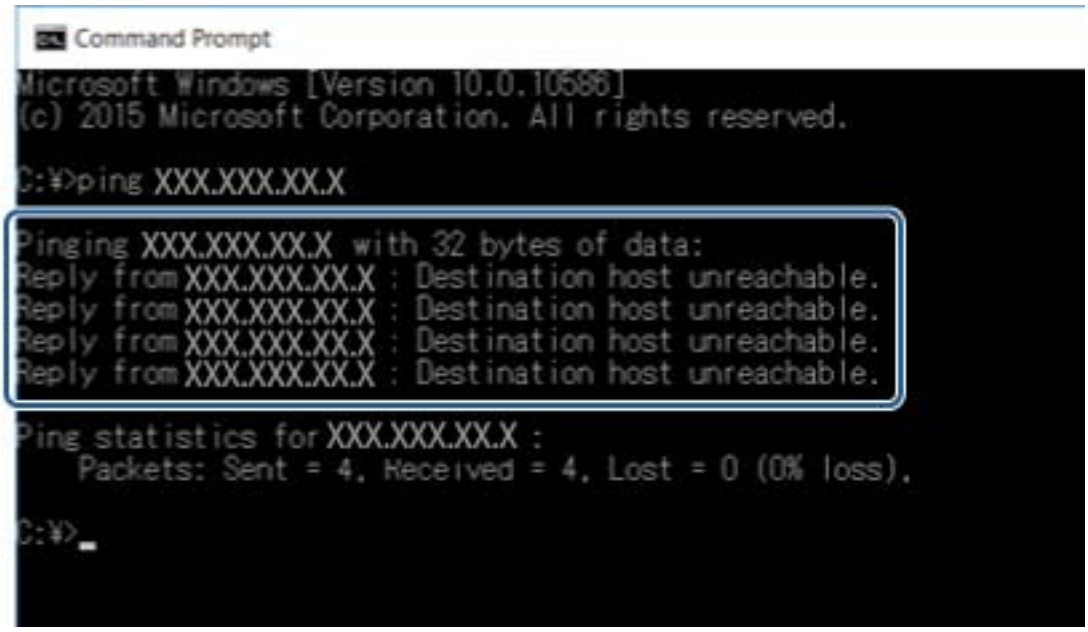
   Saisissez l'adresse IP du scanner pour xxx.xxx.xxx.xxx.

4. Vérifiez le statut de communication.

   Si le scanner et l'ordinateur communiquent, le message suivant s'affiche.



Si le scanner et l'ordinateur ne communiquent pas, le message suivant s'affiche.



Vérification de la connexion à l'aide d'une commande Ping — Mac OS

Vous pouvez utiliser une commande Ping pour vous assurer que l'ordinateur est bien connecté au scanner. Procédez comme suit pour vérifier la connexion à l'aide d'une commande Ping.

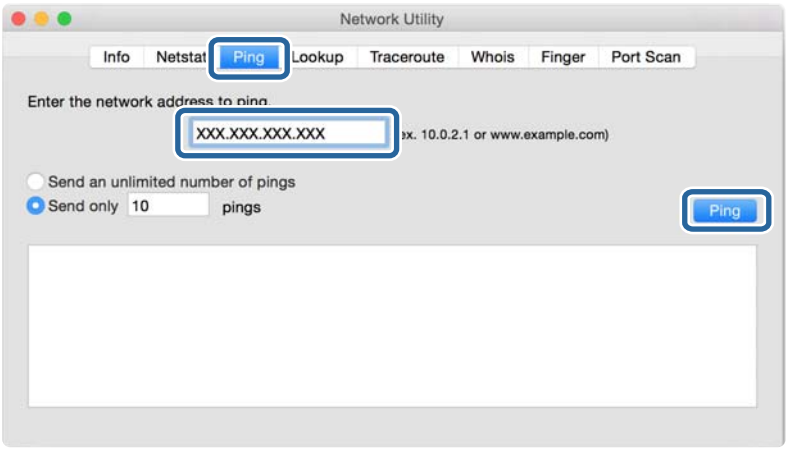
1. Vérifiez l'adresse IP du scanner pour la connexion que vous voulez contrôler.

   Vous pouvez la vérifier à l'aide d'Epson Scan 2.

2. Exécutez l'utilitaire Network Utility.

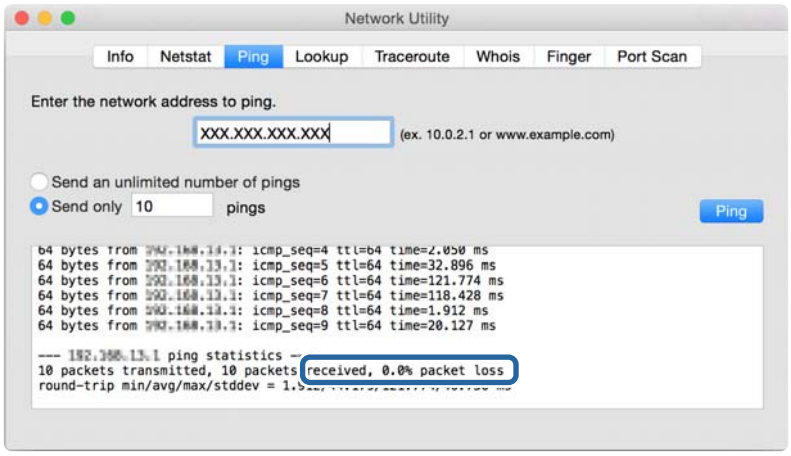
   Saisissez Network Utility sous **Spotlight**.

3. Cliquez sur l'onglet **Ping**, saisissez l'adresse IP vérifiée à l'étape 1, puis cliquez sur **Ping**.

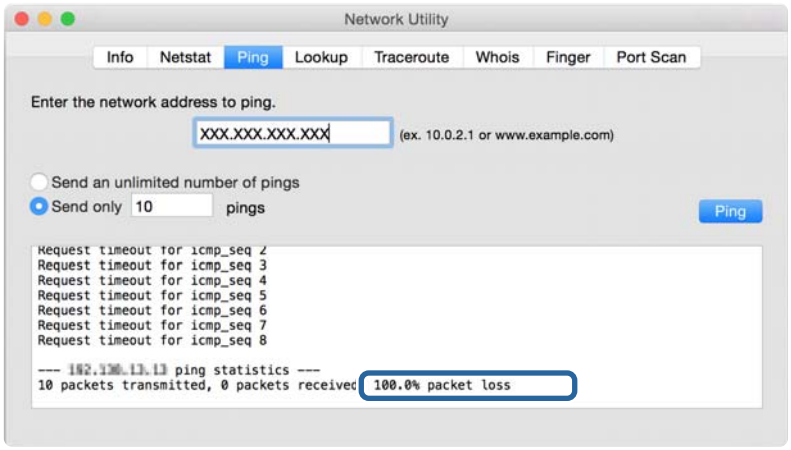


4. Vérifiez le statut de communication.

   Si le scanner et l'ordinateur communiquent, le message suivant s'affiche.



   Si le scanner et l'ordinateur ne communiquent pas, le message suivant s'affiche.



Problèmes lors de l'utilisation des logiciels réseau

Impossible d'accéder à la configuration Web

L'adresse IP du scanner est-elle correctement configurée ?

Configurez l'adresse IP à l'aide du logiciel Epson Device Admin ou EpsonNet Config.

Votre navigateur prend-il en charge les chiffrements en volume pour Force du cryptage avec le protocole SSL/TLS ?

Les chiffrements en volume pour Force du cryptage avec le protocole SSL/TLS sont indiqués ci-dessous. Web Config est uniquement accessible dans un navigateur prenant en charge les chiffrements en volume suivants. Vérifiez le chiffrement pris en charge par le navigateur.

❏ 80 bits : AES256/AES128/3DES

❏ 112 bits : AES256/AES128/3DES

❏ 128 bits : AES256/AES128

❏ 192 bits : AES256

❏ 256 bits : AES256

Le message « Pas à jour » s'affiche lorsque vous accédez au logiciel Web Config en utilisant le protocole SSL (https).

Si le certificat n'est pas à jour, vous devez obtenir un nouveau certificat. Si le message s'affiche avant la date d'expiration du certificat, vérifiez que la date du scanner est correctement configurée.

Le message « Le nom du certificat de sécurité ne correspond pas··· » s'affiche lorsque vous accédez au logiciel Web Config en utilisant le protocole SSL (https).

L'adresse IP du scanner saisie sous **Nom commun** pour la création d'un certificat à signature automatique ou d'un CSR ne correspond pas à l'adresse saisie dans le navigateur. Obtenez et importez de nouveau le certificat ou modifiez le nom du scanner.

Vous accédez au scanner via un serveur proxy.

Si vous utilisez un serveur proxy avec le scanner, vous devez configurer les paramètres proxy du navigateur.

❏ Windows :

Sélectionnez **Panneau de configuration** > **Réseau et Internet** > **Options Internet** > **Connexions** > **Paramètres de réseau local** > **Serveur proxy**, puis sélectionnez l'option permettant de ne pas utiliser le serveur proxy pour les adresses locales.

❏ Mac OS :

Sélectionnez **Préférences Système** > **Réseau** > **Avancé** > **Proxys**, puis enregistrez l'adresse locale sous **Ignorer les réglages 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

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23

➡ « Attribution de l'adresse IP » à la page 15

➡ « Attribution d'une adresse IP avec EpsonNet Config » à la page 57

Le nom du modèle et/ou l'adresse IP ne sont pas affichés au niveau du logiciel EpsonNet Config

Avez-vous sélectionné l'option Bloquer, Annuler ou Arrêter lorsque l'écran de sécurité Windows ou l'écran du pare-feu s'est affiché ?

Si vous avez sélectionné l'option **Bloquer**, **Annuler** ou **Arrêter**, l'adresse IP et le nom du modèle ne s'affichent pas dans le logiciel EpsonNet Config ou EpsonNet Setup.

Pour corriger cela, enregistrez EpsonNet Config en tant qu'exception à l'aide du pare-feu Windows et d'un logiciel de sécurité disponible dans le commerce. Si vous utilisez un programme antivirus ou de sécurité, fermez-le et utilisez plutôt EpsonNet Config.

Le réglage de l'expiration en cas d'erreur de communication est-il trop court ?

Exécutez le logiciel EpsonNet Config et sélectionnez **Tools** > **Options** > **Timeout**, puis augmentez la durée du réglage **Communication Error**. Notez que cela peut ralentir l'exécution du logiciel EpsonNet Config.

Informations connexes

➡ « Exécution du logiciel EpsonNet Config — Windows » à la page 57

➡ « Exécution du logiciel EpsonNet Config — Mac OS » à la page 57

Annexe

Présentation du logiciel réseau

Cette section décrit le logiciel qui configure et gère les périphériques.

Epson Device Admin

Epson Device Admin est une application qui vous permet d'installer des périphériques sur le réseau, puis de les configurer et de les gérer. Vous pouvez obtenir des informations supplémentaires sur ces périphériques tels que leur statut et leurs consommables, envoyer des alertes et créer des rapports d'utilisation. Vous pouvez aussi créer un modèle contenant les options de paramètres, puis l'appliquer aux autres périphériques en tant que paramètres partagés. Vous pouvez télécharger Epson Device Admin depuis le site Web de support Epson. Pour plus d'informations, reportez-vous à la documentation ou à l'aide du logiciel Epson Device Admin.

Exécution de Epson Device Admin (Windows uniquement)

Sélectionnez **All Programs** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**.

Remarque:
Si l'alerte du pare-feu s'affiche, autorisez l'accès pour le logiciel Epson Device Admin.

EpsonNet Config

Le logiciel EpsonNet Config permet à l'administrateur de configurer les paramètres réseau du scanner, tels que l'attribution d'une adresse IP et la modification du mode de connexion. La fonctionnalité de paramétrage par lot est prise en charge sous Windows. Pour plus d'informations, reportez-vous à la documentation ou à l'aide du logiciel EpsonNet Config.

Exécution du logiciel EpsonNet Config — Windows

Sélectionnez **Tous les programmes** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

Remarque:
Si l'alerte du pare-feu s'affiche, autorisez l'accès pour le logiciel EpsonNet Config.

Exécution du logiciel EpsonNet Config — Mac OS

Sélectionnez **Aller** > **Applications** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

EpsonNet SetupManager

EpsonNet SetupManager permet de créer un ensemble qui facilite l'installation du scanner (installation et configuration du pilote du scanner et installation de Document Capture Pro). Ce logiciel permet à l'administrateur de créer des ensembles logiciels uniques et de les distribuer aux groupes.

Pour plus d'informations, consultez le site web Epson régional.

Attribution d'une adresse IP avec EpsonNet Config

Vous pouvez attribuer une adresse IP au scanner avec EpsonNet Config. EpsonNet Config permet d'affecter une adresse IP à un scanner qui n'en a pas encore après avoir été connecté à l'aide d'un câble Ethernet.

Attribution d'une adresse IP par définition des paramètres par lot

Création du fichier des paramètres par lot

En utilisant l'adresse MAC et le nom du modèle comme clés, vous pouvez créer un nouveau fichier SYLK pour définir l'adresse IP.

1. Ouvrez une application de tableur (comme Microsoft Excel) ou un éditeur de texte.

2. Saisissez « Info_MACAddress », « Info_ModelName » et « TCPIP_IPAddress » sur la première ligne comme noms des éléments de paramétrage.

   Saisissez les éléments de paramétrage pour les chaînes texte suivantes. Pour faire la distinction entre les majuscules/minuscules et les caractères sur un/deux octets, si un seul caractère est différent l'élément n'est pas reconnu.

   Saisissez le nom de l'élément de paramétrage de la façon indiquée ci-dessous. Dans le cas contraire, EpsonNet Config ne peut pas reconnaître les éléments de paramétrage.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. Saisissez l'adresse MAC, le nom de modèle et l'adresse IP de chaque interface réseau.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress
0000XXXX0001	ALC-XXXXX	192.168.100.102
0000XXXX0002	ALC-XXXXX	192.168.100.103
0000XXXX0003	ALC-XXXXX	192.168.100.104

4. Saisissez un nom et enregistrez-le en tant que fichier SYLK (*.slk).

Définition des paramètres par lot à l'aide du fichier de configuration

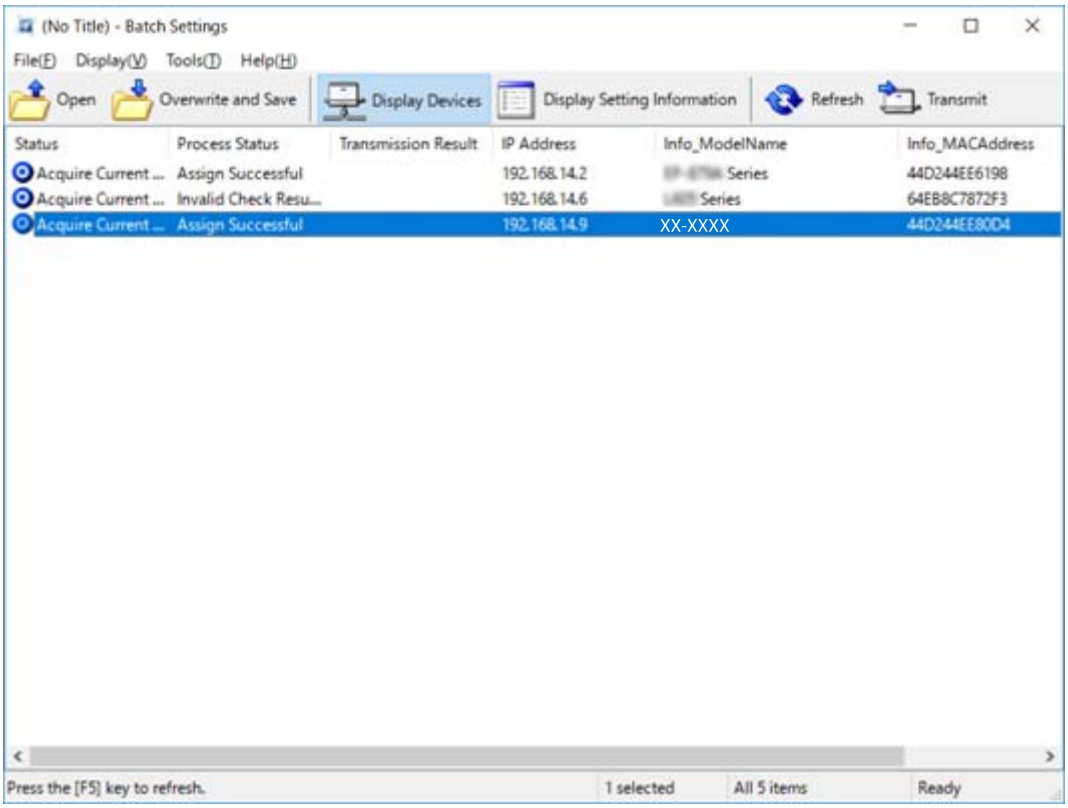
Affectez en une seule fois les adresses IP dans le fichier de configuration (fichier SYLK). Vous devez préalablement créer le fichier de configuration.

1. Connectez tous les périphériques au réseau à l'aide de câbles Ethernet.
2. Mettez le scanner sous tension.
3. Lancez l'application EpsonNet Config.

   Une liste des scanners du réseau s'affiche. Elle peut mettre du temps à apparaître.
4. Cliquez sur **Tools** > **Batch Settings**.
5. Cliquez sur **Open**.
6. Dans l'écran de sélection de fichier, sélectionnez le fichier SYLK (*.slk) contenant les paramètres puis cliquez sur **Open**.

7. Sélectionnez les périphériques dont vous voulez définir les paramètres par lot en définissant la colonne **Status** sur **Unassigned**, et le **Process Status** sur **Assign Successful**.

   Pour procéder à des sélections multiples, appuyez sur Ctrl ou Maj et cliquez ou faites glisser la souris.



8. Cliquez sur **Transmit**.

9. Lorsque l'écran de saisie de mot de passe est affiché, entrez le mot de passe et cliquez sur **OK**.

   Transmettez les paramètres.

   Remarque:
   Les informations sont transmises à l'interface réseau jusqu'à ce que l'indicateur de progression ait terminé. N'éteignez pas le périphérique ou l'adaptateur sans fil et n'envoyez pas de données au périphérique.

10. Sur l'écran **Transmitting Settings**, cliquez sur **OK**.

11. Vérifiez le statut du périphérique que vous avez paramétré.

    Dans le cas des périphériques qui affichent  ou  , vérifiez le contenu du fichier de paramétrage ou assurez-vous que le périphérique a redémarré normalement.

Icône	Status	Process Status	Explications
	Setup Complete	Setup Successful	Paramétrage réussi.
	Setup Complete	Rebooting	Une fois les informations transmises, chaque périphérique doit redémarrer pour activer les paramètres. Un contrôle est effectué pour déterminer si le périphérique peut être connecté après le redémarrage.
	Setup Complete	Reboot Failed	Impossible de confirmer le périphérique après transmission des paramètres. Vérifiez que le périphérique est sous tension ou qu'il a redémarré normalement.
	Setup Complete	Searching	Recherche du périphérique indiqué dans le fichier de paramétrages.*
	Setup Complete	Search Failed	Impossible de vérifier les périphériques déjà paramétrés. Vérifiez que le périphérique est sous tension ou qu'il a redémarré normalement.*

    * Seulement lorsque les informations de paramétrage sont affichées.

Informations connexes

➡ « Exécution du logiciel EpsonNet Config — Windows » à la page 57

➡ « Exécution du logiciel EpsonNet Config — Mac OS » à la page 57

Attribution d'une adresse IP à chaque appareil

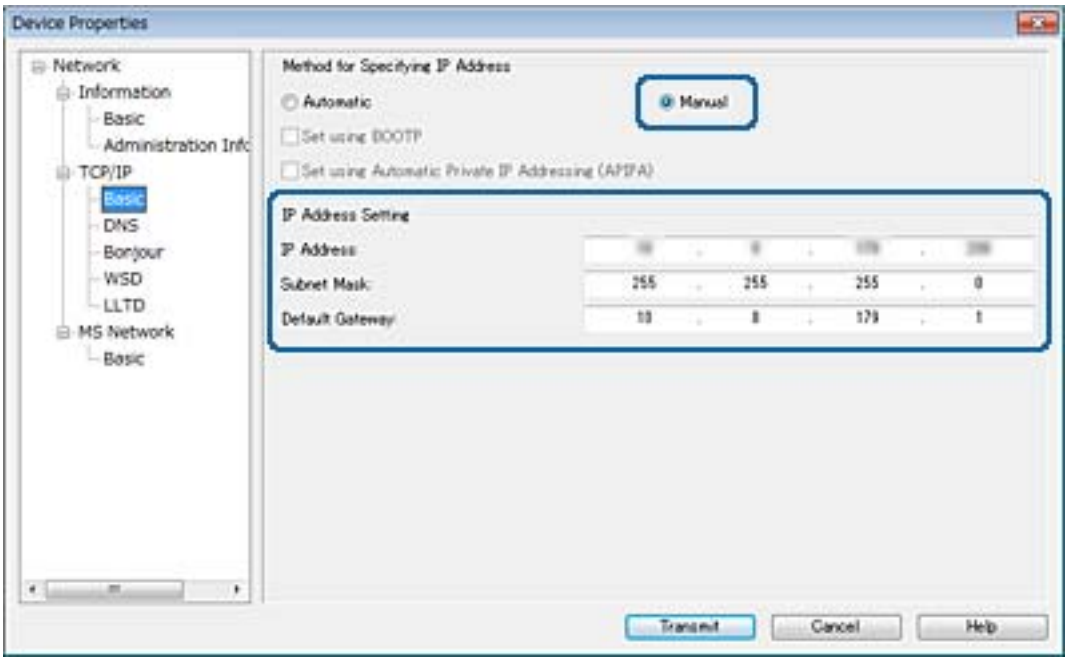
Attribuez une adresse IP au scanner avec EpsonNet Config.

1. Mettez le scanner sous tension.
2. Connectez le scanner au réseau à l'aide d'un câble Ethernet.
3. Lancez l'application EpsonNet Config.

   Une liste des scanners du réseau s'affiche. Elle peut mettre du temps à apparaître.
4. Double-cliquez sur le scanner auquel vous voulez attribuer une adresse IP.

   Remarque:
   Si plusieurs scanners du même modèle sont connectés, vous pouvez identifier le scanner par son adresse MAC.
5. Sélectionnez **Network** > **TCP/IP** > **Basic**.

6. Saisissez les adresses pour **IP Address**, **Subnet Mask**, et **Default Gateway**.



Remarque:
Saisissez une adresse statique lorsque vous connectez le scanner à un réseau sécurisé.

7. Cliquez sur **Transmit**.

   L'écran confirmant la transmission des informations s'affiche.

8. Cliquez sur **OK**.

   L'écran de fin de transmission s'affiche.

   Remarque:
   Les informations sont transmises au périphérique, puis le message « Configuration terminée. » s'affiche. N'éteignez pas le périphérique et n'envoyez pas de données au service.

9. Cliquez sur **OK**.

Informations connexes

➡ « Exécution du logiciel EpsonNet Config — Windows » à la page 57
➡ « Exécution du logiciel EpsonNet Config — Mac OS » à la page 57

Utilisation du port pour le scanner

Le scanner utilise le port suivant. L'administrateur réseau doit ouvrir ces ports pour qu'ils soient disponibles si nécessaire.

Annexe

Émetteur (client)	Utiliser	Destination (serveur)	Protocole	Numéro de port
Scanner	Envoi d'e-mail (notification par e-mail)	Serveur SMTP	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	Connexion POP avant SMTP (notification par e-mail	Serveur POP	POP3 (TCP)	110
	Contrôle WSD	Ordinateur client	WSD (TCP)	5357
	Recherche de l'ordinateur lors de la numérisation poussée à partir de Document Capture Pro	Ordinateur client	Recherche numérisation poussée réseau	2968
	Collecte d'informations relatives à la tâche lors d'une numérisation poussée depuis Document Capture Pro	Ordinateur client	Numérisation poussée réseau	2968
Ordinateur client	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	Recherche WS (UDP)	3702
	Transfert des données numérisées depuis Document Capture Pro	Scanner	Numérisation réseau (TCP)	1865

Paramètres de sécurité avancés pour les entreprises

Ce chapitre décrit les fonctions de sécurité avancées.

Paramètres de sécurité et prévention des risques

Lorsqu'un périphérique est connecté à un réseau, vous pouvez y accéder à distance. De plus, le périphérique peut être partagé entre plusieurs personnes pour rendre l'utilisation plus pratique et améliorer la productivité. Toutefois, ce mode d'utilisation augmente les risques d'accès non autorisé, d'utilisation abusive et de piratage des données. Si vous utilisez le périphérique dans un environnement doté d'un accès Internet, les risques sont encore plus importants.

Pour prévenir ces risques, les périphériques Epson sont dotées de plusieurs technologies de sécurité.

Paramétrez le périphérique selon les besoins en fonction des conditions de l'environnement du client.

Nom	Type de fonction	Que définir	Risques à éviter
Communication SSL/TLS	Le chemin de communication d'un ordinateur et d'un périphérique est chiffré par SSL/TLS. Le contenu d'une communication passant par un navigateur est protégé.	Définissez un certificat CA pour le serveur détenteur d'un certificat signé par une autorité de certification pour le périphérique.	Évitez les fuites d'informations de paramétrage et de contenu des données transférées entre l'ordinateur et le scanner. L'accès au serveur Epson sur Internet depuis le périphérique peut également être protégé par une mise à jour du microprogramme, etc.
Filtrage IPsec/IP	Vous pouvez paramétrer le blocage des données provenant d'un certain client ou d'un type particulier. Du fait que IPsec protège les données par unité de paquet IP (chiffrement et authentification), vous pouvez communiquer de manière sécurisée un protocole de numérisation non protégé.	Créez une politique de base et une politique individuelle pour définir les clients ou types de données autorisés à accéder au périphérique.	Prévenez les accès non autorisés ainsi que le piratage et l'interception des données de communication à destination du périphérique.
SNMPv3	Des fonctionnalités ont été ajoutées, telles que la surveillance des périphériques connectés du réseau, intégrité des données vers le protocole SNMP à contrôler, chiffrement, authentification utilisateur, etc.	Activez SNMPv3 puis définissez la méthode d'authentification et de chiffrement.	Protégez les paramètres de modification via le réseau, la confidentialité de la surveillance du statut.

Nom	Type de fonction	Que définir	Risques à éviter
IEEE802.1X	Autorisez seulement les utilisateurs authentifiés en Ethernet à se connecter. Permettez uniquement aux utilisateurs autorisés d'utiliser le périphérique.	Paramètre d'authentification auprès du serveur RADIUS (serveur d'authentification).	Évitez les accès et utilisation non autorisés du périphérique.
Lecture d'une carte d'identité	Vous pouvez utiliser le périphérique en passant une carte d'identité sur le périphérique d'identification connecté. Vous pouvez limiter l'acquisition de journaux pour chaque utilisateur et périphérique et limiter l'utilisation possible des périphériques ainsi que les fonctionnalités disponibles de chaque utilisateur et groupe.	Connectez un appareil d'authentification au périphérique puis entrez-y les informations des utilisateurs.	Empêchez l'utilisation non autorisée et l'usurpation du périphérique.

Informations connexes

➡ « Communication SSL/TLS avec le scanner » à la page 64
➡ « Communication chiffrée par filtrage IPsec/IP » à la page 72
➡ « Utilisation du protocole SNMPv3 » à la page 84
➡ « Connexion du scanner à un réseau IEEE802.1X » à la page 86

Paramètres des fonctions de sécurité

Lorsque vous définissez le filtrage IPsec/IP ou IEEE802.1X, il est conseillé d'accéder à Web Config via SSL/TLS pour communiquer les informations de paramétrage afin de limiter les risques de sécurité tels que le piratage et l'interception.

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.

À propos de la certification numérique

❏ Certificat signé par une autorité de certification

Un certificat signé par une autorité de certification doit être obtenu auprès d'une autorité de certification. Vous pouvez sécuriser les communications en utilisant un certificat signé par une autorité de certification. Vous pouvez utiliser un certificat signé par une autorité de certification pour chaque fonctionnalité de sécurité.

❏ Certificat d'une autorité de certification

Le certificat d'une autorité de certification indique qu'un tiers a vérifié l'identité du serveur. Il s'agit d'un composant essentiel d'une sécurité de type WOT (toile de confiance). Vous devez obtenir un certificat pour l'authentification du serveur auprès d'une autorité de certification qui émet de tels certificats.

❏ Certificat à signature automatique

Le certificat à signature automatique est un certificat que le scanner émet et signe lui-même. Ce certificat n'est pas fiable et ne permet pas d'éviter l'usurpation d'identité. Si vous utilisez ce certificat en guise de certificat SSL/TLS, il est possible qu'une alerte de sécurité s'affiche au niveau du navigateur. Vous pouvez uniquement utiliser ce certificat pour les communications SSL/TLS.

Informations connexes

➡ « Obtention et importation d'un certificat signé par une autorité de certification » à la page 65

➡ « Suppression d'un certificat signé par une autorité de certification » à la page 69

➡ « Mise à jour d'un certificat à signature automatique » à la page 69

Obtention et importation d'un certificat signé par une autorité de certification

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, et sélectionnez **Paramètres de sécurité réseau**. Sélectionnez ensuite **SSL/TLS** > **Certificat** ou **IPsec/filtrage IP** > **Certificat client** ou **IEEE802.1X** > **Certificat client**.

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 **Paramètres de 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 pas 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.

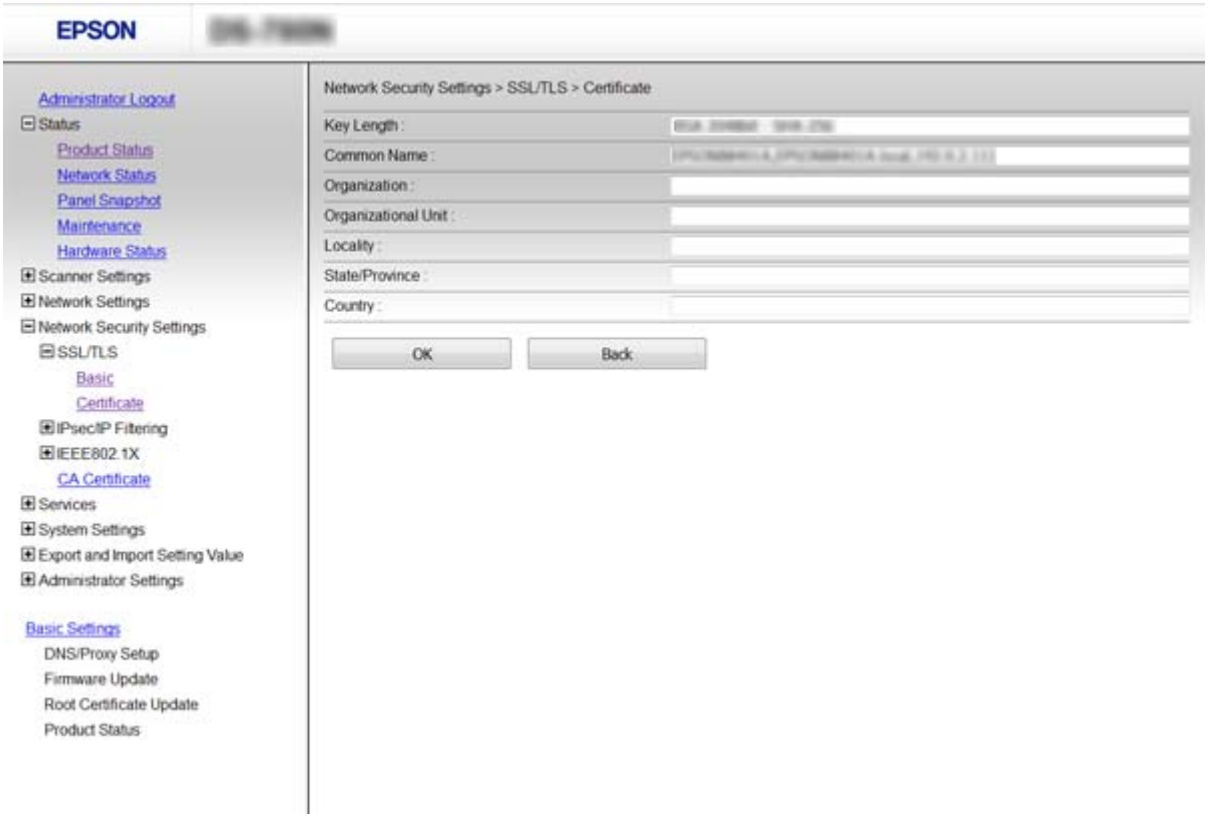
Informations connexes

➡ « Accès au logiciel Web Config » à la page 23

➡ « Éléments de paramétrage de la demande de signature de certificat » à la page 66

➡ « Importation d'un certificat signé par une autorité de certification » à la page 67

Éléments de paramétrage de la demande de signature de certificat



Éléments	Paramètres et explication
Longueur de la clé	Sélectionnez une longueur de clé pour la demande de signature de certificat.

Éléments	Paramètres et explication
Nom commun	Vous pouvez saisir de 1 à 128 caractères. S'il s'agit d'une adresse IP, cela doit être une adresse IP statique. Exemple : Adresse URL pour accéder au logiciel Web Config : https://10.152.12.225 Nom commun : 10.152.12.225
Organisation/ Unité organisationnelle/ Localité/ État / Province	Vous pouvez saisir entre 0 et 64 caractères au format ASCII (0x20–0x7E). Vous pouvez diviser les noms uniques par des virgules.
Pays	Saisissez le code de pays sous la forme d'un numéro à deux chiffres comme indiqué dans la norme ISO-3166.

Informations connexes

➡ « Obtention d'un certificat signé par une autorité de certification » à la page 65

Importation d'un certificat signé par une autorité de certification

Important:

❏ *Assurez-vous que la date et l'heure du scanner sont correctement définies.*

❏ *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 et sélectionnez **Paramètres de 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.

   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 configurez pas cette option.

      ❏ **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 configurez pas cette option.

      ❏ **Certificat CA 1/Certificat CA 2** : en option

❏ Certificat au format PKCS#12 obtenu à partir d'un ordinateur

❏ **Clé privée** : ne configurez pas cette option.

❏ **Mot de passe** : en option

❏ **Certificat CA 1/Certificat CA 2** : ne configurez pas cette option.

4. Cliquez sur **OK**.

   Un message de finalisation s'affiche.

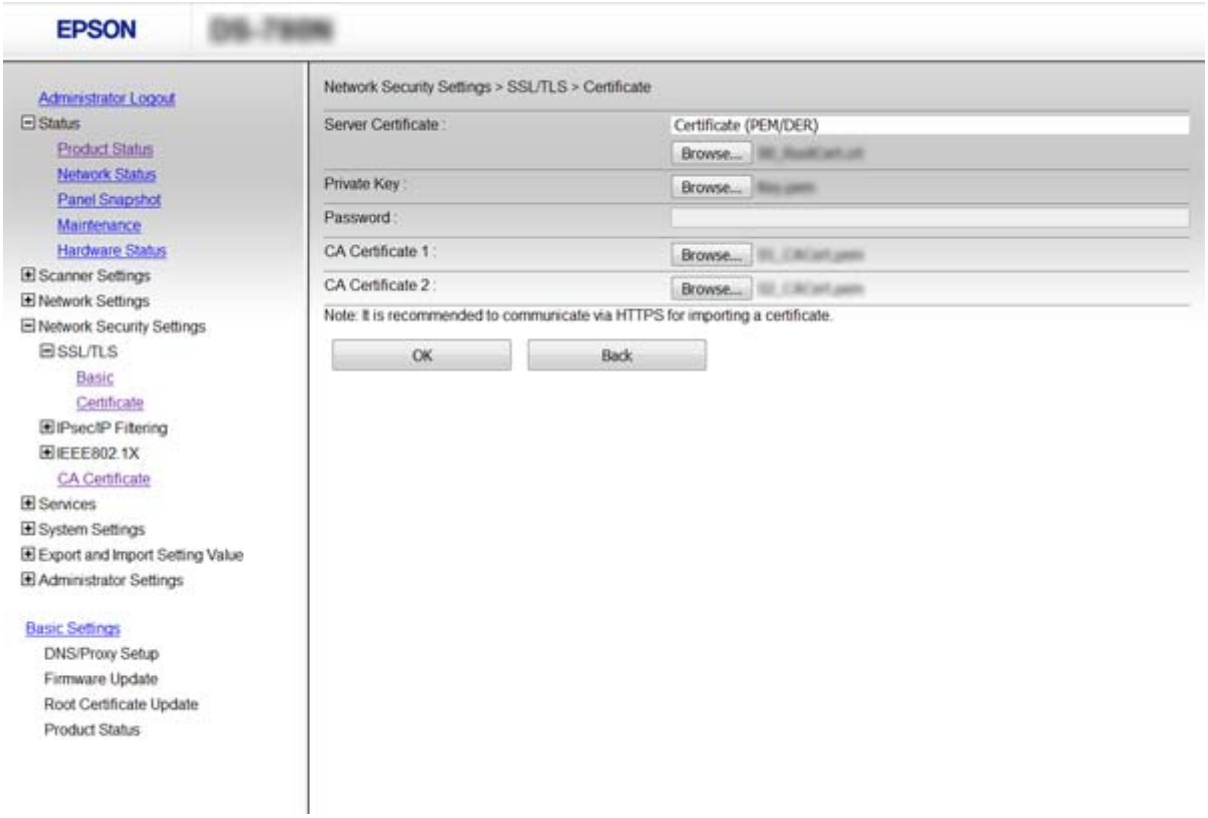
Remarque:
Cliquez sur ***Confirmer*** *pour vérifier les informations du certificat.*

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23

➡ « Éléments de paramétrage pour l'importation d'un certificat signé par une autorité de certification » à la page 68

Éléments de paramétrage pour l'importation d'un certificat signé par une autorité de certification



Éléments	Paramètres et explications
Certificat de serveur ou Certificat client	Sélectionnez le format du certificat.
Clé privée	Si vous obtenez un certificat au format PEM/DER à l'aide d'une demande de signature de certificat créée à partir d'un ordinateur, sélectionnez un fichier de clé privée qui correspond au certificat.

Éléments	Paramètres et explications
Mot de passe	Saisissez le mot de passe de chiffrement de la clé privée.
Certificat CA 1	Si le format de certificat est **Certificat (PEM / DER)**, importez le certificat d'une autorité de certification qui émet un certificat de serveur. Sélectionnez un fichier si nécessaire.
Certificat CA 2	Si le format de certificat est **Certificat (PEM / DER)**, importez le certificat d'une autorité de certification qui émet un certificat **Certificat CA 1**. Sélectionnez un fichier si nécessaire.

Informations connexes

➡ « Importation d'un certificat signé par une autorité de certification » à la page 67

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 Web Config et sélectionnez **Paramètres de 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

➡ « Accès au logiciel Web Config » à la page 23

Mise à jour d'un certificat à signature automatique

Si le scanner gère la fonctionnalité de serveur HTTPS, vous pouvez mettre à jour les certificats à signature automatique. Un message d'avertissement s'affiche lors de l'accès au logiciel Web Config à l'aide d'un certificat à signature automatique.

Utilisez un certificat à signature automatique de manière temporaire, jusqu'à obtention et importation d'un certificat signé par l'autorité de certification.

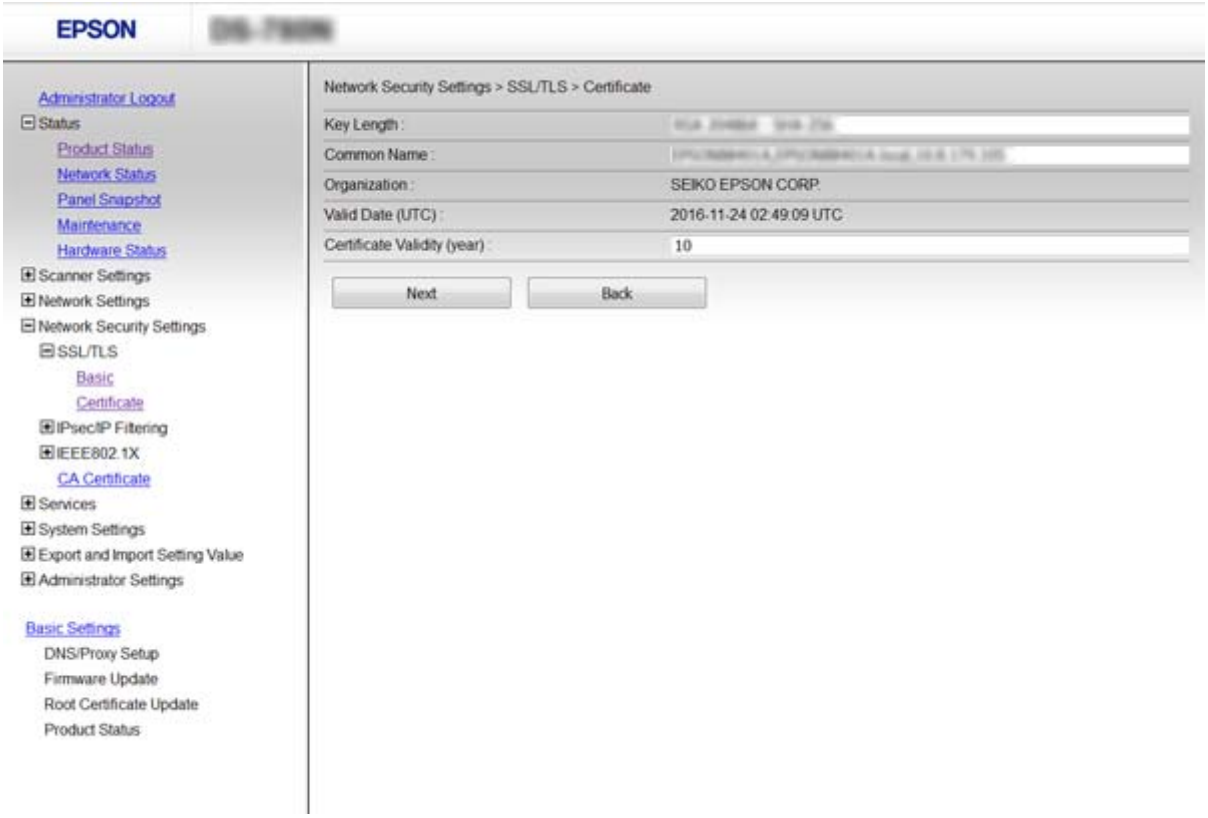
1. Accédez à Web Config et sélectionnez **Paramètres de sécurité réseau** > **SSL/TLS** > **Certificat**.
2. Cliquez sur **Mettre à jour**.

3. Saisissez le paramètre **Nom commun**.

   Saisissez une adresse IP ou un identifiant tel qu'un nom de domaine complet du scanner. Vous pouvez saisir de 1 à 128 caractères.

   Remarque:
   Vous pouvez séparer les noms uniques (CN) par des virgules.

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

Informations connexes

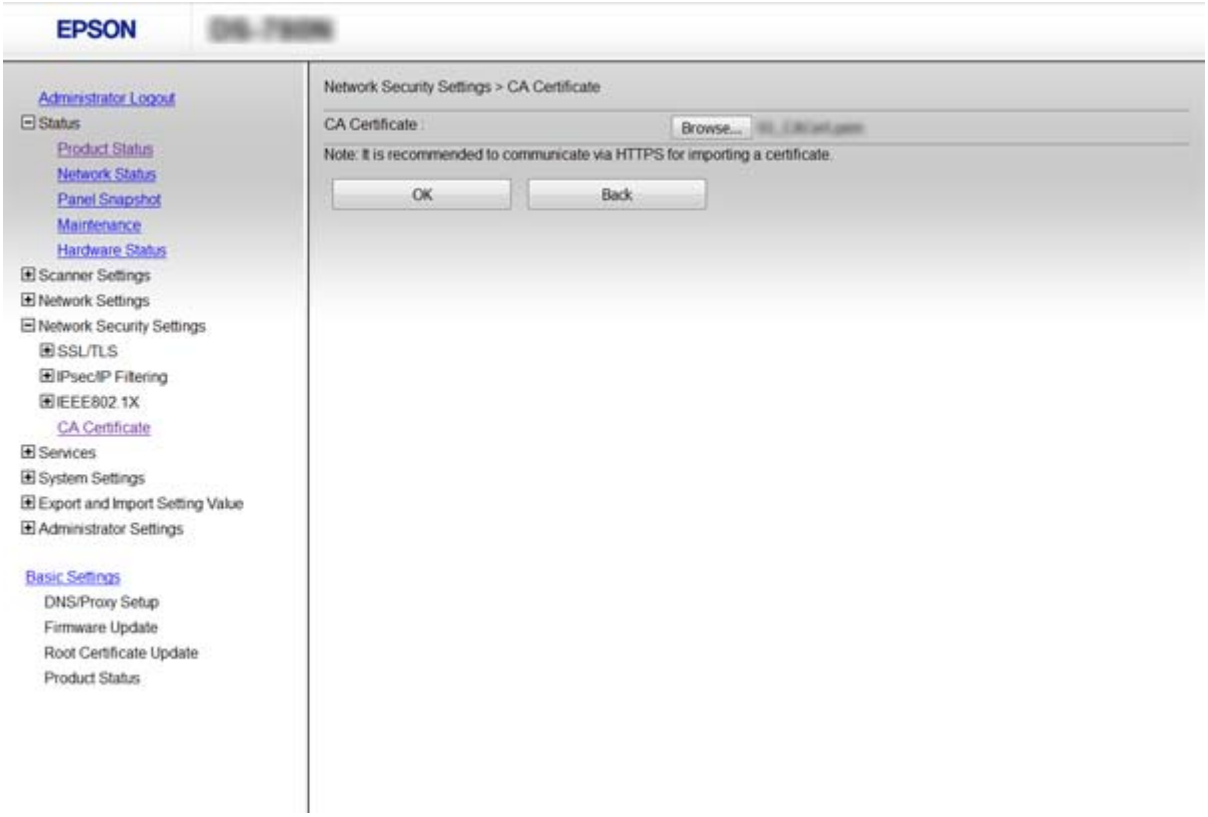
➡ « Accès au logiciel Web Config » à la page 23

Configurer la fonctionnalité Certificat CA

Vous pouvez importer, afficher ou supprimer un Certificat CA.

Importer un Certificat CA

1. Accédez à Web Config, et sélectionnez **Paramètres de sécurité réseau** > **Certificat CA**.
2. Cliquez sur **Importer**.
3. Spécifiez le Certificat CA que vous souhaitez importer.



4. Cliquez sur **OK**.

Une fois l'importation terminée, vous revenez à l'écran **Certificat CA** et le Certificat CA s'affiche.

Informations connexes

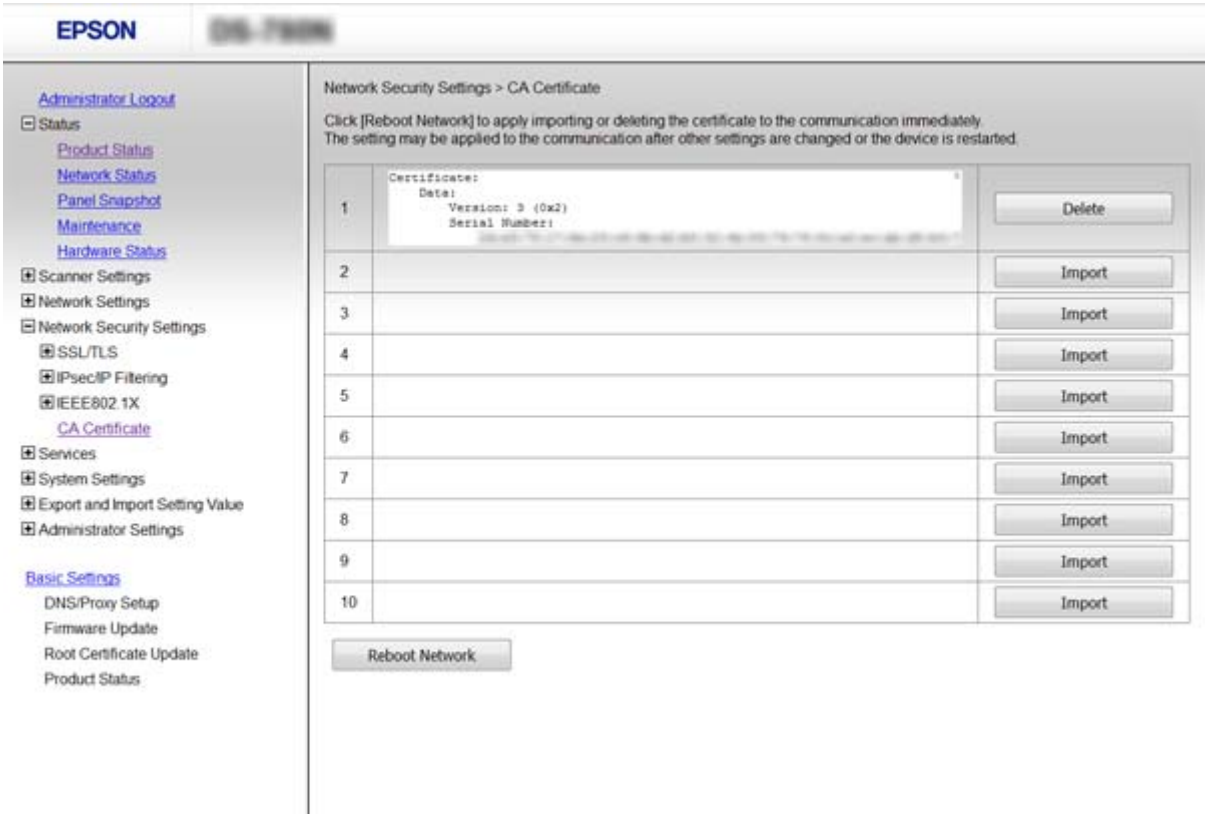
➡ « Accès au logiciel Web Config » à la page 23

Supprimer un Certificat CA

Vous pouvez supprimer le Certificat CA importé.

1. Accédez à Web Config, et sélectionnez **Paramètres de sécurité réseau** > **Certificat CA**.

2. Cliquez sur **Supprimer** à côté du Certificat CA que vous souhaitez supprimer.



3. Confirmez que vous souhaitez supprimer le certificat dans le message qui s'affiche.

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23

Communication chiffrée par filtrage IPsec/IP

À propos d'IPsec/filtrage IP

Si le scanner prend en charge le filtrage IPsec/IP, vous pouvez filtrer le trafic en fonction des adresses IP, des services et du port. 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.

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. 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.

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

Configuration de Politique par défaut

1. Accédez à Web Config et sélectionnez **Paramètres de sécurité réseau** > **IPsec/filtrage IP** > **De base**.
2. Saisissez une valeur pour chaque élément.
3. Cliquez sur **Suivant**.

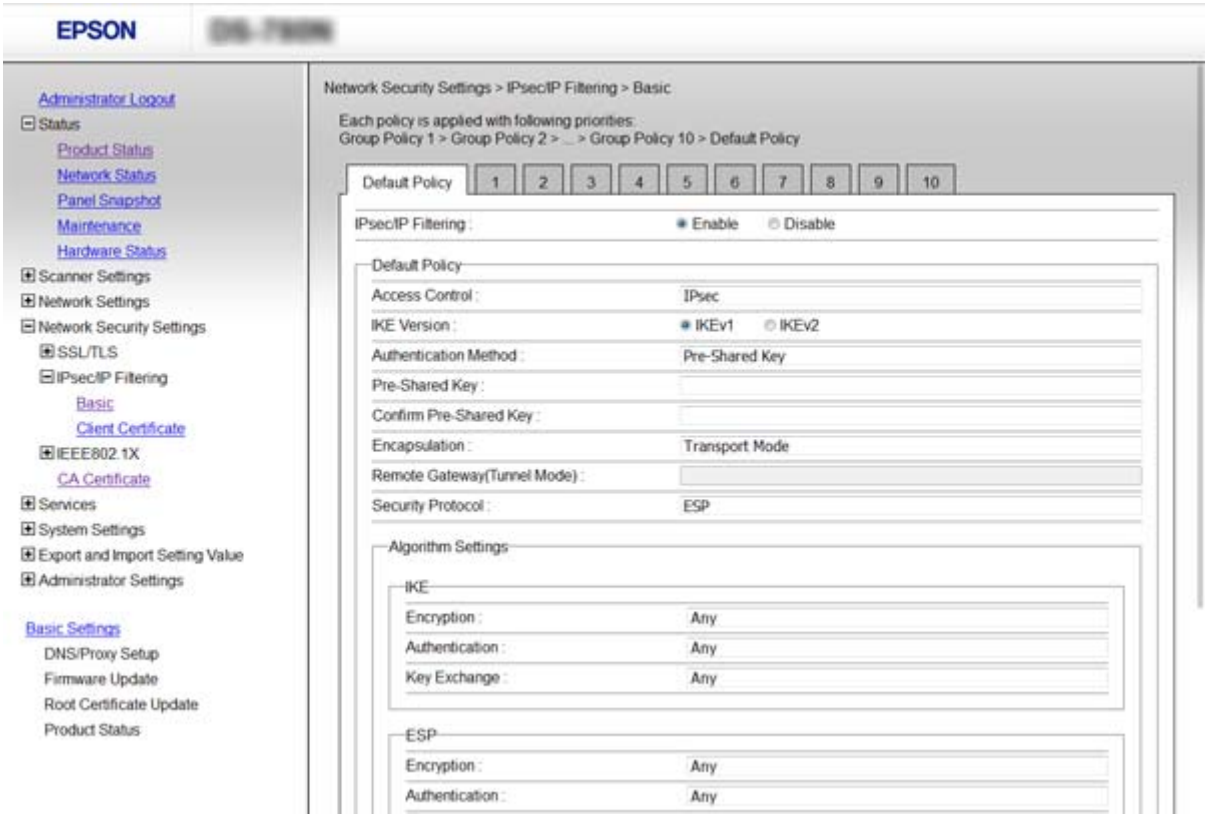
   Un message de confirmation s'affiche.
4. Cliquez sur **OK**.

   Le scanner est mis à jour.

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23
➡ « Éléments de paramétrage Politique par défaut » à la page 73

Éléments de paramétrage Politique par défaut



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

Paramètres de sécurité avancés pour les entreprises

Éléments	Paramètres et explication	
Contrôle des accès	Configurez la méthode de contrôle pour le trafic de paquets IP.	
	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	Pour la version de IKE, sélectionnez IKEv1 ou IKEv2. 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**.	
	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**.	
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	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 128 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 128 caractères ASCII sur 1 octet (0x20 à 0x7E). Vous devez inclure « @ ». **ID clé** : Saisissez de 1 à 128 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.

Paramètres de sécurité avancés pour les entreprises

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	Sélectionnez le type d'ID 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 128 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 128 caractères ASCII sur 1 octet (0x20 à 0x7E). Vous devez inclure « @ ». **ID clé** : Saisissez de 1 à 128 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.	
	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	**IPsec** pour **Contrôle des accès**, sélectionnez une option.	
	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 chiffrage des données est interdit.
Paramètres algorithme		

Paramètres de sécurité avancés pour les entreprises

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 **ESP** est sélectionné pour **Protocole de sécurité**.
	Authentification	Sélectionnez l'algorithme d'authentification pour ESP. Disponible lorsque **ESP** est sélectionné pour **Protocole de sécurité**.
AH	Authentification	Sélectionnez l'algorithme de chiffrement pour AH. Disponible lorsque **AH** est sélectionné pour **Protocole de sécurité**.

Informations connexes

➡ « Configuration de Politique par défaut » à la page 73

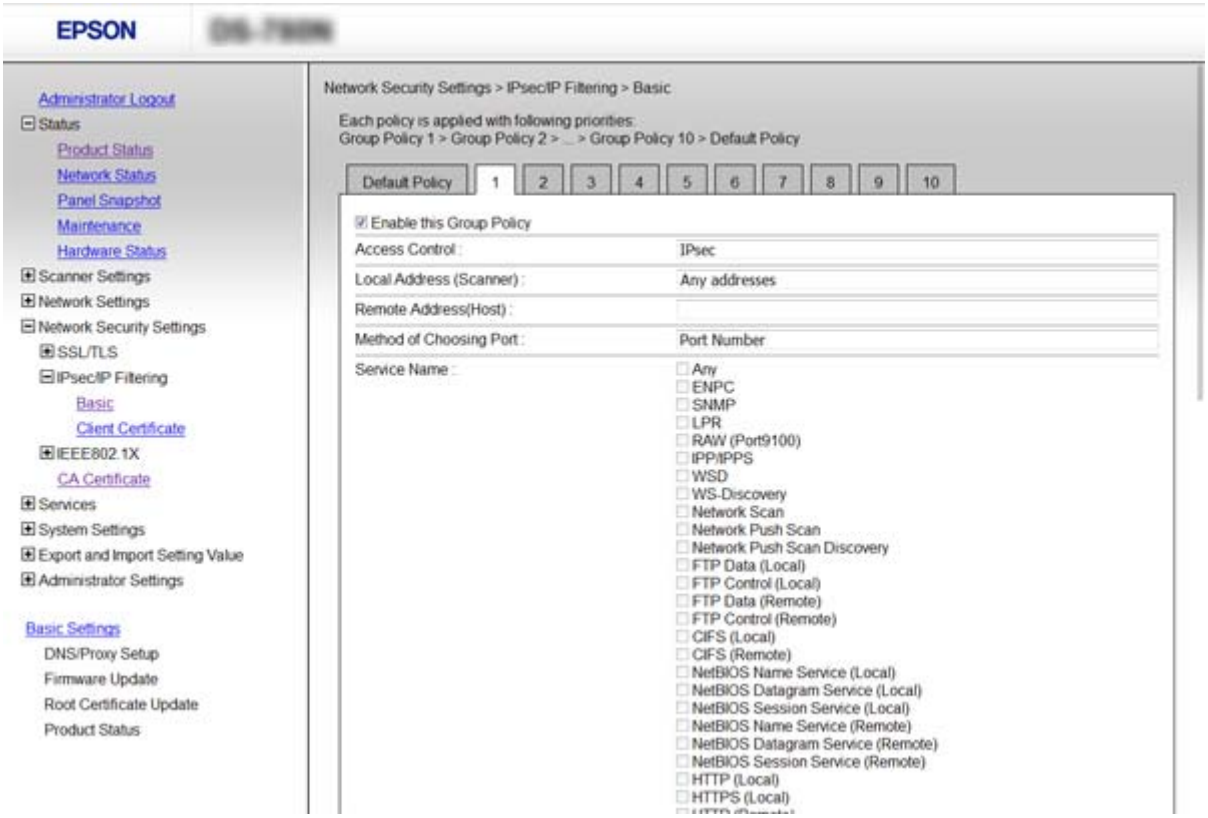
Configuration de Politique de groupe

1. Accédez à Web Config et sélectionnez **Paramètres de 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.

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23
➡ « Éléments de paramétrage Politique de groupe » à la page 77

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.	
	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**.	
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.	

Paramètres de sécurité avancés pour les entreprises

Éléments	Paramètres et explication	
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.	
	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	Pour la version de IKE, sélectionnez IKEv1 ou IKEv2. 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**.	
	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**.	

Paramètres de sécurité avancés pour les entreprises

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	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 128 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 128 caractères ASCII sur 1 octet (0x20 à 0x7E). Vous devez inclure « @ ». **ID clé** : Saisissez de 1 à 128 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	Sélectionnez le type d'ID 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 128 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 128 caractères ASCII sur 1 octet (0x20 à 0x7E). Vous devez inclure « @ ». **ID clé** : Saisissez de 1 à 128 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.

Paramètres de sécurité avancés pour les entreprises

Éléments	Paramètres et explication	
Encapsulation	Si vous sélectionnez l'option **IPsec** pour le paramètre **Contrôle des accès**, vous devez configurer un mode d'encapsulation.	
	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.	
	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 chiffrage des données est interdit.
Paramètres algorithme		
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 **ESP** est sélectionné pour **Protocole de sécurité**.
	Authentification	Sélectionnez l'algorithme d'authentification pour ESP. Disponible lorsque **ESP** est sélectionné pour **Protocole de sécurité**.
AH	Authentification	Sélectionnez l'algorithme d'authentification pour AH. Disponible lorsque **AH** est sélectionné pour **Protocole de sécurité**.

Informations connexes

➡ « Configuration de Politique de groupe » à la page 76

➡ « Combinaison de Adresse locale (scanner) et Adresse distante (hôte) sur une Politique de groupe » à la page 81

➡ « Références du nom de service et de la politique de groupe » à la page 81

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.

Références du nom de service et de la politique de groupe

Remarque:
Les services indisponibles sont affichés mais ne peuvent être sélectionnés.

Nom de service	Type de protocole	Numéro de port local	Numéro de port distant	Fonctions contrôlées
N'importe lequel	–	–	–	Tous les services
ENPC	UDP	3289	Tous les ports	Recherche d'un scanner à partir d'applications telles que EpsonNet Config et d'un pilote de scanner
SNMP	UDP	161	Tous les ports	Acquisition et configuration de MIB à partir d'applications telles que EpsonNet Config et le pilote de scanner Epson
WSD	TCP	Tous les ports	5357	Contrôle WSD
WS-Discovery	UDP	3702	Tous les ports	Recherche d'un scanner depuis WSD
Network Scan	TCP	1865	Tous les ports	Transfert de données numérisées depuis Document Capture Pro
Network Push Scan Discovery	UDP	2968	Tous les ports	Recherchez un ordinateur à partir du scanner.
Network Push Scan	TCP	Tous les ports	2968	Acquisition d'informations relatives à un travail de tâche de numérisation poussée depuis Document Capture Pro ou Document Capture
HTTP (local)	TCP	80	Tous les ports	Serveur HTTP(S) (transfert des données de Web Config et WSD)
HTTPS (local)	TCP	443	Tous les ports	

Nom de service	Type de protocole	Numéro de port local	Numéro de port distant	Fonctions contrôlées
HTTP (distant)	TCP	Tous les ports	80	Client HTTP(S) (communique entre mise à jour du microprogramme et mise à jour du certificat racine)
HTTPS (distant)	TCP	Tous les ports	443	

Exemples de configuration de la fonctionnalité IPsec/filtrage IP

Réception de paquets IPsec uniquement

Cet exemple illustre la configuration d'une politique par défaut.

Politique par défaut :

❏ **IPsec/filtrage IP**: **Activer**

❏ **Contrôle des accès**: **IPsec**

❏ **Méthode d'authentification**: **Clé pré-partagée**

❏ **Clé pré-partagée** : Saisissez un maximum de 127 caractères.

Politique de groupe :

Ne configurez pas cette option.

Acceptation de la numérisation à l'aide de Epson Scan 2 et des paramètres de numérisation

Cet exemple autorise la communication des données de numérisation et de la configuration du scanner depuis les services indiqués.

Politique par défaut :

❏ **IPsec/filtrage IP**: **Activer**

❏ **Contrôle des accès**: **Refuser l'accès**

Politique de groupe :

❏ **Activer cette politique de groupe** : Cochez 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** : Cochez la case de **ENPC**, **SNMP**, **Network Scan**, **HTTP (local)** et **HTTPS (local)**.

Réception de l'accès uniquement à partir d'une adresse IP précisée

Cet exemple permet à l'adresse IP indiquée 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** : Cochez la case.

❏ **Contrôle des accès**: **Autoriser l'accès**

❏ **Adresse distante (hôte)** : Adresse IP d'un client administrateur

Remarque:
Le client peut accéder au scanner et le configurer, quelle que soit la configuration de la politique.

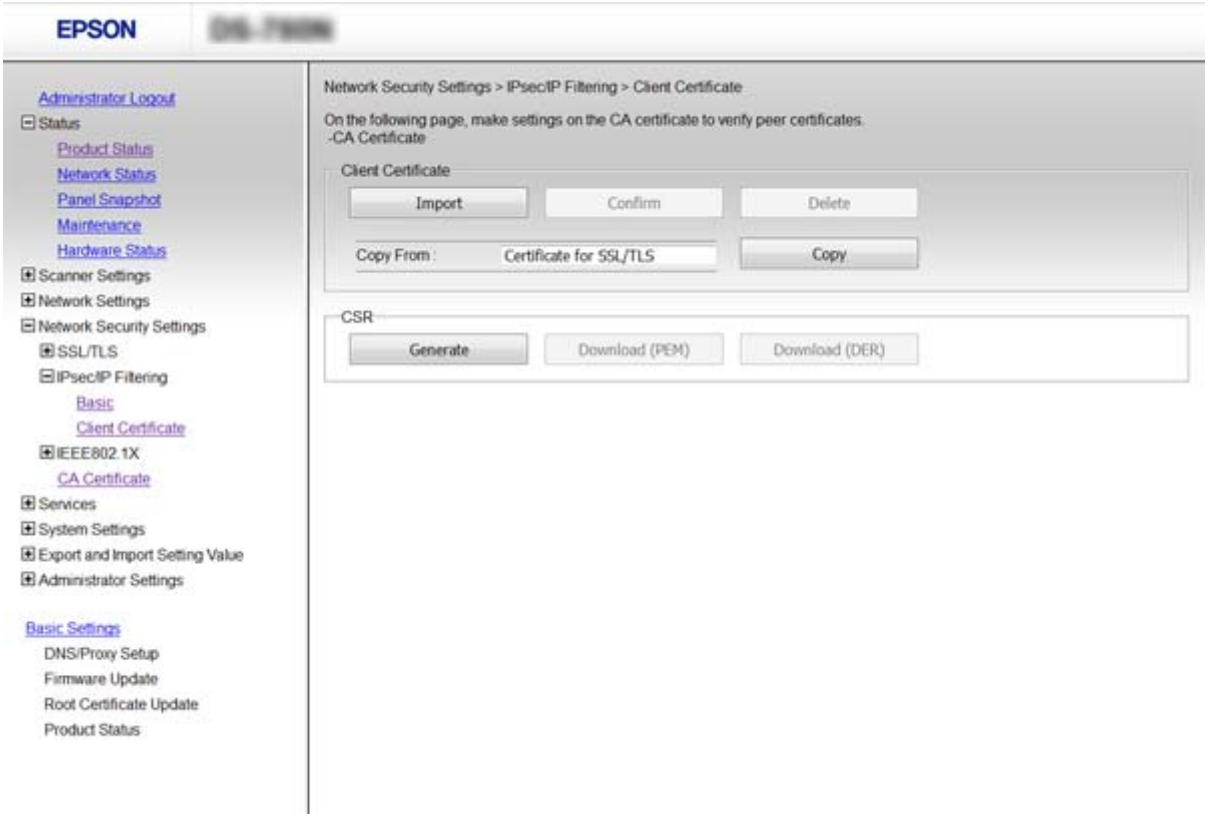
Configuration d'un certificat pour la fonctionnalité IPsec/filtrage IP

Configurez le certificat client pour le filtrage IPsec/IP. Si vous souhaitez configurer l'autorité de certification, allez dans **Certificat CA**.

1. Accédez à Web Config et sélectionnez **Paramètres de sécurité réseau** > **IPsec/filtrage IP** > **Certificat client**.

2. Importez le certificat **Certificat client**.

   Si vous avez déjà importé un certificat publié par une autorité de certification dans IEEE802.1X ou SSL/TLS, vous pouvez copier le certificat et l'utiliser dans le filtrage IPsec/IP. Pour copier, sélectionnez le certificat dans **Copier de**, puis cliquez sur **Copier**.



Informations connexes

➡ « Accès au logiciel Web Config » à la page 23

➡ « Obtention et importation d'un certificat signé par une autorité de certification » à la page 65

Utilisation du protocole SNMPv3

À propos de SNMPv3

SNMP est un protocole qui assure une fonction de surveillance et de contrôle pour collecter les informations des appareils connectés au réseau. SNMPv3 est la version étendue de la fonction de sécurité de gestion.

Avec SNMPv3, les modifications apportées à la surveillance de l'état et aux paramètres de la communication SNMP (paquet) peuvent être authentifiées et chiffrées de manière à protéger la communication SNMP (paquet) des risques inhérents au réseau, tels que l'interception des transmissions, l'usurpation d'identité et le piratage.

Configuration de SNMPv3

Si le scanner gère le protocole SNMPv3, vous pouvez surveiller et contrôler les accès au scanner.

1. Accédez à Web Config et sélectionnez **Services** > **Protocole**.
2. Saisissez une valeur pour chaque élément de **Param SNMPv3**.
3. Cliquez sur **Suivant**.

   Un message de confirmation s'affiche.
4. Cliquez sur **OK**.

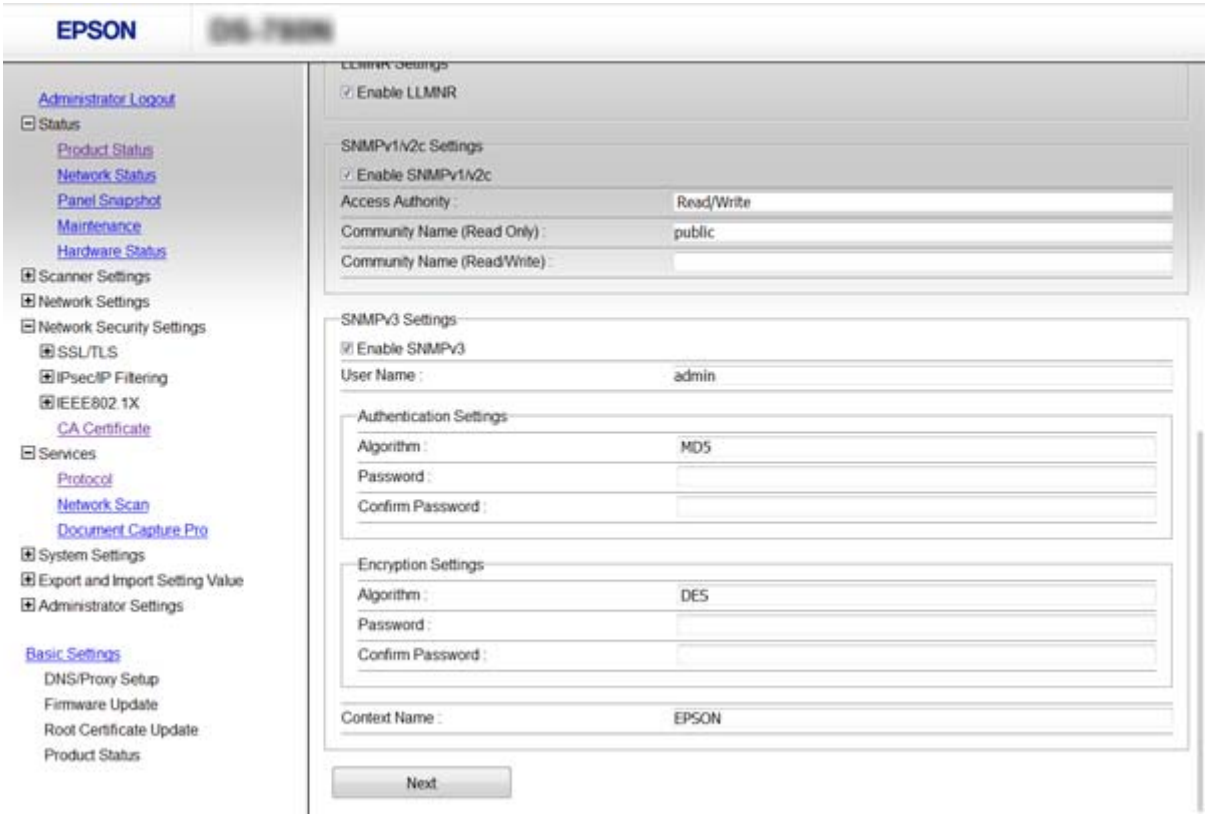
   Le scanner est mis à jour.

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23

➡ « Éléments de paramétrage SNMPv3 » à la page 85

Éléments de paramétrage SNMPv3



Éléments	Paramètres et explications
Activer SNMPv3	Le protocole SNMPv3 est activé lorsque la case à cocher est sélectionnée.
Nom d'utilisateur	Saisissez entre 1 et 32 caractères à un octet.
Param authentification	
Algorithme	Sélectionnez un algorithme d'authentification.
Mot de passe	Saisissez entre 8 et 32 caractères au format ASCII (0x20-0x7E).
Confirmer le mot de passe	Saisissez le mot de passe configuré pour confirmation.
Param cryptage	
Algorithme	Sélectionnez un algorithme de chiffrement.
Mot de passe	Saisissez entre 8 et 32 caractères au format ASCII (0x20-0x7E).
Confirmer le mot de passe	Saisissez le mot de passe configuré pour confirmation.
Nom contexte	Saisissez entre 1 et 32 caractères à un octet.

Informations connexes

➡ « Configuration de SNMPv3 » à la page 84

Connexion du scanner à un réseau IEEE802.1X

Configuration d'un réseau IEEE802.1X

Si le scanner gère le protocole IEEE802.1X, vous pouvez l'utiliser sur un réseau avec authentification connecté à un serveur RADIUS et un concentrateur en tant qu'authentifiant.

1. Accédez à Web Config et sélectionnez **Paramètres de sécurité réseau** > **IEEE802.1X** > **De base**.
2. Saisissez une valeur pour chaque élément.
3. Cliquez sur **Suivant**.

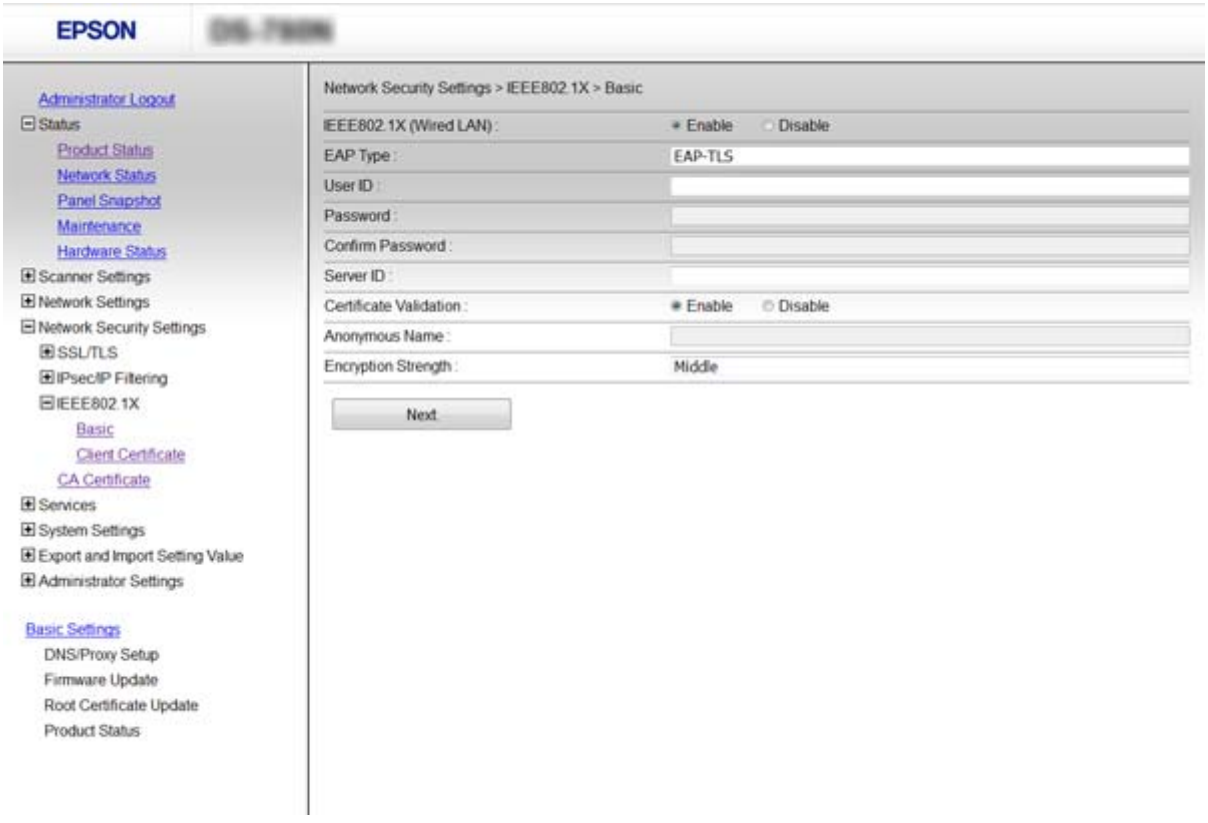
   Un message de confirmation s'affiche.
4. Cliquez sur **OK**.

   Le scanner est mis à jour.

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23
➡ « Éléments de paramétrage du réseau IEEE802.1X » à la page 86
➡ « Impossible d'accéder à l'imprimante ou au scanner après avoir configuré IEEE802.1X » à la page 91

Éléments de paramétrage du réseau IEEE802.1X



Paramètres de sécurité avancés pour les entreprises

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 câblé).	
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.
Identifiant utilisateur	Configurez un identifiant à utiliser pour l'authentification du serveur RADIUS. Saisissez de 1 à 128 caractères ASCII sur 1 octet (0x20 à 0x7E).	
Mot de passe	Configurez un mot de passe pour l'authentification du scanner. Saisissez de 1 à 128 caractères ASCII sur 1 octet (0x20 à 0x7E). Si vous utilisez un serveur Windows en tant que serveur RADIUS, vous pouvez saisir jusqu'à 127 caractères.	
Confirmer le mot de passe	Saisissez le mot de passe configuré pour confirmation.	
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	Vous pouvez définir la validation de certificat indépendamment de la méthode d'authentification. Importez le certificat **Certificat CA**.	
Nom anonyme	Si vous sélectionnez l'option **PEAP-TLS** ou **PEAP/MSCHAPv2** pour le paramètre **Méthode d'authentification**, vous pouvez configurer un nom anonyme à la place d'un identifiant utilisateur pour la phase 1 de l'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 réseau IEEE802.1X » à la page 86

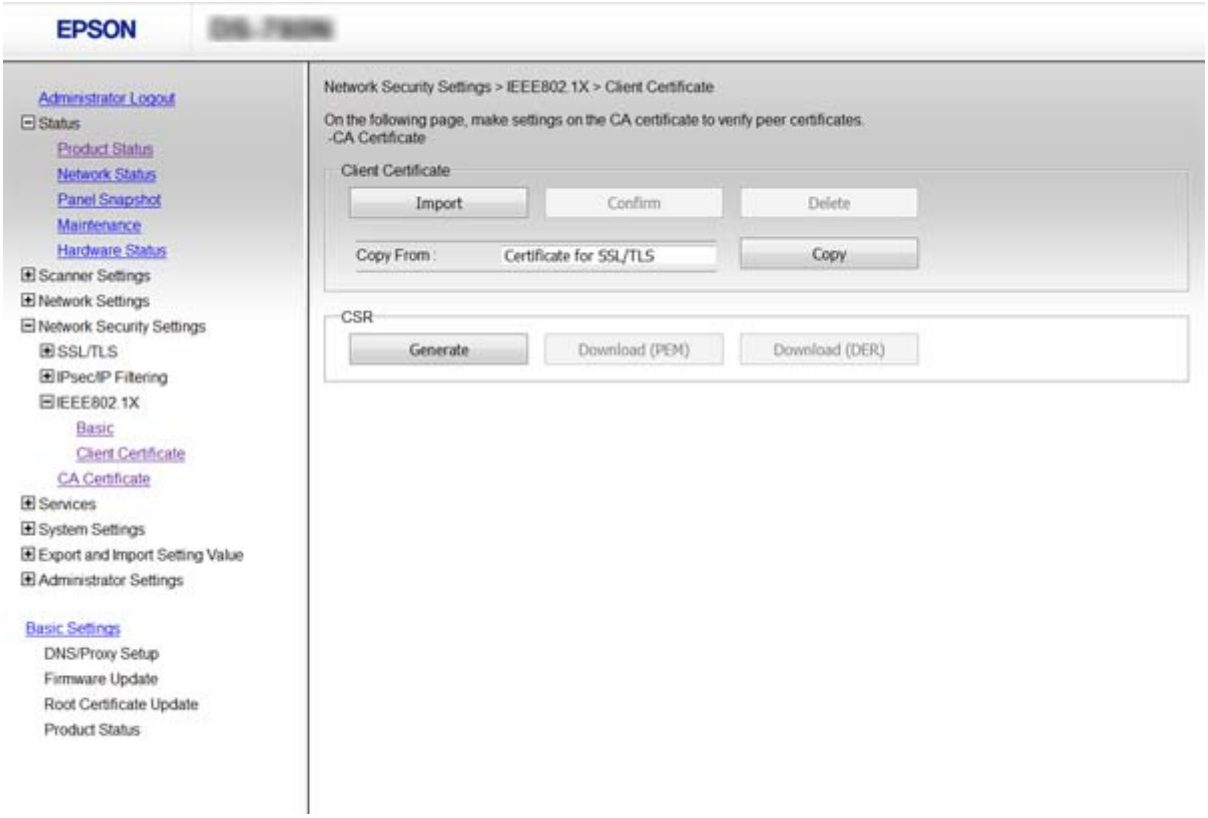
Configuration d'un certificat pour la fonctionnalité IEEE802.1X

Configurez le certificat client pour IEEE802.1X. Si vous souhaitez configurer le certificat de l'autorité de certification, allez dans **Certificat CA**.

1. Accédez à Web Config et sélectionnez **Paramètres de sécurité réseau** > **IEEE802.1X** > **Certificat client**.

2. Saisissez un certificat dans le **Certificat client**.

   Vous pouvez copier le certificat s'il est publié par une autorité de certification. Pour copier, sélectionnez le certificat dans **Copier de**, puis cliquez sur **Copier**.



Informations connexes

➡ « Accès au logiciel Web Config » à la page 23

➡ « Obtention et importation d'un certificat signé par une autorité de certification » à la page 65

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 ou IEEE802.1X, 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 du panneau de commande

Vous pouvez désactiver le filtrage IPsec/IP ou IEEE802.1X depuis le panneau de commande du scanner.

1. Appuyez sur **Param.** > **Paramètres réseau**.

2. Appuyez sur **Modifier les param.**.
3. Appuyez sur les éléments que vous souhaitez désactiver.
   - ❏ **IPsec/filtrage IP**
   - ❏ **IEEE802.1X**
4. Lorsqu'un message de finalisation s'affiche, appuyez sur **Continu**.

Restauration de la fonction de sécurité via Web Config

Avec IEEE802.1X, il est possible que les périphériques ne soient pas reconnus sur le réseau. Dans ce cas, désactivez la fonction à l'aide du panneau de commande du scanner.

Avec le filtrage IPsec/IP, vous pouvez désactiver la fonction si vous pouvez accéder au périphérique depuis l'ordinateur.

Désactivation du filtrage IPsec/IP à l'aide de Web Config

1. Accédez à Web Config et sélectionnez **Paramètres de sécurité réseau** > **IPsec/filtrage IP** > **De base**.
2. Sélectionnez **Désactiver** pour **IPsec/filtrage IP** dans **Politique par défaut**.
3. Cliquez sur **Suivant**, et décochez **Activer cette politique de groupe** pour toutes les politiques de groupe.
4. Cliquez sur **OK**.

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23

Problèmes lors de l'utilisation des fonctionnalités de sécurité réseau

Oubli de clé prépartagée

Configurez de nouveau la clé à l'aide du logiciel Web Config.

Pour modifier la clé, accédez à Web Config et sélectionnez **Paramètres de 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

➡ « Accès au logiciel Web Config » à la page 23

Communication avec le protocole IPsec impossible

Utilisez-vous un algorithme non pris en charge pour les paramètres de l'ordinateur ?

Le scanner prend en charge les algorithmes suivants.

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
Algorithme d'échange de clé IKE	Groupe DH 1, Groupe DH 2, Groupe DH 5, Groupe DH 14, Groupe DH 15, Groupe DH 16, Groupe DH 17, Groupe DH 18, Groupe DH 19, Groupe DH 20, Groupe DH 21, Groupe DH 22, Groupe DH 23, Groupe DH 24, Groupe DH 25, Groupe DH 26, Groupe DH 27*, Groupe DH 28*, Groupe DH 29*, Groupe DH 30*
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 72

Communication soudainement impossible

L'adresse IP du scanner est-elle incorrecte ou a-t-elle été modifiée ?

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 Web Config (**Paramètres de 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 est-elle incorrecte ou a-t-elle été modifiée ?

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 Web Config (**Paramètres de sécurité réseau** > **IPsec/filtrage IP** > **De base** > **Politique de groupe** > **Adresse distante (hôte)**) soit introuvable.

Utilisez une adresse IP statique.

Informations connexes

➡ « Accès au logiciel Web Config » à la page 23

➡ « Communication chiffrée par filtrage IPsec/IP » à la page 72

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

La valeur définie peut être incorrecte.

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 72

Impossible d'accéder à l'imprimante ou au scanner après avoir configuré IEEE802.1X

Les paramètres peuvent être incorrects.

Désactivez IEEE802.1X à partir du panneau de commande du scanner. Connectez le scanner et l'ordinateur et configurez à nouveau IEEE802.1X.

Informations connexes

➡ « Configuration d'un réseau IEEE802.1X » à la page 86

Problèmes lors de l'utilisation d'un certificat numérique

Importation d'un certificat signé par une autorité de certification impossible

Les informations du certificat signé par l'autorité de certification et de la demande de signature du certificat correspondent-elles ?

Si les informations du certificat signé par l'autorité de certification 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 par l'autorité de certification est-elle supérieure à 5 Ko ?

Vous ne pouvez pas importer un certificat signé par une autorité de certification dont la taille est supérieure à 5 Ko.

Le mot de passe d'importation du certificat est-il correct ?

Vous ne pouvez pas importer le certificat en cas d'oubli du mot de passe.

Informations connexes

➡ « Importation d'un certificat signé par une autorité de certification » à la page 67

Mise à jour d'un certificat à signature automatique impossible

Le paramètre Nom commun a-t-il été défini ?

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

Des caractères non pris en charge ont-ils été saisis pour la valeur Nom commun ? Le japonais, par exemple, n'est pas pris en charge.

Saisissez entre 1 et 128 caractères ASCII (0x20-0x7E) au format IPv4, IPv6, nom d'hôte ou FQDN.

La valeur définie pour le paramètre Nom commun inclut-elle une virgule ou un espace ?

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 69

Création d'une demande de signature de certificat impossible

Le paramètre Nom commun a-t-il été défini ?

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

Des caractères non pris en charge ont-ils été saisis pour la valeur Nom commun, Organisation, Unité organisationnelle, Localité, État / Province ? Le japonais, par exemple, n'est pas pris en charge.

Saisissez des caractères ASCII (0x20-0x7E) au format IPv4, IPv6, nom d'hôte ou FQDN.

La valeur définie pour le paramètre Nom commun inclut-elle une virgule ou un espace ?

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 65

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**.
Certificat CA 1 n'est pas entré.	**Cause :** Le certificat de l'autorité de certification 1 n'est pas saisi, seul le certificat de l'autorité de certification 2 est saisi. **Procédure à suivre :** Commencez par importer le certificat de l'autorité de certification 1.
Valeur invalide ci-dessous.	**Cause :** Le chemin d'accès au fichier et/ou le mot de passe incluent des caractères non pris en charge. **Procédure à suivre :** Vérifiez que les caractères sont correctement saisis pour l'élément.
Date et heure non valides.	**Cause :** La date et l'heure du scanner n'ont pas été définies. **Procédure à suivre :** Définissez la date et l'heure à l'aide du logiciel Web Config ou EpsonNet Config.
MdPasse non valide.	**Cause :** Le mot de passe défini pour le certificat de l'autorité de certification et le mot de passe saisi ne correspondent pas. **Procédure à suivre :** Saisissez le mot de passe correct.

Paramètres de sécurité avancés pour les entreprises

Messages	Cause/procédure à suivre
Fichier non valide.	**Cause :** Le fichier de certificat que vous importez n'est pas au format X509. **Procédure à suivre :** Veillez à sélectionner le certificat correct, envoyé par une autorité de certification digne de confiance.
	Cause : Le fichier importé est trop volumineux. La taille du fichier ne doit pas dépasser 5 Ko. **Procédure à suivre :** Si vous avez sélectionné le fichier correct, il est possible que le certificat soit corrompu ou contrefait.
	Cause : La chaîne incluse dans le certificat est incorrecte. **Procédure à suivre :** Pour plus d'informations au sujet du certificat, reportez-vous au site Web de l'autorité de certification.
Impossible d'utiliser les certificats de serveur qui incluent plus de trois certificats CA.	**Cause :** Le fichier de certificat au format PKCS#12 comprend plus de trois certificats d'autorités de certification. **Procédure à suivre :** 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.
Le certificat a expiré. Vérifiez que le certificat est valide ou vérifiez les date et heure sur le produit.	**Cause :** Le certificat n'est plus à jour. **Procédure à suivre :** ❏ Si le certificat n'est plus à jour, vous devez obtenir et importer un nouveau certificat. ❏ Si le certificat est à jour, vérifiez que la date et l'heure du scanner sont correctement réglées.

Messages	Cause/procédure à suivre
La clé privée est nécessaire.	**Cause :** Aucune clé privée n'est associée au certificat. **Procédure à suivre :** ❏ 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. ❏ 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.
	Cause : Vous avez réimporté le certificat PEM/DER obtenu à partir d'une demande de signature de certificat à l'aide du logiciel Web Config. **Procédure à suivre :** 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.
Échec de la configuration.	**Cause :** 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. **Procédure à suivre :** Une fois le fichier sélectionné et la communication vérifiés, importez de nouveau le fichier.

Informations connexes

➡ « À propos de la certification numérique » à la page 64

Suppression accidentelle d'un certificat signé par une autorité de certification

Existe-t-il un fichier de sauvegarde du certificat ?

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

➡ « Suppression d'un certificat signé par une autorité de certification » à la page 69

➡ « Importation d'un certificat signé par une autorité de certification » à la page 67