EPSON®

Guide de l'administrateur

Table des matières

Guide de l'administrateur

Bienvenue au *Guide de l'administrateur*.

Pour une version PDF imprimable de ce guide, cliquez ici.

Deux utilitaires sont à votre disposition pour configurer les paramètres réseau avancés de votre produit : Web Config et EpsonNet Config. Ce guide traite de l'utilitaire Web Config de façon détaillée; pour obtenir plus d'informations sur EpsonNet Config, consultez l'aide de l'utilitaire EpsonNet Config.

Les fonctions réseau disponibles varient selon le produit. (Les fonctions non disponibles ne sont pas affichées sur le panneau de commande du produit ou sur l'écran des paramètres du logiciel.) Les produits Epson prennent en charge les fonctions d'administration du système suivantes :

- Communication SSL/TLS : Utilise le protocole SSL/protocole TLS afin de chiffrer les communications et de prévenir la mystification (spoofing) entre le produit et un ordinateur.
- Filtrage d'adresse IP/Ipsec : Contrôle l'accès et sécurise les communications entre le produit et la passerelle de réseau.
- Contrôle individuel du protocole : Active et désactive les services simples.
- Activation et désactivation des connexions directes via USB.
- Importation et exportation des paramètres de l'imprimante : Transfère les paramètres d'un produit à l'autre.

Utilisation du logiciel de configuration réseau Web Config

Suivez les instructions dans ces sections pour configurer les paramètres d'administration réseau de votre produit à l'aide du logiciel Web Config.

À propos de Web Config

Web Config est une application par navigateur que vous pouvez utiliser pour configurer les paramètres d'un produit. Elle vous donne accès à des pages de paramètres de base et avancés.

Remarque: Avant de pouvoir configurer les paramètres d'administration du système, vous devez connecter le produit à un réseau. Consultez le *Guide de l'utilisateur* du produit pour des instructions à ce sujet.

Vous pouvez verrouiller les paramètres que vous choisissez avec le mot de passe administrateur pour votre produit. Consultez le *Guide de l'utilisateur* du produit pour des instructions à ce sujet.

Sujet parent: Utilisation du logiciel de configuration réseau Web Config

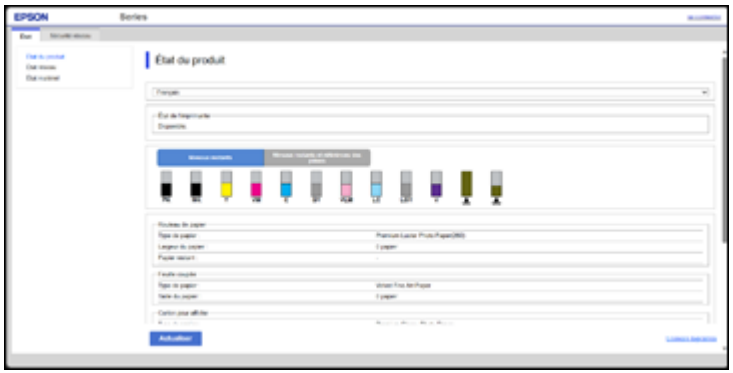
Accès à Web Config

Vous pouvez accéder à Web Config depuis votre navigateur via le protocole HTTP ou HTTPS.

Par défaut, le protocole HTTP sera utilisé la première fois que vous accéderez à Web Config. Si vous continuez d'utiliser le protocole HTTP, Web Config n'affichera pas tous les menus disponibles.

1. Imprimez une feuille d'état réseau afin de connaître l'adresse IP de votre produit. Consultez le *Guide de l'utilisateur* du produit pour des instructions à ce sujet.
2. Démarrez votre navigateur Web et assurez-vous que JavaScript est activé.
3. Entrez l'adresse IP de votre produit dans la barre d'adresse du navigateur comme suit, selon la version du protocole Internet que vous utilisez :
   - IPv4 : http://*adresse IP du produit*
   - IPv6 : http://[*adresse IP du produit*]/

La page d'état s'affiche :



4. Si un avertissement concernant le certificat auto-signé s'affiche, ignorez l'avertissement et accédez à l'adresse IP du produit. Consultez l'aide du navigateur pour obtenir des détails.

   Remarque: Vous pouvez désactiver les exigences HTTPS, mettre à jour le certificat auto-signé ou importer un certificat CA (certificat de l'autorité de certification) afin d'effacer le message d'avertissement. Consultez les liens ci-dessous pour obtenir plus d'informations.

Pour accéder à Web Config après avoir configuré le protocole HTTPS, entrez https:// avant l'adresse IP du produit, tel que décrit à l'étape 3.

Remarque: Si le nom du produit est enregistré sur le serveur DNS, vous pouvez utiliser ce nom au lieu de l'adresse IP du produit pour accéder à Web Config.

Sujet parent: Utilisation du logiciel de configuration réseau Web Config

Tâches associées

Configuration des paramètres SSL/TLS
Obtention et importation d'un certificat signé par l'AC
Mise à jour d'un certificat auto-signé

Limitation des fonctions disponibles aux utilisateurs

Suivez les instructions dans ces sections pour empêcher les utilisateurs d'avoir accès à certaines fonctions du produit en utilisant le mot de passe administrateur et le logiciel Web Config.

Sujet parent: Utilisation du logiciel de configuration réseau Web Config

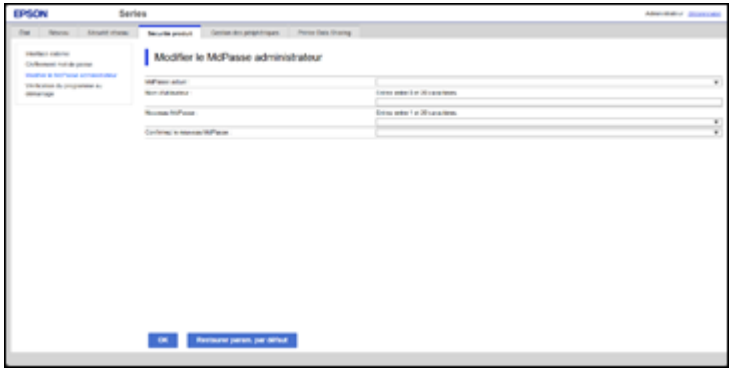
Modification du mot de passe administrateur dans Web Config

Vous pouvez modifier le mot de passe administrateur à l'aide du panneau de commande de votre produit, Web Config ou Epson Device Admin. Vous utiliserez le même mot de passe administrateur dans tous les cas.

Remarque: Consultez le *Guide de l'utilisateur* pour des instructions sur la façon de configurer un mot de passe administrateur à l'aide du panneau de commande. Si vous oubliez votre mot de passe administrateur, contactez le soutien Epson tel que décrit dans le *Guide de l'utilisateur* du produit.

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité du produit**.
2. Sélectionnez **Modifier le MdPasse administrateur**.

   Une fenêtre comme celle-ci s'affiche :



3. Entrez un nom d'utilisateur, si nécessaire.

4. Entrez le mot de passe actuel, puis entrez et confirmez le nouveau mot de passe dans les champs indiqués.

   Remarque: Le mot de passe par défaut est le numéro de série du produit. Pour trouver le numéro de série, consultez l'étiquette apposée à l'arrière de l'imprimante. Il n'y a pas de nom d'utilisateur entré par défaut.

5. Cliquez sur **OK**.

Sujet parent: Limitation des fonctions disponibles aux utilisateurs

Verrouillage des paramètres

Avec le mot de passe de l'administrateur, vous pouvez utiliser l'interface Web Config ou le panneau de commande pour éviter que des utilisateurs sans droits administratifs puissent modifier certains paramètres dans le menu des paramètres.

1. Accédez à Web Config et ouvrez une session en utilisant le nom et le mot de passe de l'administrateur.

   Remarque: Le mot de passe par défaut est le numéro de série du produit. Pour trouver le numéro de série, consultez l'étiquette apposée à l'arrière de l'imprimante. Il n'y a pas de nom d'utilisateur entré par défaut.

2. Sélectionnez **Gestion de l'appareil** > **Panneau de commande**.
3. Activez le paramètre **Verrouillage du panneau** et cliquez sur **OK**.

Si vous voulez désactiver le paramètre **Verrouiller le réglage** à partir du panneau de commande, touchez l'icône  dans le coin supérieur droit de l'écran d'accueil pour ouvrir une session en tant qu'administrateur. L'icône  ne s'affiche pas sur l'écran d'accueil lorsque le paramètre **Verrouiller le réglage** est désactivé.

Sujet parent: Limitation des fonctions disponibles aux utilisateurs

Désactivation de l'interface externe

Vous pouvez restreindre la fonctionnalité permettant d'imprimer via une connexion USB en désactivant le port USB.

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

2. Sélectionnez **PC Connexion via USB** et effectuez l'une des actions suivantes :
   - Sélectionnez **Désactiver** pour interdire les connexions USB.
   - Sélectionnez **Activer** pour permettre les connexions USB.
3. Cliquez sur **OK** pour sauvegarder vos paramètres.

Sujet parent: Limitation des fonctions disponibles aux utilisateurs

Mise à jour du micrologiciel à l'aide de Web Config

Si votre produit est connecté à Internet, vous pouvez mettre à jour le micrologiciel du produit à l'aide de Web Config.

1. Accédez à Web Config et sélectionnez **Gestion de l'appareil** > **Mise à jour du micrologiciel**.

   Une fenêtre comme celle-ci s'affiche :

2. Cliquez sur **Démarrer** pour rechercher la version la plus récente du micrologiciel.
3. S'il existe une nouvelle version du micrologiciel, cliquez sur **Démarrer** pour lancer la mise à jour.

   Remarque: Assurez-vous que le produit n'est pas en cours d'utilisation et effacez toute erreur à l'écran ACL avant de commencer la mise à jour.

Sujet parent: Utilisation du logiciel de configuration réseau Web Config

Utilisation de votre produit sur un réseau sécurisé

Suivez les instructions dans ces sections pour configurer les fonctions de sécurité de votre produit sur le réseau à l'aide du logiciel Web Config.

Chiffrement du mot de passe
Configuration des communications SSL/TLS
Configuration du protocole IPsec/du filtrage IP
Configuration des paramètres du protocole SNMPv3
Connexion du produit à un serveur IEEE 802.1X
Utilisation d'un certificat numérique
Configuration des protocoles sous Web Config

Sujet parent: Utilisation du logiciel de configuration réseau Web Config

Chiffrement du mot de passe

Vous pouvez configurer le chiffrement par mot de passe pour protéger les informations confidentielles stockées dans le produit.

1. Accédez à Web Config et ouvrez une session comme administrateur.
2. Sélectionnez **Sécurité du produit** > **Chiffrement du mot de passe**.
3. Sélectionnez **Activé** pour activer le chiffrement.
4. Cliquez sur **OK** pour sauvegarder vos paramètres.

Vous pouvez aussi activer le chiffrement du mot de passe sur le panneau de commande du produit ( Menu > **Paramètres généraux** > **Administration système** > **Param. de sécurité** > **Chiffrement du mot de passe**).

Sujet parent: Utilisation de votre produit sur un réseau sécurisé

Configuration des communications SSL/TLS

Suivez les instructions dans ces sections pour configurer les communications SSL/TLS à l'aide de Web Config.

Configuration des paramètres SSL/TLS
Configuration d'un certificat de serveur pour le produit

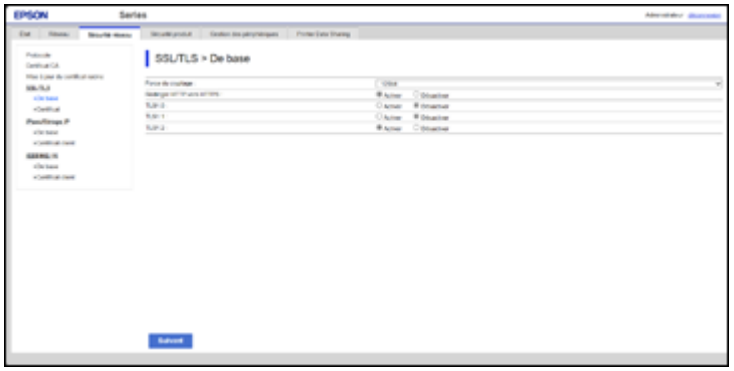
Sujet parent: Utilisation de votre produit sur un réseau sécurisé

Configuration des paramètres SSL/TLS

Si votre produit prend en charge le protocole HTTPS, vous pouvez configurer le protocole SSL/TLS pour chiffrer les communications avec votre produit.

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité du réseau**.
2. Sous **SSL/TLS**, sélectionnez **De base**.

   Une fenêtre comme celle-ci s'affiche :



3. Sélectionnez l'une des options au paramètre **Force du cryptage**.
4. Sélectionnez **Activer** ou **Désactiver** au paramètre **Rediriger HTTP vers HTTPS**, tel que nécessaire.
5. Cliquez sur **Suivant**.

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

Sujet parent: Configuration des communications SSL/TLS

Configuration d'un certificat de serveur pour le produit

Vous pouvez configurer un certificat de serveur pour votre produit.

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité du réseau**.
2. Sous **SSL/TLS**, sélectionnez **Certificat**.

Une fenêtre comme celle-ci s'affiche :

3. Sélectionnez l'une des options suivantes :
   - **Certificat signé CA** : Sélectionnez **Importer** si vous avez obtenu un certificat signé par l'AC (autorité de certification). Choisissez le fichier à importer et cliquez sur **OK**.
   - **Certificat auto-signé** : Sélectionnez **Mettre à jour** si vous n'avez pas obtenu un certificat signé par l'AC (autorité de certification) et que vous voulez que le produit génère un certificat auto-signé.
4. Cliquez sur **Suivant**.

   Un message de confirmation s'affichera.
5. Cliquez sur **OK**.

Sujet parent: Configuration des communications SSL/TLS

Configuration du protocole IPsec/du filtrage IP

Suivez les instructions dans ces sections pour configurer le protocole IPsec ou le filtrage IP à l'aide de Web Config.

À propos d'IPsec/du filtrage IP
Configuration d'une politique IPsec/filtrage IP par défaut
Configuration d'une politique de groupe IPsec/filtrage IP
Paramètres de la politique IPsec/de filtrage IP
Exemples de configuration de la fonction IPsec/filtrage IP
Configuration d'un certificat IPsec/de filtrage IP

Sujet parent: Utilisation de votre produit sur un réseau sécurisé

À propos d'IPsec/du filtrage IP

Vous pouvez filtrer le trafic acheminé au produit sur le réseau selon l'adresse IP, le service et le port en configurant une politique par défaut qui s'applique à tous les utilisateurs ou groupes connectés au produit. Pour contrôler des utilisateurs individuels ou des groupes d'utilisateurs spécifiques, vous pouvez configurer des politiques de groupe.

Remarque: IPsec est uniquement pris en charge par les ordinateurs sous Windows Vista ou une version plus récente, ou sous Windows Server 2008 ou une version plus récente.

Sujet parent: Configuration du protocole IPsec/du filtrage IP

Configuration d'une politique IPsec/filtrage IP par défaut

Vous pouvez configurer une politique IPsec/filtrage IP par défaut à l'aide de Web Config.

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité du réseau**.
2. Sous **IPsec/filtrage IP**, sélectionnez **De base**.

   Une fenêtre comme celle-ci s'affiche :

3. Sélectionnez **Activer** pour activer le protocole IPsec/filtrage IP.
4. Sélectionnez les options de filtrage que vous souhaitez utiliser pour la politique par défaut.
5. Cliquez sur **Suivant**.

   Un message de confirmation s'affichera.
6. Cliquez sur **OK**.

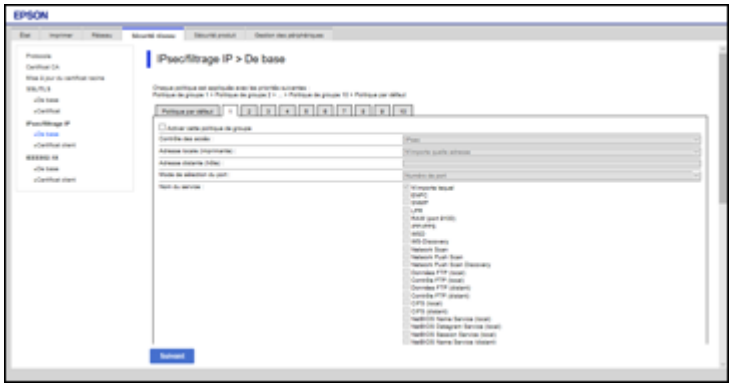
Sujet parent: Configuration du protocole IPsec/du filtrage IP

Configuration d'une politique de groupe IPsec/filtrage IP

Vous pouvez configurer une politique de groupe IPsec/filtrage IP à l'aide de Web Config.

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité du réseau**.
2. Sous **IPsec/filtrage IP**, sélectionnez **De base**.
3. Cliquez sur l'onglet numéroté de la politique que vous souhaitez configurer.

   Une fenêtre comme celle-ci apparaîtra :



4. Cochez la case **Activer cette politique de groupe**.
5. Sélectionnez les options de filtrage que vous souhaitez utiliser pour la politique de groupe.
6. Cliquez sur **Suivant**.

   Un message de confirmation s'affichera.
7. Cliquez sur **OK**.
8. Si vous souhaitez configurer des politiques de groupe additionnelles, cliquez sur le prochain onglet numéroté et répétez les étapes de configuration, si nécessaire.

Sujet parent: Configuration du protocole IPsec/du filtrage IP

Paramètres de la politique IPsec/de filtrage IP

Paramètres de la politique par défaut

Paramètre	Options/Description
Contrôle des accès	**Autoriser l'accès** : Choisissez cette option pour autoriser le passage des paquets IP. **Refuser l'accès** : Choisissez cette option pour refuser le passage des paquets IP. **IPsec** : Choisissez cette option pour autoriser le passage des paquets IPsec.
Version IKE	Sélectionnez la version du protocole Internet Key Exchange (IKE) qui correspond à votre environnement réseau.
Méthode d'authentification	Sélectionnez une méthode d'authentification, ou sélectionnez **Certificat** si vous avez importé un certificat signé par l'AC.
Clé pré-partagée	Si nécessaire, entrez une clé pré-partagée de 1 à 127 caractères.
Confirmer la clé pré-partagée	Confirmez la clé pré-partagée que vous avez entrée.
Type ID	Si vous avez sélectionné **IKEv2** au paramètre **Version IKE**, sélectionnez le type d'identification à partir de la liste.
ID	Si vous avez sélectionné **IKEv2** au paramètre **Version IKE**, entrez l'information d'identification nécessaire.
Encapsulation	Si vous avez sélectionné **IPsec** au paramètre **Contrôle des accès**, sélectionnez l'une de ces méthodes d'encapsulation : **Mode de transport** : Choisissez cette option si vous utilisez le produit sur le même LAN. Les paquets IP des couches 4 et supérieures seront chiffrés. **Mode de tunnel** : Choisissez cette option si vous utilisez le produit sur un réseau Internet tel qu'un réseau privé virtuel IPsec. L'en-tête et les données des paquets IP seront chiffrés.

Paramètre	Options/Description
Adresse de la passerelle à distance	Si vous avez sélectionné **Mode de tunnel** au paramètre **Encapsulation**, entrez une adresse de passerelle de 1 à 39 caractères.
Protocole de sécurité	Si vous avez sélectionné **IPsec** au paramètre **Contrôle des accès**, sélectionnez l'un de ces protocoles de sécurité : **ESP** : Choisissez cette option pour garantir l'intégrité de l'authentification et des données, et pour chiffrer les données. **AH** : Choisissez 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	Sélectionnez les paramètres de l'algorithme de chiffrement correspondant au protocole de sécurité sélectionné.

Paramètres de politique de groupe

Paramètre	Options/Description
Contrôle des accès	**Autoriser l'accès** : Choisissez cette option pour autoriser le passage des paquets IP. **Refuser l'accès** : Choisissez cette option pour refuser le passage des paquets IP. **IPsec** : Choisissez cette option pour autoriser le passage des paquets IPsec.
Adresse locale (imprimante)	Sélectionnez une adresse IPv4 ou IPv6 qui correspond avec votre environnement réseau; si l'adresse IP est automatiquement attribuée, sélectionnez **Utiliser l'adresse IPv4 obtenue automatiquement**; si l'adresse IP est automatiquement attribuée par IPv6, la connexion pourrait ne pas être disponible, veuillez plutôt configurer une adresse IPv6 statique.

Paramètre	Options/Description
Adresse distante (hôte)	Entrez l'adresse IP de l'appareil (entre 0 et 43 caractères) pour contrôler l'accès, ou laissez ce champ vide pour contrôler toutes les adresses. Si l'adresse IP est attribuée automatiquement, par exemple via DHCP, la connexion pourrait ne pas être disponible. Configurez plutôt une adresse statique.
Mode de sélection du port	Sélectionnez la méthode que vous souhaitez utiliser pour spécifier les ports.
Nom du service	Si vous avez sélectionné **Nom du service** au paramètre **Mode de sélection du port**, sélectionnez une option de nom de service. Consultez le tableau suivant pour plus d'informations.
Protocole de transport	Si vous avez sélectionné **Numéro de port** au paramètre **Mode de sélection du port**, sélectionnez l'une de ces méthodes d'encapsulation : **N'importe quel protocole** **TCP** **UDP** **ICMPv4** Consultez le tableau Directives pour les politiques de groupe pour plus d'informations.
Port local	Si vous avez sélectionné **Numéro de port** pour le paramètre **Mode de sélection du port**, et **TCP** ou **UDP** pour le paramètre **Protocole de transport**, entrez les numéros des ports qui contrôlent la réception des paquets (jusqu'à 10 ports), séparés par des virgules, par exemple **25,80,143,5220**. Laissez ce champ vide pour contrôler tous les ports. Consultez le tableau suivant pour plus d'informations.

Paramètre	Options/Description
Port distant	Si vous avez sélectionné **Numéro de port** pour le paramètre **Mode de sélection du port**, et **TCP** ou **UDP** pour le paramètre **Protocole de transport**, entrez les numéros des ports qui contrôlent l'envoi des paquets (jusqu'à 10 ports), séparés par des virgules, par exemple **25,80,143,5220**. Laissez ce champ vide pour contrôler tous les ports. Consultez le tableau suivant pour plus d'informations.
Version IKE	Sélectionnez **IKEv1** ou **IKEv2** selon l'appareil auquel le produit est connecté.
Méthode d'authentification	Si vous avez sélectionné **IPsec** au paramètre **Contrôle des accès**, sélectionnez une méthode d'authentification.
Clé pré-partagée	Si vous avez sélectionné **Clé pré-partagée** au paramètre **Méthode d'authentification**, entrez une clé pré-partagée de 1 à 127 caractères dans ce champ et dans le champ **Confirmer la clé pré-partagée**.
Type ID	Si vous avez sélectionné **IKEv2** au paramètre **Version IKE**, sélectionnez le type d'identification à partir de la liste.
ID	Si vous avez sélectionné **IKEv2** au paramètre **Version IKE**, entrez l'information d'identification nécessaire.
Encapsulation	Si vous avez sélectionné **IPsec** au paramètre **Contrôle des accès**, sélectionnez l'une de ces méthodes d'encapsulation : **Mode de transport** : Choisissez cette option si vous utilisez le produit sur le même LAN. Les paquets IP des couches 4 et supérieures seront chiffrés. **Mode de tunnel** : Choisissez cette option si vous utilisez le produit sur un réseau Internet tel qu'un réseau privé virtuel IPsec. L'en-tête et les données des paquets IP seront chiffrés.
Adresse de la passerelle à distance	Si vous avez sélectionné **Mode de tunnel** au paramètre **Encapsulation**, entrez une adresse de passerelle de 1 à 39 caractères.

Paramètre	Options/Description
Protocole de sécurité	Si vous avez sélectionné **IPsec** au paramètre **Contrôle des accès**, sélectionnez l'un de ces protocoles de sécurité : **ESP** : Choisissez cette option pour garantir l'intégrité de l'authentification et des données, et pour chiffrer les données. **AH** : Choisissez 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	Sélectionnez les paramètres de l'algorithme de chiffrement correspondant au protocole de sécurité sélectionné.

Directives pour les politiques de groupe

Nom du service	Type de protocole	Numéro de port local/distant	Fonctions contrôlées
N'importe lequel	—	—	Tous les services.
ENPC	UDP	3289/N'importe quel port	Recherche d'un produit depuis des applications telles que des pilotes d'imprimante ou de scanner, ou depuis EpsonNet Config.
SNMP	UDP	161/N'importe quel port	Acquisition et configuration du MIB depuis des applications telles que des pilotes d'imprimante ou de scanner, ou depuis EpsonNet Config.
LPR	TCP	515/N'importe quel port	Transfert des données LPR.
RAW (Port 9100)	TCP	9100/N'importe quel port	Transfert des données RAW.
IPP/IPPS	TCP	631/N'importe quel port	Transfert des données (impression IPP/IPPS).
WSD	TCP	N'importe quel port/5357	Contrôle du WSD.

Nom du service	Type de protocole	Numéro de port local/distant	Fonctions contrôlées
WS-Discovery	UDP	3702/N'importe quel port	Recherche d'un produit à partir du WSD.
Données FTP (local)	TCP	20/N'importe quel port	Transfert des données d'impression FTP au serveur FTP.
Contrôle FTP (local)	TCP	21/N'importe quel port	Contrôle de l'impression FTP sur un serveur FTP.
HTTP (local)	TCP	80/N'importe quel port	Transfert des données Web Config et WSD à un serveur HTTP ou HTTPS.
HTTPS (local)	TCP	443/N'importe quel port	
HTTP (distant)	TCP	N'importe quel port/80	Communication avec Epson Connect, une mise à jour du micrologiciel et une mise à jour du certificat racine sur un client HTTP ou HTTPS.
HTTPS (distant)	TCP	N'importe quel port/443	

Sujet parent: Configuration du protocole IPsec/du filtrage IP

Exemples de configuration de la fonction IPsec/filtrage IP

Vous pouvez configurer l'IPsec et le filtrage IP d'une variété de façons, tel qu'indiqué dans les exemples suivants.

Réception des paquets IPsec seulement

N'utilisez cet exemple que pour configurer une politique par défaut.

- **IPsec/filtrage IP** : **Activer**
- **Contrôle des accès** : **IPsec**
- **Méthode d'authentification** : **Clé pré-partagée**
- **Clé pré-partagée** : Entrez un maximum de 127 caractères.

Réception des données d’impression et des paramètres de l’imprimante

Utilisez cet exemple pour autoriser la communication des données d'impression et des paramètres de l'imprimante à partir de services spécifiés.

Politique par défaut :

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

Politique de groupe :

- **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** : Sélectionnez **ENPC**, **SNMP**, **HTTP (local)**, **HTTPS (local)** et **RAW (Port9100)**.

Réception de l'accès à partir d'une adresse IP spécifiée seulement

Dans ces exemples, le client pourra accéder au produit et le paramétrer, peu importe la politique configurée.

Politique par défaut :

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

Politique de groupe :

- **Contrôle des accès** : **Autoriser l'accès**
- **Adresse distante (hôte)** : Adresse IP d'un client administrateur

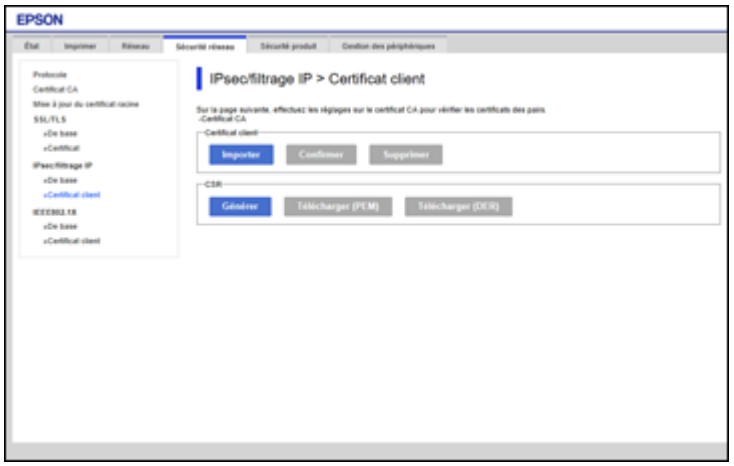
Sujet parent: Configuration du protocole IPsec/du filtrage IP

Configuration d'un certificat IPsec/de filtrage IP

Vous pouvez configurer un certificat pour le filtrage du trafic IPsec/filtrage IP à l'aide de Web Config.

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité du réseau**.
2. Sous **IPsec/filtrage IP**, sélectionnez **Certificat client**.

Une fenêtre comme celle-ci s'affiche :



3. Effectuez l'une des actions suivantes :
   - Cliquez sur **Importer** pour ajouter un nouveau certificat client.
   - Sélectionnez le certificat désiré à l'option **Copier de** et cliquez sur **Copie**.
4. Cliquez sur **OK**.

Sujet parent: Configuration du protocole IPsec/du filtrage IP

Tâches associées

Obtention et importation d'un certificat signé par l'AC

Configuration des paramètres du protocole SNMPv3

Si votre produit prend en charge le protocole SNMPv3, vous pouvez surveiller et contrôler l'accès à votre produit à l'aide de ce protocole.

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité du réseau**.

Une fenêtre comme celle-ci s'affiche :

2. Faites défiler l'écran vers le bas et cochez la case **Activer SNMPv3** pour activer les paramètres SNMPv3.
3. Sélectionnez les paramètres désirés dans la section Paramètres SNMPv3.
4. Cliquez sur **Suivant**.

   Un message de confirmation s'affichera.
5. Cliquez sur **OK**.

Paramètres SNMPv3

Sujet parent: Utilisation de votre produit sur un réseau sécurisé

Paramètres SNMPv3

Vous pouvez configurer ces paramètres SNMPv3 dans Web Config.

Paramètre	Options/Description
Nom de l'utilisateur	Définissez un nom d'utilisateur de 1 à 32 caractères ASCII.
Param authentification	
Algorithme	Sélectionnez l'algorithme pour l'authentification.
Mot de passe	Définissez un mot de passe de 8 à 32 caractères ASCII.
Confirmer le mot de passe	Entrez le mot de passe d'authentification à nouveau.
Param cryptage	

Paramètre	Options/Description
Algorithme	Sélectionnez l'algorithme de chiffrement.
Mot de passe	Définissez un mot de passe de 8 à 32 caractères ASCII.
Confirmer le mot de passe	Entrez le mot de passe de chiffrement à nouveau.
Nom contexte	Définissez un nom de contexte de 1 à 32 caractères ASCII.

Sujet parent: Configuration des paramètres du protocole SNMPv3

Connexion du produit à un serveur IEEE 802.1X

Suivez les instructions dans ces sections pour connecter le produit à un réseau IEEE 802.1X à l'aide de Web Config.

Configuration d'un réseau IEEE 802.1X

Paramètres du réseau IEEE 802.1X

Configuration d'un certificat pour un réseau IEEE 802.1X

Vérification de l'état du réseau IEEE 802.1X

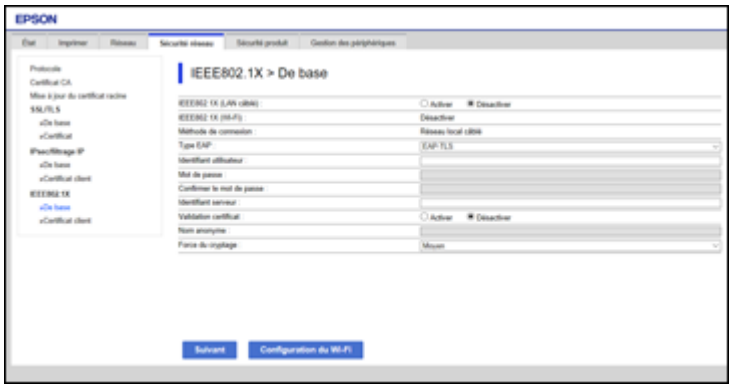
Sujet parent: Utilisation de votre produit sur un réseau sécurisé

Configuration d'un réseau IEEE 802.1X

Si votre produit prend en charge le protocole IEEE 802.1X, Web Config vous permet de 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 l'onglet **Sécurité du réseau**.
2. Sous **IEEE802.1X**, sélectionnez **De base**.

Une fenêtre comme celle-ci s'affiche :



3. Sélectionnez **Activer** au paramètre **IEEE802.1X (LAN câblé)**.
4. Pour utiliser le produit sur un réseau Wi-Fi, activez les paramètres Wi-Fi de votre produit. Consultez le *Guide de l'utilisateur* du produit pour des instructions à ce sujet.

   L'état actuel de la connexion s'affiche au paramètre **IEEE802.1X (Wi-Fi)**.

   Remarque: Vous pouvez utiliser les mêmes paramètres pour les réseaux Ethernet et Wi-Fi.
5. Sélectionnez les options que vous souhaitez utiliser au paramètre IEEE 802.1X.
6. Cliquez sur **Suivant**.

   Un message de confirmation s'affichera.
7. Cliquez sur **OK**.

Sujet parent: Connexion du produit à un serveur IEEE 802.1X

Paramètres du réseau IEEE 802.1X

Vous pouvez configurer ces paramètres du réseau IEEE 802.1X dans Web Config.

Paramètre	Options/Description
IEEE802.1X (LAN câblé)	Active ou désactive les paramètres (**IEEE802.1X** > **De Base**).
IEEE802.1X (Wi-Fi)	Affiche l'état de la connexion au réseau IEEE 802.1X (Wi-Fi).
Méthode de connexion	Affiche la méthode de connexion au réseau actuelle.

Paramètre	Options/Description
Type EAP	Sélectionnez l'une de ces méthodes d'authentification pour les connexions entre le produit et un serveur RADIUS : **EAP-TLS** ou **PEAP-TLS** : Vous devez obtenir et importer un certificat signé par l'AC. **PEAP/MSCHAPv2** ou **EAP-TTLS** : Vous devez configurer un mot de passe.
Identifiant utilisateur	Définissez un identifiant de 1 à 128 caractères ASCII pour l'authentification sur un serveur RADIUS.
Mot de passe	Définissez un mot de passe de 1 à 128 caractères ASCII pour l'authentification du produit. Si vous utilisez Windows comme un serveur RADIUS, saisissez jusqu'à 127 caractères ASCII.
Confirmer le mot de passe	Entrez le mot de passe d'authentification à nouveau.
Identifiant serveur	Définissez un identifiant serveur de 1 à 128 caractères ASCII pour l'authentification sur un serveur RADIUS indiqué. L'identifiant du serveur est comparé au contenu du champ subject/subjectAltName du certificat de serveur envoyé par le serveur RADIUS.
Validation certificat	Sélectionnez un certificat valide indépendamment de la méthode d'authentification; importez le certificat en utilisant l'option **Certificat CA**.
Nom anonyme	Si vous avez sélectionné **EAP-TTLS**, **PEAP-TLS** ou **PEAP/MSCHAPv2** au paramètre **Méthode d'authentification**, vous pouvez configurer un nom anonyme de 1 à 128 caractères ASCII au lieu d'un identifiant utilisateur pour la première phase de l'authentification PEAP.
Force du cryptage	Sélectionnez l'une des forces de cryptage : **Haut** pour AES256/3DES **Moyen** pour AES256/3DES/AES128/RC4

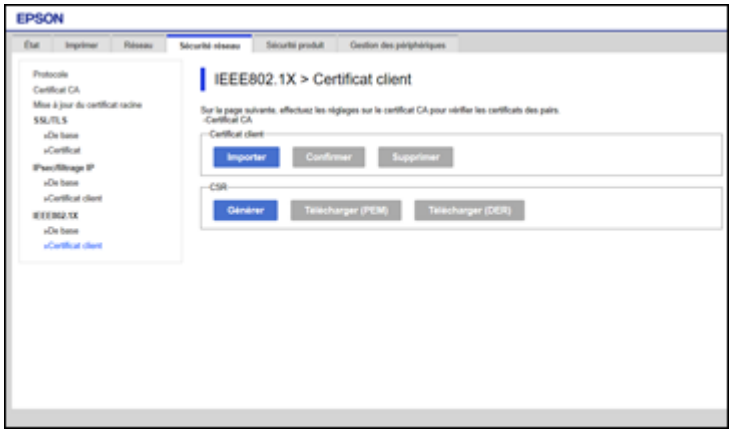
Sujet parent: Connexion du produit à un serveur IEEE 802.1X

Configuration d'un certificat pour un réseau IEEE 802.1X

Si votre produit prend en charge le protocole IEEE 802.1X, vous pouvez configurer un certificat pour le réseau à l'aide de Web Config.

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité du réseau**.
2. Sous **IEEE802.1X**, sélectionnez **Certificat client**.

   Une fenêtre comme celle-ci s'affiche :



3. Effectuez l'une des actions suivantes :
   - Cliquez sur **Importer** pour ajouter un nouveau certificat client.
   - Sélectionnez le certificat désiré à l'option **Copier de** et cliquez sur **Copie**.
4. Cliquez sur **OK**.

Sujet parent: Connexion du produit à un serveur IEEE 802.1X

Vérification de l'état du réseau IEEE 802.1X

Vous pouvez vérifier l'état du réseau IEEE 802.1X en imprimant une feuille d'état réseau depuis votre produit. Consultez le *Guide de l'utilisateur* du produit pour des instructions sur la façon d'imprimer une feuille d'état réseau.

La feuille d'état réseau affiche les informations pour les réseaux IEEE 802.1X, tel qu'indiqué dans ce tableau.

Identifiant de l'état	Description de l'état
Disable	La fonctionnalité IEEE 802.1X est désactivée.
EAP Success	L'authentification IEEE 802.1X a été confirmée et la connexion réseau est disponible.

Identifiant de l'état	Description de l'état
Authenticating	L'authentification IEEE 802.1X est en cours.
Config Error	L'authentification a échoué parce que l'identifiant utilisateur n'a pas été défini.
Client Certificate Error	L'authentification a échoué parce que le certificat client n'est plus à jour.
Timeout Error	L'authentification a échoué parce qu'il n'y a pas de réponse du serveur RADIUS et/ou de l'authentifiant.
User ID Error	L'authentification a échoué parce que l'identifiant utilisateur du produit et/ou le protocole du certificat est incorrect.
Server ID Error	L'authentification a échoué parce que l'identifiant de serveur du certificat de serveur et l'identifiant du serveur ne correspondent pas.
Server Certificate Error	L'authentification a échoué parce que le certificat du serveur n'est plus à jour ou parce que la chaîne du certificat du serveur est incorrecte.
CA Certificate Error	L'authentification a échoué parce que le certificat de l'AC est incorrect, n'a pas été importé ou n'est plus à jour.
EAP Failure	L'authentification a échoué parce que le certificat client est incorrect (EAP-TLS ou PEAP-TLS) ou parce que l'identifiant/mot de passe utilisateur est incorrect (PEAP/MSCHAPv2 ou EAP-TTLS).

Sujet parent: Connexion du produit à un serveur IEEE 802.1X

Utilisation d'un certificat numérique

Suivez les instructions dans ces sections pour configurer et utiliser des certificats numériques à l'aide de Web Config.

À propos de la certification numérique
Obtention et importation d'un certificat signé par l'AC
Configuration d’un CSR
Paramètres d'importation d’un CSR
Suppression d'un certificat signé par l'AC
Mise à jour d'un certificat auto-signé
Importation d'un certificat de l'AC
Suppression d'un certificat de l'AC

Sujet parent: Utilisation de votre produit sur un réseau sécurisé

À propos de la certification numérique

Vous pouvez configurer les certificats numériques suivants pour votre réseau à l'aide de Web Config :

Certificat signé par l'AC
Vous pouvez sécuriser les communications en utilisant un certificat signé par l'AC pour chaque fonctionnalité de sécurité. Ces certificats doivent provenir d'une AC (autorité de certification; CA ou Certificate Authority en anglais) et être signés par cette dernière.

Certificat de l'AC
Un certificat de l'AC indique qu'une tierce partie a vérifié l'identité du serveur. Vous devez obtenir un certificat de l'AC pour l'authentification du serveur venant d'une AC (autorité de certification) autorisée.

Certificat auto-signé
Un certificat auto-signé est généré et signé par le produit lui-même. Vous pouvez utiliser ce certificat pour les communications SSL/TLS seulement. Cependant, ce certificat n'est pas aussi sécuritaire que le certificat signé par l'AC, et une alerte de sécurité pourrait s'afficher dans le navigateur durant son utilisation.

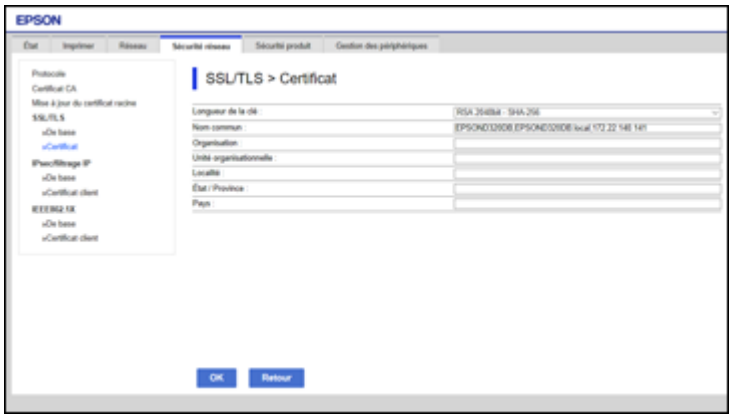
Sujet parent: Utilisation d'un certificat numérique

Obtention et importation d'un certificat signé par l'AC

Vous pouvez obtenir un certificat signé par l'AC en créant un CSR (Certificate Signing Request; demande de signature de certificat) à l'aide de Web Config et en le soumettant à une autorité de certification. Un CSR créé dans Web Config sera de format PEM/DER. Vous pouvez importer un CSR créé depuis Web Config à tout moment.

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité du réseau**.
2. Pour l'une des options de sécurité réseau suivantes, sélectionnez le certificat correspondant :
   - **SSL/TLS** et **Certificat**
   - **IPsec/filtrage IP** et **Certificat client**
   - **IEEE802.1X** et **Certificat client**
3. Dans la section CSR, sélectionnez **Générer**.

Une fenêtre comme celle-ci apparaîtra :



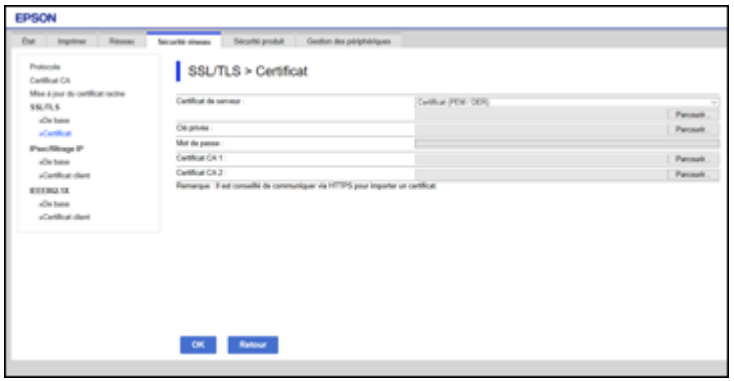
4. Entrez les informations nécessaires pour le CSR.
5. Cliquez sur **OK**.

   Un message s'affiche pour vous aviser que la tâche est terminée.
6. Sélectionnez l'onglet **Sécurité du réseau** à nouveau, et sélectionnez le certificat et l'option de sécurité correspondant à votre réseau.
7. Dans la section CSR, cliquez sur l'option **Télécharger** qui correspond au format spécifié par votre autorité de certification afin de télécharger le CSR.

   Mise en garde: Ne générez aucun autre CSR, sinon, vous risquez de ne pas pouvoir importer un certificat signé par l'AC.
8. Soumettez le CSR à l'autorité de certification en suivant les instructions fournies par cette autorité.
9. Enregistrez le certificat signé par l'AC sur un ordinateur connecté au produit.

   Avant de poursuivre, assurez-vous que les paramètres de date et d'heure du produit sont définis correctement. Consultez le *Guide de l'utilisateur* du produit pour des instructions à ce sujet.
10. Sélectionnez l'onglet **Sécurité du réseau** à nouveau, et sélectionnez le certificat et l'option de sécurité correspondant à votre réseau.
11. Dans la section Certificat CA, cliquez sur **Importer**.

Une fenêtre comme celle-ci s'affiche :



12. Sélectionnez le format du certificat au paramètre **Certificat de serveur**.
13. Sélectionnez les paramètres d'importation du certificat qui correspondent à son format et à la source d'où il provient.
14. Cliquez sur **OK**.

    Un message de confirmation s'affichera.
15. Cliquez sur **Confirmer** pour confirmer les informations du certificat.

Sujet parent: Utilisation d'un certificat numérique

Configuration d'un CSR

Vous pouvez sélectionner ces paramètres lorsque vous configurez un CSR dans Web Config.

Remarque: La longueur de la clé et les abréviations disponibles varient selon l'autorité de certification. Suivez les règles dictées par l'autorité en question lorsque vous entrez les informations du CSR.

Paramètre	Options/Description
Longueur de la clé	Sélectionnez la longueur de la clé du CSR.

Paramètre	Options/Description
Nom commun	Définissez un nom ou une adresse IP statique d'une longueur de 1 à 128 caractères, par exemple **Imprimante réception** ou **https://10.152.12.225**. Vous pouvez ajouter jusqu'à 5 adresses IPv4, adresses IPv6, noms d'hôtes ou FQDN séparés par des virgules.
Organisation, **Unité organisationnelle**, **Localité**, **État/Province**	Entrez des informations de 0 à 64 caractères ASCII dans chaque champ, au besoin. Séparez les noms uniques par des virgules.
Pays	Entrez le code de pays à deux chiffres tel qu'indiqué dans la norme ISO-3166.

Sujet parent: Utilisation d'un certificat numérique

Paramètres d'importation d’un CSR

Vous pouvez configurer ces paramètres lorsque vous importez un CSR dans Web Config.

Remarque: Les paramètres d'importation à configurer varient selon le format du certificat et la façon dont vous l'avez obtenu.

Format du certificat	Description des paramètres
Certificat au format PEM/DER obtenu depuis Web Config	**Clé privée** : Ne pas configurer (le produit contient une clé privée) **Mot de passe** : Ne pas configurer **Certificat CA 1/Certificat CA 2** : Optionnel
Certificat au format PEM/DER obtenu depuis un ordinateur	**Clé privée** : Configurer une clé privée **Mot de passe** : Ne pas configurer **Certificat CA 1/Certificat CA 2** : Optionnel
Certificat au format PKCS#12 obtenu depuis un ordinateur	**Clé privée** : Ne pas configurer **Mot de passe** : Optionnel **Certificat CA 1/Certificat CA 2** : Ne pas configurer

Sujet parent: Utilisation d'un certificat numérique

Suppression d'un certificat signé par l'AC

Vous pouvez supprimer un certificat signé par l'AC importé avec Web Config si le certificat est expiré ou si vous n'avez plus besoin d'une connexion chiffrée.

Remarque: Si vous avez obtenu un certificat signé par l'AC depuis Web Config, vous ne pourrez pas le réimporter si vous le supprimez; vous devrez obtenir et importer un nouveau certificat.

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité du réseau**.
2. Pour l'une des options de sécurité réseau suivantes, sélectionnez le certificat correspondant :
   - **SSL/TLS** et **Certificat**
   - **IPsec/filtrage IP** et **Certificat client**
   - **IEEE802.1X** et **Certificat client**
3. Cliquez sur **Supprimer**.

   Un message s'affichera pour vous aviser que la tâche est terminée.
4. Cliquez sur **OK**.

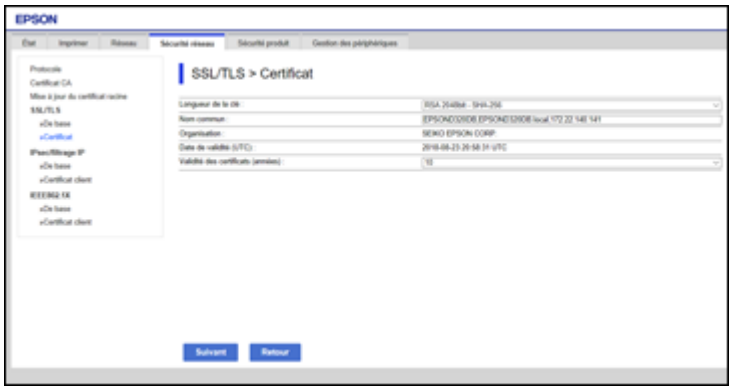
Sujet parent: Utilisation d'un certificat numérique

Mise à jour d'un certificat auto-signé

Si votre produit prend en charge les fonctions du protocole HTTPS, vous pouvez mettre à jour un certificat auto-signé à l'aide de Web Config.

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité du réseau**.
2. Sous **SSL/TLS**, sélectionnez **Certificat**.
3. Cliquez sur **Mettre à jour**.

Une fenêtre comme celle-ci apparaîtra :



4. Définissez un identifiant pour votre produit dans le champ **Nom commun** (de 1 à 128 caractères).

   Remarque: Vous pouvez ajouter jusqu'à 5 adresses IPv4, adresses IPv6, noms d'hôtes ou FQDN séparés par des virgules. La première valeur est attribuée au champ Nom commun et les autres sont ajoutées dans le champ d'alias du sujet du certificat. Vous ne pouvez pas entrer une espace avant ou après une virgule.

5. Définissez la période de validité du certificat au paramètre **Validité des certificats (années)**.
6. Cliquez sur **Suivant**.

   Un message s'affichera pour vous aviser que la tâche est terminée.
7. Cliquez sur **OK**.
8. Cliquez sur **Confirmer** pour confirmer les informations du certificat.

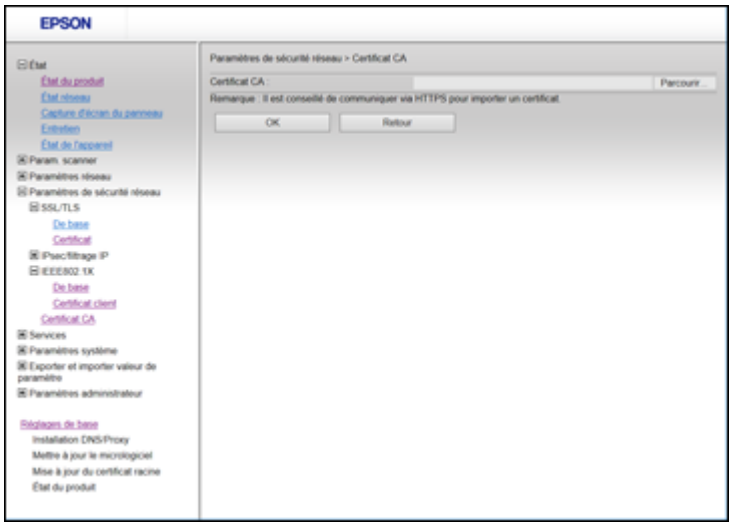
Sujet parent: Utilisation d'un certificat numérique

Importation d'un certificat de l'AC

Vous pouvez importer un certificat de l'AC en utilisant Web Config.

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité du réseau**.
2. Sélectionnez **Certificat CA**.
3. Sélectionnez **Importer**.

4. Sélectionnez le certificat de l'AC que vous souhaitez importer.



5. Cliquez sur **OK**.

L'importation du certificat de l'AC est complète lorsque la page **Certificat CA** apparaît et que le certificat de l'AC s'affiche.

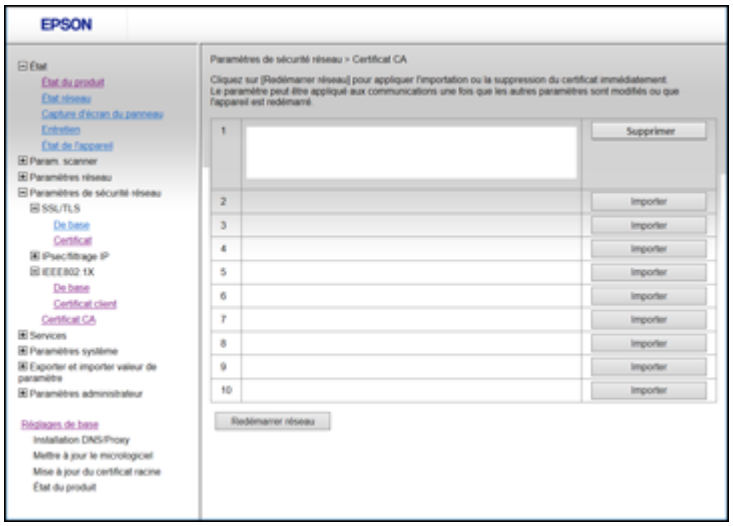
Sujet parent: Utilisation d'un certificat numérique

Suppression d'un certificat de l'AC

Vous pouvez supprimer un certificat de l'AC importé avec Web Config si le certificat est expiré ou si vous n'avez plus besoin d'une connexion chiffrée.

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité du réseau**.

2. Sélectionnez **Certificat CA**.



3. Repérez le certificat que vous souhaitez effacer et cliquez sur le bouton **Supprimer** à côté.
4. Cliquez sur **OK** pour confirmer la suppression.
5. Cliquez sur **Redémarrer réseau** et vérifiez ensuite que le Certificat CA n'est pas listé sur l'écran qui a été mis à jour.

Sujet parent: Utilisation d'un certificat numérique

Configuration des protocoles sous Web Config

Vous pouvez activer ou désactiver les protocoles en utilisant Web Config.

1. Accédez à Web Config et sélectionnez l'onglet **Sécurité du réseau**.
2. Cochez ou décochez la case à côté du nom du service afin d'activer ou de désactiver un protocole.
3. Configurez les autres paramètres du protocole disponibles.
4. Cliquez sur **Suivant**.
5. Cliquez sur **OK**.

Les changements sont appliqués après le redémarrage du protocole.

Paramètres des protocoles

Sujet parent: Utilisation de votre produit sur un réseau sécurisé

Paramètres des protocoles

Protocoles

Nom	Description
Bonjour	Bonjour est utilisé pour rechercher des appareils.
SLP	SLP permet d'utiliser la recherche réseau dans EpsonNet Config.
WSD	Permet d'ajouter des appareils ou d'imprimer depuis le port WSD.
LLTD	Permet d'afficher le produit sur la carte réseau Windows.
LLMNR	Permet d'utiliser la résolution de noms sans NetBIOS même si vous ne pouvez pas utiliser DNS.
LPR	Permet d'imprimer depuis le port LPR.
RAW(Port9100)	Permet d'imprimer depuis le port RAW (Port 9100).
IPP	Permet d'imprimer via Internet.
FTP	Permet d'imprimer depuis un FTP.
SNMPv1/v2c	Permet de configurer et de surveiller votre produit à distance.
SNMPv3	Permet de configurer et de surveiller votre produit à distance à l'aide du protocole SNMPv3.

Réglages Bonjour

Paramètre	Options/Description
Utiliser Bonjour	Permet de rechercher ou d'utiliser des appareils au moyen de Bonjour.
Nom Bonjour	Affiche le nom Bonjour.
Nom de service Bonjour	Affiche le nom de service Bonjour.
Emplacement	Affiche le nom d'emplacement Bonjour.
Protocole de priorité absolue	Sélectionne le protocole de première priorité pour l'impression avec Bonjour.

Paramètre	Options/Description
Wide-Area Bonjour	Active le protocole Wide-Area Bonjour; enregistre tous les produits sur le serveur DNS afin de les localiser sur le segment.

Paramètres SLP

Paramètre	Options/Description
Activer SLP	Permet d'activer la fonction SLP afin d'utiliser la recherche réseau dans EpsonNet Config.

Paramètres WSD

Paramètre	Options/Description
Activer WSD	Permet d'activer des appareils utilisant WSD et d'imprimer depuis le port WSD (si vous ne souhaitez pas que ce produit recherche des appareils, désactivez ce paramètre et désactivez **Activer IPP**).
Expiration impression (sec)	Permet de saisir la valeur d'expiration pour l'impression WSD entre 3 et 3600 secondes.
Nom de l'appareil	Affiche le nom de l'appareil WSD.
Emplacement	Affiche le nom d'emplacement WSD.

Paramètres LLTD

Paramètre	Options/Description
Activer LLTD	Permet d'activer LLTD afin d'afficher le produit sur la carte réseau Windows.
Nom de l'appareil	Permet d'afficher le nom de l'appareil LLTD.

Paramètres LLMNR

Paramètre	Options/Description
Activer LLMNR	Permet d'activer LLMNR afin d'utiliser la résolution de noms sans NetBIOS, même si vous ne pouvez pas utiliser DNS.

Paramètres LPR

Paramètre	Options/Description
Permettre l'impression sur Port LPR	Permet l'impression depuis le port LPR.
Expiration impression (sec)	Permet de saisir la valeur d'expiration pour l'impression LPR entre 0 et 3600 secondes.

Paramètres RAW (Port9100)

Paramètre	Options/Description
Permettre l'impression RAW (Port9100)	Permet d'autoriser l'impression depuis le port RAW (Port 9100).
Expiration impression (sec)	Permet de saisir la valeur d'expiration pour l'impression du port RAW (port 9100) entre 0 et 3600 secondes.

Paramètres IPP

Paramètre	Options/Description
Activer IPP	Permet d'activer la communication IPP. Seuls les produits qui prennent en charge IPP sont affichés.
Permettre les communications non sécurisées.	Permet à l'imprimante de communiquer sans aucune mesure de sécurité (IPP).
Temporisation communication (sec)	Permet de saisir la valeur d'expiration pour l'impression IPP entre 0 et 3600 secondes.
URL (Réseau)	Permet d'afficher les URL IPP (http et https) lorsque le produit est connecté par LAN câblé ou Wi-Fi (l'URL est une valeur combinée de l'adresse IP de l'imprimante, du numéro de port et du nom de l'imprimante IPP).

Paramètre	Options/Description
URL (Wi-Fi Direct)	Permet d'afficher les URL IPP (http et https) lorsque le produit est connecté par Wi-Fi (l'URL est une valeur combinée de l'adresse IP de l'imprimante, du numéro de port et du nom de l'imprimante IPP).
Nom de l'imprimante	Affiche le nom de l'imprimante IPP.
Emplacement	Affiche l'emplacement IPP.

Param FTP

Paramètre	Options/Description
Activer serveur FTP	Permet d'activer l'impression FTP pour les produits qui prennent en charge l'impression FTP.
Temporisation communication (sec)	Permet de saisir la valeur d'expiration pour la communication FTP entre 0 et 3600 secondes.

Paramètres SNMPv1/v2c

Paramètre	Options/Description
Activer SNMPv1/v2c	Permet d'activer SNMPv1/v2c pour les produits qui prennent en charge SNMPv3.
Autorité accès	Permet de définir l'autorité d'accès lorsque SNMPv1/v2c est activé à **En lecture seule ou Lecture/écriture**.
Nom communauté (lecture seule)	Permet de saisir de 0 à 32 caractères ASCII.
Nom communauté (lecture/écriture)	Permet de saisir de 0 à 32 caractères ASCII.
Autoriser l'accès à partir des outils Epson.	Permet d'autoriser ou non l'utilisation des outils Epson comme Epson Device Admin.

Paramètres SNMPv3

Paramètre	Options/Description
Activer SNMPv3	Permet d'activer SNMPv3 pour les produits qui prennent en charge SNMPv3.

Paramètre	Options/Description
Nom d'utilisateur	Permet de saisir de 1 à 32 caractères.
Param authentification	Permet de sélectionner un algorithme et d'entrer un mot de passe pour l'authentification.
Param cryptage	Permet de sélectionner un algorithme et d'entrer un mot de passe pour le chiffrement.
Nom contexte	Permet de saisir de 1 à 32 caractères.

Sujet parent: Configuration des protocoles sous Web Config

Références associées

Paramètres SNMPv3

Utilisation du logiciel de configuration réseau EpsonNet Config

Suivez les instructions dans ces sections pour configurer les paramètres d'administration réseau de votre produit à l'aide du logiciel EpsonNet Config.

Sous Windows, vous pouvez configurer les paramètres réseau par lot. Consultez l'utilitaire d'aide d'EpsonNet Config pour des instructions à ce sujet.

Remarque: Avant de pouvoir configurer les paramètres d'administration du système, vous devez connecter le produit à un réseau. Consultez le *Guide de l'utilisateur* du produit pour des instructions à ce sujet.

Installation d'EpsonNet Config
Configuration de l'adresse IP du produit à l'aide d'EpsonNet Config

Installation d'EpsonNet Config

Pour installer EpsonNet Config, téléchargez le logiciel sur la page de soutien du produit à l'adresse epson.ca/support et suivez les instructions à l'écran.

Sujet parent: Utilisation du logiciel de configuration réseau EpsonNet Config

Configuration de l'adresse IP du produit à l'aide d'EpsonNet Config

Vous pouvez configurer l'adresse IP du produit à l'aide d'EpsonNet Config.

1. Mettez le produit sous tension.
2. Connectez le produit à un réseau à l'aide d'un câble Ethernet.
3. Effectuez l'une des étapes suivantes pour lancer EpsonNet Config :
   - **Windows 11** : Cliquez sur  , effectuez une recherche du logiciel **EpsonNet Config** et sélectionnez-le.
   - **Windows 10** : Cliquez sur  > **Toutes les applications** > **EpsonNet** > **EpsonNet Config**.
   - **Windows 8.x** : Naviguez vers l'écran **Applications** et sélectionnez **EpsonNet** > **EpsonNet Config**.
   - **Windows** (autres versions) : Cliquez sur  ou **Démarrer**, puis sélectionnez **Tous les programmes** ou **Programmes**. Sélectionnez **EpsonNet** > **EpsonNet Config**.

- **Mac** : Ouvrez le dossier **Applications**, ouvrez le dossier **Epson Software** et sélectionnez **EpsonNet** > **EpsonNet Config** > **EpsonNet Config**.

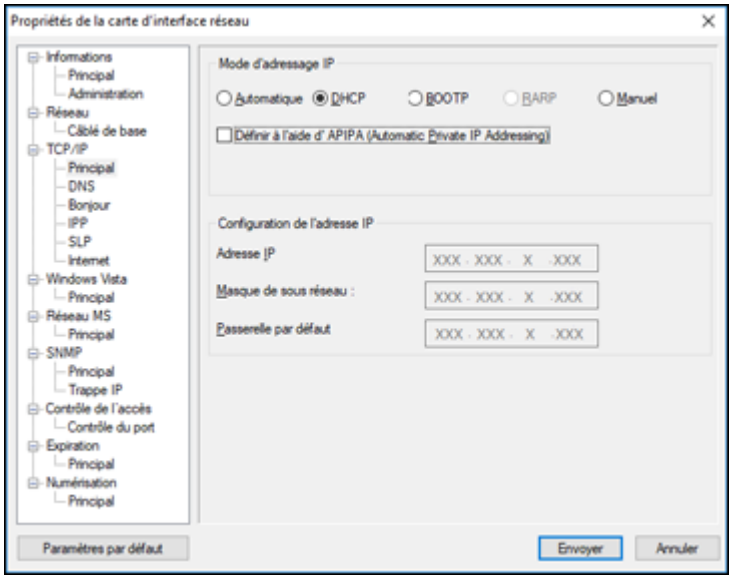
Après quelques instants, le logiciel affichera les produits connectés.

4. Double-cliquez sur le produit que vous configurez.

   Remarque: Si plusieurs produits du même modèle sont connectés, vous pouvez les identifier à l'aide de leur adresse MAC.

5. Entrez le mot de passe administrateur actuel, si nécessaire, puis cliquez sur **OK**.
6. Depuis le menu de gauche, sous **TCP/IP**, sélectionnez **De base**.

   Une fenêtre comme celle-ci s'affiche :



7. Sélectionnez **Manuel**.

8. Entrez l'**Adresse IP**, le **Masque sous-réseau** et la **Passerelle par défaut** du produit dans les champs correspondants.

   Remarque: Pour connecter le produit à un réseau sécurisé, entrez une adresse IP statique. Vous pouvez aussi configurer les paramètres **DNS** et les paramètres du proxy en sélectionnant **Internet** dans le menu **TCP/IP**.

9. Sélectionnez **Envoyer**.
10. Entrez le mot de passe administrateur actuel, si nécessaire, puis cliquez sur **OK**.

Sujet parent: Utilisation du logiciel de configuration réseau EpsonNet Config

Utilisation du logiciel de configuration Epson Device Admin

Sous Windows, vous pouvez découvrir et surveiller des dispositifs à distance, et configurer les paramètres réseau par lot. Consultez l'aide d'Epson Device Admin pour obtenir les instructions.

Pour installer Epson Device Admin, téléchargez le logiciel sur la page de soutien du produit à l'adresse epson.ca/soutien et suivez les instructions à l'écran.

Résolution de problèmes

Consultez ces sections pour des solutions aux problèmes reliés aux logiciels de configuration du réseau.

Résolution des problèmes d'utilisation des logiciels réseau
Résolution des problèmes de sécurité réseau
Solutions aux problèmes reliés aux certificats numériques
Comment obtenir de l'aide

Résolution des problèmes d'utilisation des logiciels réseau

Consultez ces sections si vous avez des problèmes lors de l'utilisation des logiciels réseau.

Impossible d'accéder à Web Config
Le message « Certificate has expired » s'affiche
Le message « The name of the security certificate does not match » s'affiche
Le nom du modèle ou l'adresse IP ne s'affiche pas dans EpsonNet Config

Sujet parent: Résolution de problèmes

Impossible d'accéder à Web Config

Si vous n'arrivez pas à accéder à Web Config depuis votre produit, essayez ces solutions :

- Assurez-vous que votre produit est allumé et connecté à votre réseau à l'aide de la bonne adresse IP. Vérifiez la connexion à l'aide du panneau de commande de votre produit, ou imprimez une feuille d'état du réseau. Consultez le *Guide de l'utilisateur* du produit pour des instructions à ce sujet.
- Si vous avez sélectionné **Haut** au paramètre **Force du cryptage** dans Web Config, votre navigateur doit prendre en charge le chiffrement AES (256 bits) ou 3DES (168 bits). Vérifiez le type de chiffrement pris en charge par votre navigateur ou sélectionnez une autre option de **Force du cryptage**.
- Si vous utilisez un serveur proxy avec votre produit, configurez les paramètres du proxy de cette façon :
  - **Windows 11 :** Cliquez sur  , puis effectuez une recherche pour **Paramètres proxy**. Faites défiler les options et réglez **Utiliser un serveur proxy** à **Activé**.
  - **Windows 10** : Cliquez sur  > **Paramètres** > **Réseau & Internet** > **Proxy**. Faites défiler les options et réglez **Utiliser un serveur proxy** à **Activé**. Sélectionnez **Ne pas utiliser le serveur proxy pour les adresses (Intranet) locales**.

- **Windows 8.x** : Naviguez vers l'écran **Applications** et sélectionnez **Paramètres du PC** > **Réseau** > **Proxy**. Faites défiler les options et réglez **Utiliser un serveur proxy** à **Activé**. Sélectionnez **Ne pas utiliser le serveur proxy pour les adresses (Intranet) locales**.
- **Windows (autres versions)** : Cliquez sur ou **Démarrer** et sélectionnez **Panneau de configuration** > **Réseau et Internet** > **Options Internet** > **Connexions** > **Paramètres réseau** > **Serveur Proxy** > **Utiliser un serveur proxy pour votre réseau local**.
- **Mac** : Sélectionnez **Préférences Système** > **Réseau** > **Avancé** > **Proxys**. Enregistrez l'adresse locale sous **Ignorer les réglages proxy pour ces hôtes et domaines**. Par exemple, 192.168.1.* : adresse locale 192.168.1.XXX, masque de sous-réseau 255.255.255.0.

Sujet parent: Résolution des problèmes d'utilisation des logiciels réseau

Le message « Certificate has expired » s'affiche

Si le message « Certificate has expired » [Le certificat a expiré] s'affiche lorsque vous accédez à Web Config à l'aide de la communication SSL (HTTPS), le certificat n'est plus à jour. Assurez-vous que la date et l'heure du produit sont réglées correctement et obtenez un nouveau certificat.

Sujet parent: Résolution des problèmes d'utilisation des logiciels réseau

Le message « The name of the security certificate does not match » s'affiche

Si un message commençant avec « The name of the security certificate does not match... » [Le nom du certificat de sécurité ne correspond pas...] s'affiche lorsque vous accédez à Web Config à l'aide de la communication SSL (HTTPS), l'adresse IP du produit sur le CSR ou le certificat auto-signé ne correspond pas à ce que vous avez entré dans le navigateur. Changez l'adresse IP que vous avez entrée au paramètre **Nom commun** et obtenez un certificat à nouveau, ou changez le nom du produit.

Sujet parent: Résolution des problèmes d'utilisation des logiciels réseau

Le nom du modèle ou l'adresse IP ne s'affiche pas dans EpsonNet Config

Si le nom du modèle et/ou l'adresse IP du produit ne s'affichent pas dans EpsonNet Config, essayez ces solutions :

- Si vous avez sélectionné l'option Bloquer, Annuler ou Arrêter lorsque l'écran de sécurité Windows ou l'écran du pare-feu s'est affiché, l'adresse IP et le nom du modèle du produit ne pourront pas s'afficher dans EpsonNet Config. Enregistrez EpsonNet Config en tant qu'exception dans votre logiciel de pare-feu ou de sécurité, ou fermez le logiciel de sécurité et essayez de redémarrer EpsonNet Config.
- Le délai d'expiration de l'opération s'est peut-être écoulé. Sélectionnez **Outils** > **Options** > **Expiration**, puis augmentez la durée au paramètre **Erreur de communication**. Cependant, sachez qu'EpsonNet Config pourrait alors devenir plus lent.

Sujet parent: Résolution des problèmes d'utilisation des logiciels réseau

Résolution des problèmes de sécurité réseau

Consultez ces sections si vous avez des problèmes avec les fonctions de sécurité du réseau.

Oubli de la clé pré-partagée
Impossible de communiquer avec le produit via la communication IPsec
La communication s'est interrompue soudainement
Impossible de créer un port d'impression IPP sécurisé
Connexion impossible après la configuration du protocole IPsec/du filtrage IP
Impossible d'accéder au produit après avoir configuré le réseau IEEE 802.1X

Sujet parent: Résolution de problèmes

Oubli de la clé pré-partagée

Si vous avez oublié la clé pré-partagée, changez-la en utilisant Web Config pour la politique par défaut ou la politique de groupe.

Sujet parent: Résolution des problèmes de sécurité réseau

Impossible de communiquer avec le produit via la communication IPsec

Assurez-vous que votre ordinateur utilise l'un de ces algorithmes pris en charge pour communiquer avec le produit :

Méthode de sécurité	Algorithme pris en charge
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 clés IKE	DH Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30*
Algorithme de chiffrement ESP	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES

Méthode de sécurité	Algorithme pris en charge
Algorithme d'authentification ESP	SHA-1, SHA-256, SHA-384, SHA-512, MD5
Algorithme d'authentification AH	

* Disponible pour IKEv2 seulement

Sujet parent: Résolution des problèmes de sécurité réseau

La communication s'est interrompue soudainement

Si la communication au réseau fonctionnait correctement, puis s'est soudainement interrompue, l'adresse IP du produit et/ou de l'ordinateur s'est peut-être modifiée ou est peut-être invalide. Essayez ces solutions :

- Désactivez IPsec à l'aide du panneau de commande du produit.
- Si le DHCP n'est plus à jour, ou si l'adresse IPv6 n'est plus à jour ou n'a pas été obtenue, il pourrait vous être impossible de trouver l'adresse IP enregistrée dans Web Config.
- Si le problème n'est toujours pas résolu, entrez une adresse IP statique à l'aide de Web Config.

Sujet parent: Résolution des problèmes de sécurité réseau

Impossible de créer un port d'impression IPP sécurisé

Si vous n'arrivez pas à créer un port d'impression IPP sécurisé, essayez ces solutions :

- Assurez-vous que vous avez spécifié le bon certificat pour les communications SSL/TLS à l'aide de Web Config.
- Si vous utilisez un certificat de l'AC, assurez-vous que vous l'avez importé sur l'ordinateur ayant accès au produit.

Sujet parent: Résolution des problèmes de sécurité réseau

Connexion impossible après la configuration du protocole IPsec/du filtrage IP

La valeur déterminée est peut-être erronée. Désactivez IPsec/le filtrage IP depuis le panneau de commande du produit. Établissez une connexion depuis l'ordinateur et configurez les paramètres IPsec/de filtrage IP de nouveau.

Pour désactiver IPsec/filtrage IP depuis le panneau de commande, sélectionnez Menu > **Paramètres généraux** > **Paramètres réseau** > **Avancé** > **Désactiver IPsec/filtrage IP** > **Commencer la configuration**. Lorsqu'un message d'achèvement s'affiche, sélectionnez **Fermer**.

Sujet parent: Résolution des problèmes de sécurité réseau

Impossible d'accéder au produit après avoir configuré le réseau IEEE 802.1X

Si vous ne pouvez plus accéder au produit après l'avoir configuré pour le réseau IEEE 802.1X, désactivez le réseau IEEE 802.1X et le Wi-Fi à l'aide du panneau de commande du produit. Puis, connectez le produit à un ordinateur et configurez le réseau IEEE 802.1X à nouveau en utilisant Web Config.

Pour désactiver IEEE802.1X depuis le panneau de commande, sélectionnez Menu > **Paramètres généraux** > **Paramètres réseau** > **Avancé** > **Désactiver IEEE802.1X** > **Commencer la configuration**. Lorsqu'un message d'achèvement s'affiche, sélectionnez **Fermer**.

Sujet parent: Résolution des problèmes de sécurité réseau

Solutions aux problèmes reliés aux certificats numériques

Consultez ces sections si vous avez des problèmes lors de l'utilisation d'un certificat numérique.

Messages d'avertissement des certificats numériques
Impossible d'importer un certificat numérique
Impossible de mettre à jour un certificat ou de créer un CSR
Suppression accidentelle d'un certificat signé par l'AC

Sujet parent: Résolution de problèmes

Messages d'avertissement des certificats numériques

Si un message d'avertissement en relation avec un certificat numérique s'affiche, consultez les solutions dans le tableau suivant.

Message	Solution
Entrez un certificat de serveur.	Sélectionnez le fichier d'un certificat et cliquez sur **Importer**.
Certificat CA 1 n'est pas entré.	Importez le premier certificat signé par l'AC avant d'importer des certificats additionnels.

Message	Solution
Valeur invalide ci-dessous.	Supprimez tous les caractères non pris en charge dans le chemin d'accès au fichier ou le mot de passe.
Date et heure non valides.	Réglez la date et l'heure sur le produit à l'aide de Web Config, EpsonNet Config ou le panneau de commande du produit.
MdPasse non valide.	Entrez le bon mot de passe du certificat signé par l'AC.
Fichier non valide.	Essayez l'une des solutions suivantes : • N'importez que les fichiers de certificat de format X509 envoyés par une autorité de certification digne de confiance. • Assurez-vous que le fichier ne dépasse pas 5 Ko et qu'il n'est pas corrompu ou contrefait. • Assurez-vous que la chaîne incluse dans le certificat est valide. Reportez-vous au site Web de l'autorité de certification.
Impossible d'utiliser les certificats de serveur qui incluent plus de trois certificats CA.	Importez des fichiers de certificat de format PKCS#12 qui contiennent un ou deux certificats de l'AC, ou convertissez chaque certificat au format PRM et importez-les à nouveau.
Le certificat a expiré. Vérifiez si le certificat est valide, ou vérifiez la date et l'heure sur votre imprimante.	Assurez-vous que la date et l'heure sur votre produit sont réglées correctement, et si le certificat est expiré, obtenez-en un nouveau et importez-le.

Message	Solution
La clé privée est nécessaire.	Effectuez l'une des procédures suivantes pour associer une clé privée au certificat : • Pour les certificats de format PEM/DER obtenus avec un CSR depuis un ordinateur, sélectionnez le fichier de la clé privée. • Pour les certificats de format PKCS#12 obtenus avec un CSR depuis un ordinateur, créez un fichier contenant la clé privée. Si vous tentez d'importer à nouveau un certificat de format PEM/DER obtenu avec un CSR depuis Web Config, sachez que vous ne pouvez l'importer qu'une seule fois. Vous devez obtenir et importer un nouveau certificat.
Échec de la configuration.	Assurez-vous que l'ordinateur et le produit sont connectés, et que le fichier du certificat n'est pas corrompu, puis importez le fichier du certificat à nouveau.

Sujet parent: Solutions aux problèmes reliés aux certificats numériques

Impossible d'importer un certificat numérique

Si l'importation d'un certificat numérique échoue, essayez les solutions suivantes :

- Assurez-vous que les informations du certificat signé par l'AC et du CSR correspondent. Si elles ne correspondent pas, importez le certificat sur un appareil possédant les mêmes informations, ou utilisez le CSR pour obtenir le certificat signé par l'AC à nouveau.
- Assurez-vous que la taille du certificat signé par l'AC ne dépasse pas 5 Ko.
- Assurez-vous que vous entrez le bon mot de passe.

Sujet parent: Solutions aux problèmes reliés aux certificats numériques

Impossible de mettre à jour un certificat ou de créer un CSR

Si la mise à jour d'un certificat auto-signé ou la création d'un CSR pour un certificat signé par l'AC échoue, essayez les solutions suivantes :

- Assurez-vous que vous avez bien défini le paramètre **Nom commun** dans Web Config.

- Assurez-vous que vous n'avez entré aucun caractère non pris en charge au paramètre **Nom commun** et que vous ne l'avez pas incorrectement divisé par une virgule. Corrigez la valeur du paramètre et lancez à nouveau la mise à jour du certificat.

Sujet parent: Solutions aux problèmes reliés aux certificats numériques

Suppression accidentelle d'un certificat signé par l'AC

Si vous avez accidentellement supprimé un certificat signé par l'AC, essayez les solutions suivantes :

- Si vous avez conservé une copie de sauvegarde du certificat, importez-le à nouveau.
- Si vous avez obtenu le certificat à l'aide d'un CSR créé dans Web Config, vous ne pourrez pas l'importer à nouveau après l'avoir supprimé. Créez un autre CSR et obtenez un nouveau certificat.

Sujet parent: Solutions aux problèmes reliés aux certificats numériques

Comment obtenir de l'aide

Si vous avez besoin de contacter Epson pour obtenir des services de soutien technique, utilisez l'une des options suivantes :

Assistance par Internet

Visitez le site Web de soutien d'Epson à l'adresse epson.ca/support et sélectionnez votre produit pour obtenir des solutions aux problèmes courants. Vous pouvez y télécharger des pilotes et de la documentation en français, consulter une foire aux questions et des conseils de dépannage, ou envoyer vos questions par courriel à Epson.

Contacter un représentant du soutien

Avant de communiquer avec Epson pour obtenir du soutien, ayez les informations suivantes sous la main :

- Nom de produit
- Numéro de série du produit (situé sur une étiquette sur le produit)
- Preuve d'achat (telle qu'un reçu de magasin) et date d'achat
- Configuration informatique
- Description du problème

Puis, consultez le *Guide de l'utilisateur* de votre produit pour obtenir les coordonnées.

Sujet parent: Résolution de problèmes

Avis

Consultez ces sections pour des avis importants.

Marques de commerce

EPSON® est une marque déposée, le logo EPSON est un logotype déposé et Epson Connect[MC] est une marque de commerce de Seiko Epson Corporation.

Mac et OS X sont des marques de commerce d'Apple Inc., enregistrées aux É.-U. et dans d'autres pays.

Microsoft, Windows, Windows Server et Windows Vista sont des marques de commerce du groupe d'entreprises Microsoft.

Wi-Fi Direct® est une marque déposée de Wi-Fi Alliance®.

Avis général : les autres noms de produit figurant dans le présent document ne sont cités qu'à des fins d'identification et peuvent être des marques de commerce de leurs propriétaires respectifs. Epson renonce à tous les droits associés à ces marques.

Sujet parent: Avis

Avis sur les droits d'auteur

Seiko Epson Corporation décline toute responsabilité en cas de dommages ou de problèmes découlant de l'utilisation d'options ou de produits consommables autres que les produits désignés comme produits Epson d'origine ou comme produits approuvés pour Epson par Seiko Epson Corporation.

Seiko Epson Corporation ne pourra être tenue responsable des dommages résultant des interférences électromagnétiques se produisant à la suite de l'utilisation de câbles d'interface autres que ceux désignés par Seiko Epson Corporation comme étant des Produits approuvés par Epson.

L'information contenue dans ce guide peut être modifiée sans préavis.

Attribution du droit d'auteur

Sujet parent: Avis

Attribution du droit d'auteur

1/24

CPD-64337

Sujet parent: Avis sur les droits d'auteur