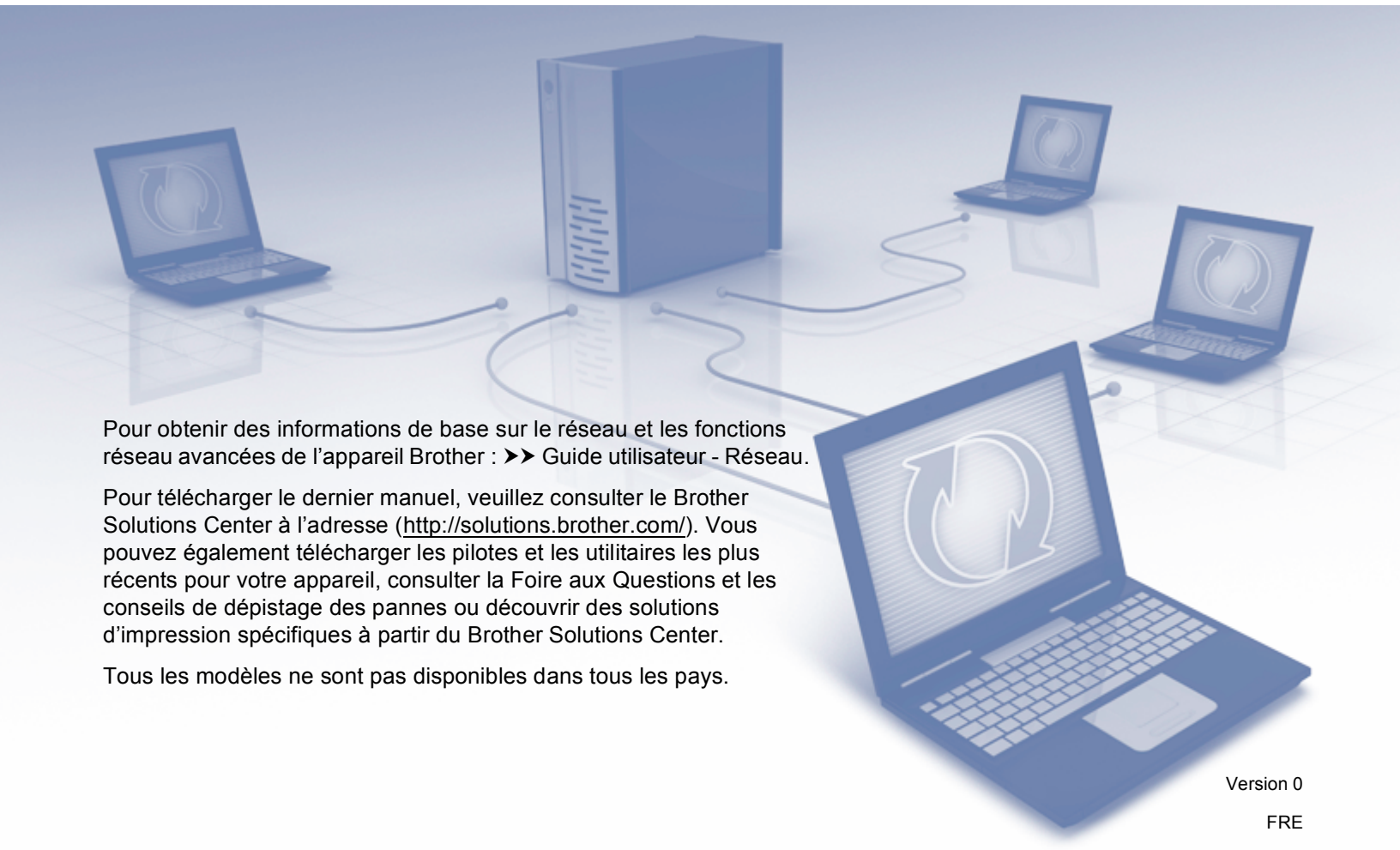
Guide SSL

(Secure Socket Layer)



Pour obtenir des informations de base sur le réseau et les fonctions réseau avancées de l'appareil Brother : ➤➤ Guide utilisateur - Réseau.

Pour télécharger le dernier manuel, veuillez consulter le Brother Solutions Center à l'adresse (http://solutions.brother.com/). Vous pouvez également télécharger les pilotes et les utilitaires les plus récents pour votre appareil, consulter la Foire aux Questions et les conseils de dépistage des pannes ou découvrir des solutions d'impression spécifiques à partir du Brother Solutions Center.

Tous les modèles ne sont pas disponibles dans tous les pays.

Version 0

FRE

Modèles concernés

Ce Guide utilisateur s’applique aux modèles suivants.

HL-5450DN(T)/5470DW(T)/6180DW(T)/S7000DN

DCP-8110DN/8150DN/8155DN/8250DN/MFC-8510DN/8710DW/8910DW/8950DW(T)

Définitions des remarques

Ce guide de l’utilisateur utilise les icônes suivantes :

Remarque	Les notes vous indiquent comment répondre à une situation donnée ou vous donnent des conseils sur le fonctionnement des options disponibles.

Marques commerciales

Le logo Brother est une marque déposée de Brother Industries, Ltd.

Microsoft, Windows, Windows Server et Internet Explorer sont des marques déposées ou des marques commerciales de Microsoft Corporation aux Etats-Unis et/ou dans d’autres pays.

Windows Vista est une marque déposée ou une marque de Microsoft Corporation aux Etats-Unis et/ou dans d’autres pays.

Google Cloud Print est une marque commerciale de Google Inc.

Toute société dont le logiciel est mentionné dans ce guide possède un Contrat de licence logiciel spécifique à ses programmes exclusifs.

Tous les noms de marques et de produits de sociétés apparaissant sur les produits Brother, les documents associés et toute autre documentation sont des marques commerciales ou déposées de ces différentes sociétés.

REMARQUE IMPORTANTE

- Ce produit est approuvé uniquement dans le pays d'achat. Ne l'utilisez pas dans d'autres pays car il pourrait enfreindre les réglementations relatives aux télécommunications sans fil et à l'alimentation électrique de ces pays.
- Sauf indication contraire, les écrans du modèle MFC-8950DW(T) sont utilisés dans ce manuel.
- Windows® XP dans ce document représente Windows® XP Professional, Windows® XP Professional x64 Edition et Windows® XP Home Edition.
- Windows Server® 2003 dans ce document représente Windows Server® 2003 et Windows Server® 2003 x64 Edition.
- Windows Server® 2008 dans ce document représente Windows Server® 2008 et Windows Server® 2008 R2.
- Windows Vista® dans ce document représente toutes les éditions de Windows Vista®.
- Windows® 7 dans ce document représente toutes les éditions de Windows® 7.
- Visitez le Brother Solutions Center à l'adresse http://solutions.brother.com/ et cliquez sur Manuels sur la page de votre modèle pour télécharger les autres manuels.

Table des matières

1 Introduction

Généralités

SSL (Secure Socket Layer) est une méthode efficace de protection des données transitant sur un réseau local ou étendu. Elle crypte les données envoyées sur un réseau, par exemple un travail d'impression, de manière à ce que toute personne essayant de capturer ces données ne puisse pas les lire.

Elle peut être configurée sur les réseaux filaires et sans fil, et fonctionne avec d'autres outils de sécurité, tels que les pare-feu et les clés WPA™.

Bref historique de SSL

SSL a été créé à l'origine pour sécuriser les informations circulant sur Internet, notamment les données envoyées entre les navigateurs Web et les serveurs. Par exemple, lorsque vous utilisez un service bancaire dans Internet Explorer®, si vous voyez https:// accompagné d'un petit cadenas dans le navigateur Web, cela signifie que vous utilisez SSL. Cette méthode a ensuite été développée pour fonctionner avec d'autres applications, telles que Telnet, les imprimantes et les logiciels FTP, et est devenue une solution universelle de sécurité en ligne. Ses fonctions premières sont toujours utilisées actuellement par de nombreux revendeurs en ligne et par la plupart des banques pour sécuriser leurs données sensibles, telles que les numéros de carte de crédit, les fichiers clients, etc.

SSL utilise des niveaux de cryptage extrêmement élevés et est agréé par les banques du monde entier, car la violation d'un tel système est peu probable.

Avantage de l'utilisation de SSL

L'unique avantage à utiliser SSL sur les appareils Brother est d'assurer une impression sécurisée sur un réseau IP en empêchant les utilisateurs non autorisés de lire les données envoyées à l'appareil. Le principal argument de cette méthode est qu'elle peut être utilisée pour imprimer des données confidentielles en toute sécurité. Par exemple, le service des ressources humaines d'une grande entreprise est amené à imprimer des bulletins de paye régulièrement. Sans cryptage, les données figurant sur ces bulletins de paye pourraient être lues par d'autres utilisateurs du réseau. Avec SSL, toute personne essayant de capturer ces données ne verra qu'une page codée illisible et non le bulletin de paye réel.

Utilisation de certificats pour la sécurité de la machine

Votre machine Brother prend en charge l'utilisation de multiples certificats de sécurité afin de sécuriser la gestion, l'authentification et les communications avec l'appareil. Les fonctionnalités de certificat de sécurité suivantes peuvent être utilisées avec l'appareil. Lorsque vous imprimez un document ou utilisez la Gestion à partir du Web (navigateur Web) de manière sécurisée à l'aide de SSL, vous devez installer le certificat sur votre ordinateur. Consultez *Installation d'un certificat numérique* ➤➤ page 4.

- Communication SSL/TLS
- Communication SSL pour SMTP/POP3

L'appareil Brother prend en charge les certificats suivants.

- Certificat pré-installé

  Votre appareil possède un certificat auto-signé pré-installé.

  Avec ce certificat, vous pouvez facilement utiliser la communication via SSL/TLS sans créer ou installer de certificat. Si vous souhaitez utiliser la fonction Google Cloud Print™ de votre appareil, vous pouvez définir les paramètres de cette application de manière sécurisée à l'aide de ce certificat pré-installé. Pour plus d'informations sur Google Cloud Print, visitez le Brother Solutions Center à l'adresse http://solutions.brother.com/ et cliquez sur Manuels sur la page de votre modèle pour télécharger le Guide d'impression Google Cloud.

Remarque

- La fonction Google Cloud Print n'est pas disponible pour le modèle HL-S7000DN.
- Le certificat auto-signé pré-installé ne protège pas vos communications contre les programmes espions. Pour assurer une meilleure sécurité, il est recommandé d'utiliser un certificat émis par une organisation digne de confiance.

- Certificat auto-signé

  Ce serveur d'impression émet son propre certificat. Avec ce certificat, vous pouvez facilement utiliser la communication via SSL/TLS sans avoir de certificat émis par une CA. (Consultez *Création d'un certificat auto-signé* ➤➤ page 6.)

- Certificat émis par une CA

  Il existe deux méthodes d'installation d'un certificat émis par une CA. Si vous avez déjà un certificat émis par une CA ou si vous souhaitez utiliser un certificat émis par une CA autorisée externe :

  - Si vous utilisez une CSR (Certificate Signing Request) depuis ce serveur d'impression. (Consultez *Création d'une demande de signature de certificat (CSR)* ➤➤ page 7.)
  - Si vous importez un certificat et une clé privée. (Consultez *Importez et exportez le certificat et la clé privée* ➤➤ page 17.)

■ Certificat CA

Si vous utilisez un certificat CA qui identifie la CA (Certificate Authority) proprement dite, vous devez importer un certificat CA émis par la CA avant de procéder à la configuration. (Consultez *Importer et exporter un certificat CA* ➤➤ page 18.)

Remarque

- Si vous êtes sur le point d'utiliser une communication SSL/TLS, nous vous conseillons de contacter votre administrateur système auparavant.
- Si vous restaurez les paramètres d'usine par défaut du serveur d'impression, le certificat et la clé privée installés seront supprimés. Si vous souhaitez conserver le même certificat et la même clé privée après la restauration du serveur d'impression, exportez-les avant la restauration et réinstallez-les. (Consultez *Comment importer le certificat auto-signé, le certificat émis par la CA et la clé privée* ➤➤ page 17.)

2 Certificat numérique pour les communications SSL

Installation d’un certificat numérique

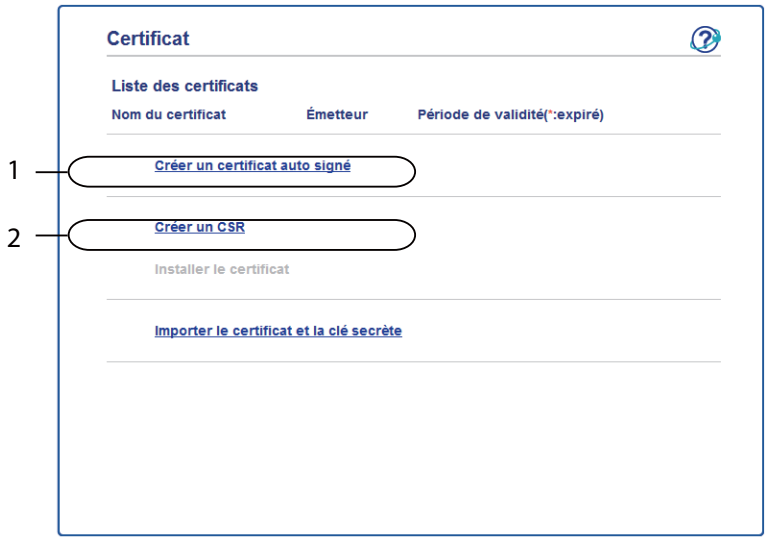
L’impression sur un réseau sécurisé ou la gestion sécurisée à l’aide de la Gestion à partir du Web (navigateur Web) exigent l’installation d’un certificat numérique sur l’appareil et sur le périphérique qui lui envoie les données (par exemple, un ordinateur). Votre appareil possède un certificat pré-installé. Pour configurer le certificat, l’utilisateur doit se connecter à distance à l’appareil via un navigateur Web à l’aide de son adresse IP.

Remarque

Il est recommandé d’utiliser Windows® Internet Explorer® 7.0/8.0 ou Firefox® 3.6 pour Windows® et Safari 4.0/5.0 pour Macintosh. Veuillez aussi vous assurer que JavaScript et Cookies sont toujours activés, quel que soit le navigateur utilisé. Si vous utilisez un autre navigateur Web, assurez-vous qu’il est compatible avec HTTP 1.0 et HTTP 1.1.

1. Lancez votre navigateur Web.
2. Tapez « http://adresse IP de l’appareil/ » dans la barre d’adresse de votre navigateur (où « adresse IP de l’appareil » correspond à l’adresse IP ou au nom du serveur d’impression).
   - Par exemple : http://192.168.1.2/
3. Aucun mot de passe n’est requis par défaut. Si vous en avez défini un mot de passe au préalable, saisissez-le et appuyez sur .
4. Cliquez sur **Réseau**.
5. Cliquez sur **Sécurit**.
6. Cliquez sur **Certificat**.

7 Vous pouvez configurer les paramètres du certificat.
Pour créer un certificat auto-signé à l'aide de la Gestion à partir du Web, consultez *Création d'un certificat auto-signé* ➤➤ page 6.
Pour créer une demande de signature de certificat (Certificate Signing Request, CSR), consultez *Création d'une demande de signature de certificat (CSR)* ➤➤ page 7.



1 Pour créer et installer un certificat auto-signé

2 Pour utiliser un certificat émis par une CA (Certificate Authority)

Remarque

- Les fonctions grisées et n'apparaissant pas sous forme de lien indiquent qu'elles ne sont pas disponibles.
- Pour en savoir plus sur la configuration, consultez le texte d'aide dans la gestion via le Web.

Création d’un certificat auto-signé

1. Cliquez sur **Créer un certificat auto signé**.
2. Entrez un **Nom commun** et un **Date de validité**.

Remarque

- La longueur du **Nom commun** doit être inférieure à 64 caractères. Entrez un identifiant comme une adresse IP, un nom de nœud ou un nom de domaine à utiliser au cours de l’accès à cet appareil via une communication SSL/TLS. Le nom du nœud est affiché par défaut.
- Une fenêtre contextuelle d’avertissement apparaîtra si vous utilisez le protocole IPPS ou HTTPS et entrez un autre nom dans l’URL que le **Nom commun** utilisé pour le certificat auto-signé.

3. Vous avez le choix entre les paramètres **Algorithme de clé publique** et **Algorithme de chiffrement** dans la liste déroulante. Les réglages par défaut sont **RSA (2048 bits)** pour **Algorithme de clé publique** et **SHA256** pour **Algorithme de chiffrement**.
4. Cliquez sur **Envoyer**.
5. Le certificat auto-signé a été créé et est correctement enregistré dans la mémoire de votre appareil.

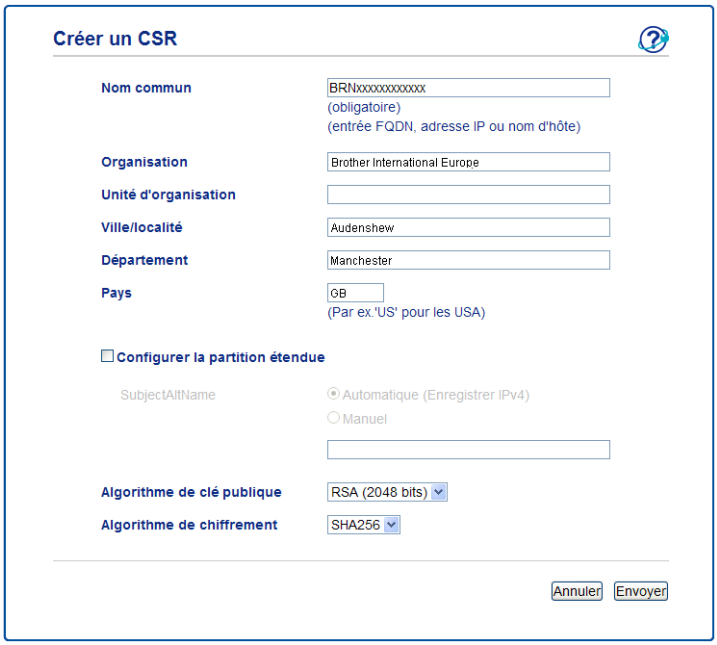
Création d’une demande de signature de certificat (CSR)

Une demande de signature de certificat (Certificate Signing Request, CSR) est une demande envoyée à une CA afin d’authentifier les informations d’identification figurant sur le certificat.

Remarque

Nous vous conseillons d’installer le Root Certificate du CA sur votre ordinateur avant de créer la CSR.

1. Cliquez sur **Créer un CSR**.
2. Entrez un **Nom commun** ainsi que vos informations, comme **Organisation**.
   Les informations relatives à votre société sont nécessaires pour qu’une CA puisse confirmer votre identité à des tiers.



Remarque

- La longueur du **Nom commun** doit être inférieure à 64 caractères. Entrez un identifiant comme une adresse IP, un nom de nœud ou un nom de domaine à utiliser au cours de l’accès à cet appareil via une communication SSL/TLS. Le nom du nœud est affiché par défaut. Le **Nom commun** est nécessaire.
- Une fenêtre contextuelle d’avertissement apparaîtra si vous entrez un nom commun différent dans l’URL que celui utilisé pour le certificat.
- La longueur de l’**Organisation**, de l’**Unité d'organisation**, de la **Ville/localité** et du **Département** doit être inférieure à 64 caractères.
- Le **Pays** devrait être un code pays ISO 3166 composé de deux caractères.
- Si vous configurez l’extension de certificat X.509v3, activez la case à cocher **Configurer la partition étendue**, puis sélectionnez **Automatique (Enregistrer IPv4)** ou **Manuel**.

3 Vous avez le choix entre les paramètres **Algorithme de clé publique** et **Algorithme de chiffrement** dans la liste déroulante. Les réglages par défaut sont **RSA (2048 bits)** pour **Algorithme de clé publique** et **SHA256** pour **Algorithme de chiffrement**.

4 Cliquez sur **Envoyer**. L'écran suivant apparaît.

5 Après quelques instants, le certificat apparaît et vous pouvez l'enregistrer dans un fichier de petite taille ou le copier-coller directement dans un formulaire de CSR en ligne fourni par une CA (Certificate Authority). Cliquez sur **Enregistrer** pour enregistrer le fichier de CSR sur votre ordinateur.

Remarque

Suivez la politique de votre CA concernant la méthode d'envoi d'une CSR.

6 La CSR est désormais créée. Pour obtenir des instructions relatives à la procédure d'installation du certificat sur votre appareil, consultez *Comment installer le certificat sur votre appareil* ➤➤ page 9.

Comment installer le certificat sur votre appareil

Lorsque vous recevez le certificat du CA, suivez les étapes ci-dessous pour l'installer sur le serveur d'impression.

Remarque

Seul un certificat émis avec la CSR de cet appareil peut être installé. Si vous souhaitez créer une autre CSR, vérifiez que le certificat est installé avant de la créer. Installez le certificat sur l'appareil avant de créer une autre CSR. Sinon, la CSR créée avant l'installation ne sera pas valide.

1. Cliquez sur **Installer le certificat** sur la page **Certificat**.

2. Précisez le fichier du certificat émis par un CA, puis cliquez sur **Envoyer**.

3. Le certificat a été créé et est maintenant correctement enregistré dans la mémoire de votre appareil. Pour utiliser la communication SSL/TLS, le Root Certificate du CA doit être installé sur votre ordinateur. Contactez votre administrateur réseau au sujet de l'installation.
Vous avez terminé la configuration du certificat numérique. Si vous souhaitez envoyer ou recevoir un e-mail au moyen de SSL, consultez *Envoi ou réception (pour les modèles DCP et MFC) sécurisés d'e-mails* ➤➤ page 25 pour connaître la procédure de configuration à suivre.

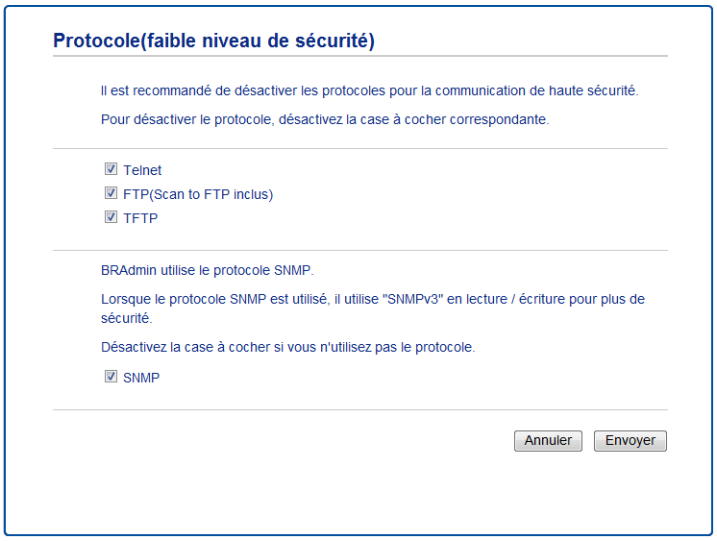
Choix du certificat

Lorsque vous avez installé le certificat, suivez les étapes ci-dessous pour choisir le certificat à utiliser.

1. Cliquez sur **Réseau**.
2. Cliquez sur **Protocole**.
3. Cliquez sur **Paramètres du serveur HTTP**, puis choisissez le certificat dans la liste déroulante **Sélectionnez le certificat**.

Remarque

- Pour une communication sécurisée, Brother recommande de désactiver les protocoles Telnet, FTP, TFTP et la gestion réseau avec des versions antérieures de BRAdmin Professional (2.8 ou inférieur) si la boîte de dialogue suivante s'affiche. Si vous les activez, l'authentification des utilisateurs ne sera pas sécurisée.



- Pour les modèles DCP et MFC :

  Si vous désactivez FTP, la fonction Numériser vers FTP est désactivée.

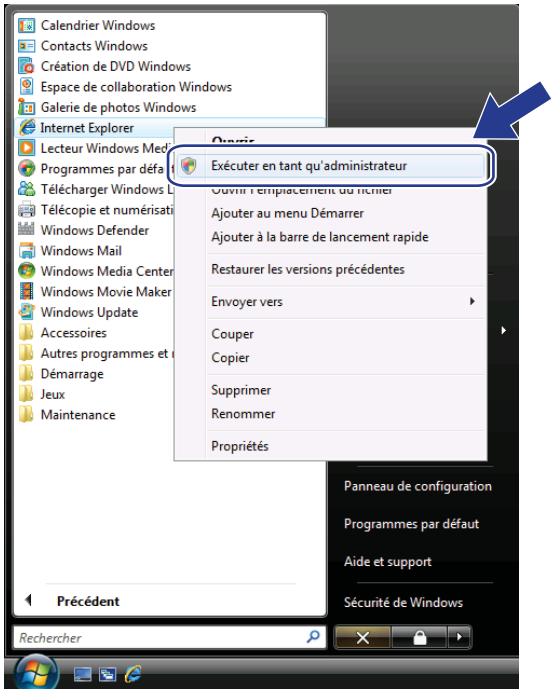
4 Cliquez sur **Envoyer**.

Installation du certificat auto-signé ou pré-installé pour les utilisateurs de Windows Vista®, Windows® 7 et Windows Server® 2008 avec des droits d'administrateur

Remarque

- Les étapes suivantes sont pour Windows® Internet Explorer®. Si vous utilisez un autre navigateur web, suivez le texte d'aide du navigateur web lui-même.
- Vous devez disposer de droits d'administrateur pour installer le certificat auto-signé ou pré-installé.

1. Cliquez sur le bouton puis sur **Tous les programmes**.
2. Cliquez avec le bouton droit sur **Internet Explorer**, puis cliquez sur **Exécuter en tant qu'administrateur**.



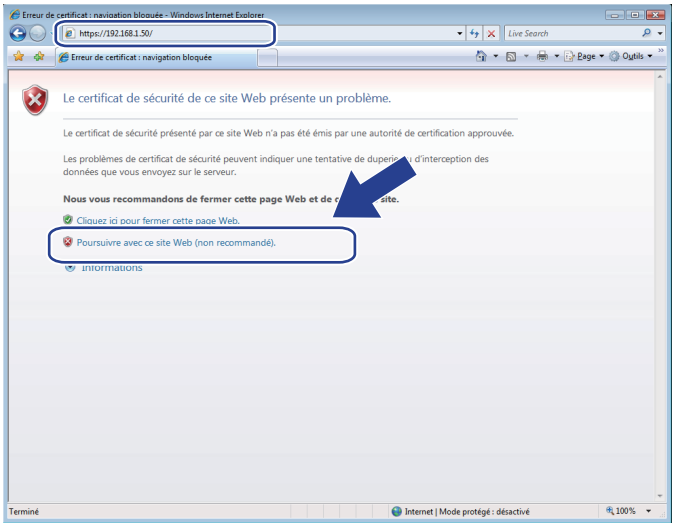
Remarque

Si l'écran **Contrôle de compte d'utilisateur** s'affiche,

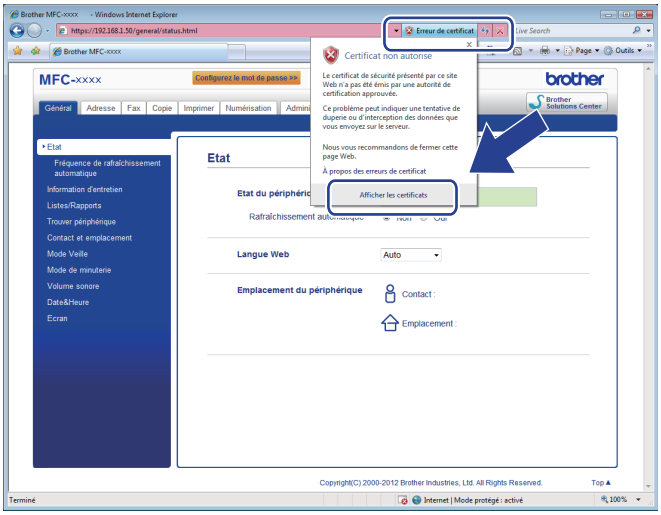
(Windows Vista®) Cliquez sur **Continuer (Autoriser)**.

(Windows® 7) Cliquez sur **Oui**.

❸ Tapez « https://adresse IP de l'appareil/ » dans votre navigateur pour accéder à votre appareil (où « adresse IP de l'appareil » correspond à l'adresse IP de l'appareil ou au nom de nœud attribué pour le certificat).
Puis cliquez sur **Poursuivre avec ce site Web (non recommandé)**.

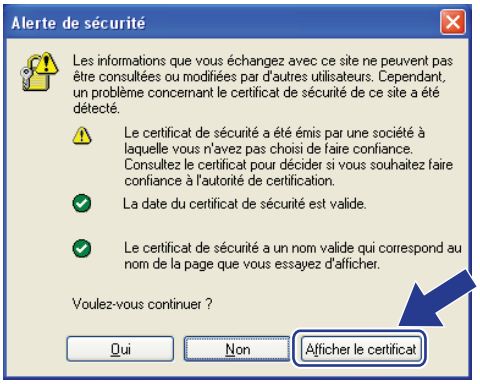


❹ Cliquez sur **Erreur de certificat** puis sur **Afficher les certificats**. Pour le reste des instructions, suivez la procédure à partir de l'étape ❹ de la section *Installation du certificat auto-signé ou pré-installé pour les utilisateurs de Windows® XP et Windows Server® 2003* ➤➤ page 14.

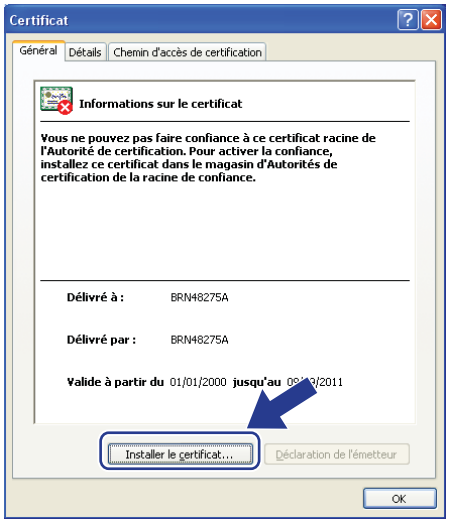


Installation du certificat auto-signé ou pré-installé pour les utilisateurs de Windows® XP et Windows Server® 2003

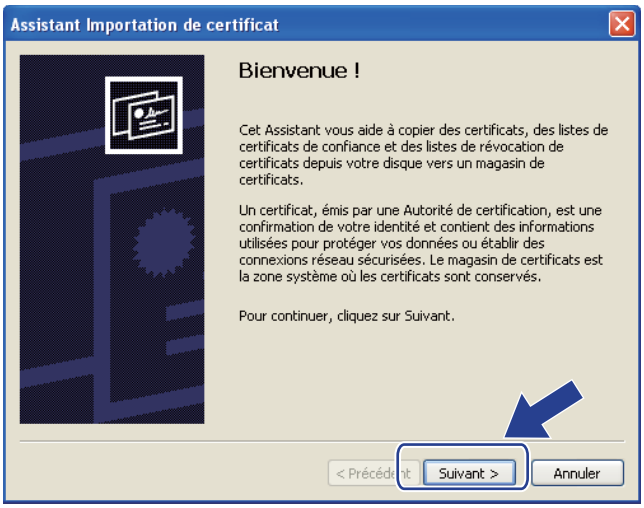
1. Lancez votre navigateur Web.
2. Tapez « https://adresse IP de l'appareil/ » dans votre navigateur pour accéder à votre appareil (où « adresse IP de l'appareil » correspond à l'adresse IP ou au nom de nœud attribué pour le certificat).
3. Lorsque la boîte de dialogue d'alerte de sécurité apparaît, effectuez l'une des opérations suivantes :
   - Cliquez sur **Poursuivre avec ce site Web (non recommandé)**. Cliquez sur **Erreur de certificat** puis sur **Afficher les certificats**.
   - Si la boîte de dialogue suivante apparaît, cliquez sur **Afficher le certificat**.



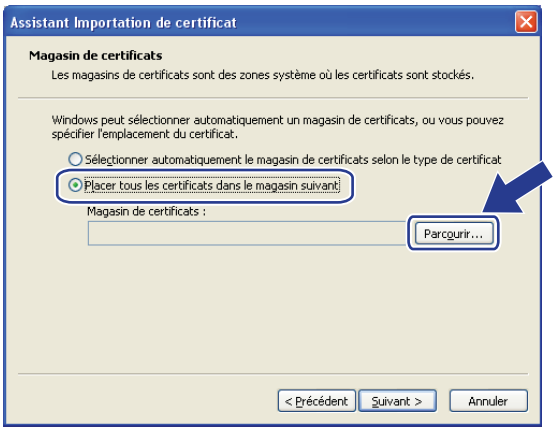
4. Cliquez sur **Installer le certificat...** à partir de l'onglet **Général**.



5 Lorsque **Assistant Importation de certificat** apparaît, cliquez sur **Suivant**.

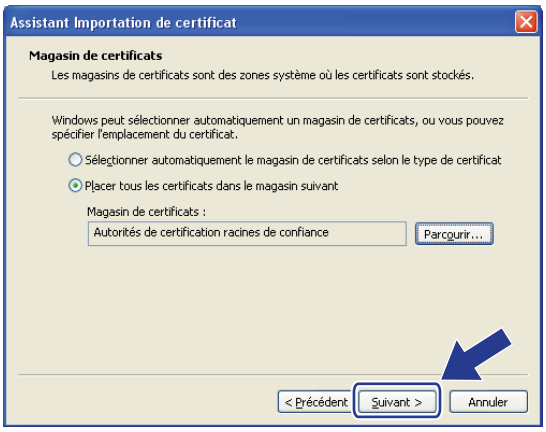


6 Vous devez spécifier l'emplacement d'installation du certificat. Il est recommandé de sélectionner **Placer tous les certificats dans le magasin suivant**, puis de cliquer sur **Parcourir...**.



7 Choisissez **Autorités de certification racines de confiance** puis cliquez sur **OK**.

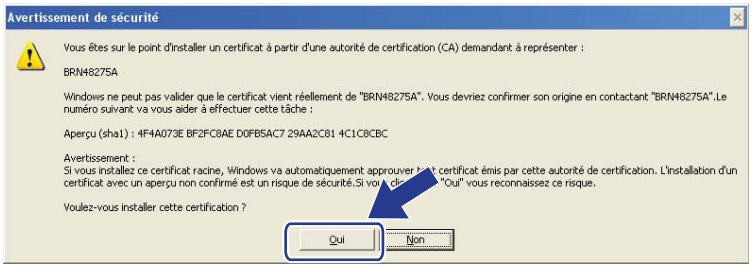
8 Cliquez sur **Suivant**.



9 Dans l'écran suivant, cliquez sur **Terminer**.

10 Vous serez ensuite invité à installer le certificat.
Effectuez l'une des opérations suivantes :

- Si vous installez le certificat auto-signé, vérifiez l'empreinte digitale (empreinte du pouce), puis cliquez sur **Oui**.
- Si vous installez le certificat pré-installé, cliquez sur **Oui**.



Remarque

- Pour le certificat auto-signé, l'empreinte digitale (empreinte du pouce) est imprimée sur le rapport de configuration réseau.

  Pour savoir comment imprimer la configuration réseau, consultez *Impression de la page Paramètres imprimante (Pour HL-5450DN(T))* ➤➤ page 29 ou *Impression du rapport de configuration réseau (pour les autres modèles)* ➤➤ page 29.

- Pour le certificat pré-installé, l'empreinte digitale n'est pas imprimée sur le rapport de configuration réseau.

11 Cliquez sur **OK**.

12 Le certificat auto-signé ou pré-installé est à présent installé sur votre ordinateur et la communication SSL/TLS est disponible.

Chaque ordinateur souhaitant imprimer de manière sécurisée doit procéder de la même manière. Toutefois, une fois ce certificat installé, il ne sera plus nécessaire de répéter ces étapes, sauf si le certificat est modifié.

Importez et exportez le certificat et la clé privée

Vous pouvez stocker le certificat et la clé privée sur l'appareil et les gérer en procédant à des importations et exportations.

Comment importer le certificat auto-signé, le certificat émis par la CA et la clé privée

1. Cliquez sur **Importer le certificat et la clé secrète** sur la page **Certificat**.
2. Précisez le fichier à importer.
3. Entrez le mot de passe si le fichier est crypté, puis cliquez sur **Envoyer**.
4. Le certificat et la clé privée sont maintenant correctement importés dans votre appareil.

Comment exporter le certificat auto-signé, le certificat émis par la CA et la clé privée

1. Cliquez sur **Exporter** affiché avec **Liste des certificats** sur le page **Certificat**.
2. Entrez un mot de passe si vous souhaitez crypter le fichier.

Remarque

Si le mot de passe est laissé vide, la sortie ne sera pas cryptée.

3. Entrez à nouveau le mot de passe pour confirmation, puis cliquez sur **Envoyer**.
4. Précisez l'emplacement souhaité pour l'enregistrement du fichier.
5. Le certificat et la clé privée sont à présent bien exportés vers votre ordinateur.

Importer et exporter un certificat CA

Vous pouvez stocker un certificat sur l'appareil en procédant à des importations et exportations.

Comment importer un certificat CA

1. Cliquez sur **Certificat AC** sur la page **Sécurité**.
2. Cliquez sur **Importer un certificat AC**, puis sélectionnez le certificat. Cliquez sur **Envoyer**.

Comment exporter un certificat CA

1. Cliquez sur **Certificat AC** sur la page **Sécurité**.
2. Sélectionnez le certificat à exporter et cliquez sur **Exporter**. Cliquez sur **Envoyer**.
3. Cliquez sur **Enregistrer**, puis sélectionnez le dossier de destination.
4. Choisissez l'emplacement dans lequel vous voulez enregistrer le certificat exporté, puis enregistrez ce dernier.

Gestion de plusieurs certificats

Les certificats multiples vous permettent de gérer chaque certificat installé à l'aide de la Gestion à partir du Web. Lorsque vous avez installé des certificats, vous pouvez vérifier les certificats installés à partir de la page **Certificat**, puis afficher le contenu de chaque certificat, supprimer le certificat ou l'exporter. Pour plus d'informations sur la manière d'accéder à la page **Certificat**, consultez *Installation d'un certificat numérique* ➤➤ page 4.

- Pour les modèles d'imprimantes

  L'appareil Brother permet de stocker jusqu'à trois certificats auto-signés ou jusqu'à trois certificats émis par une CA. Les certificats stockés vous permettront d'utiliser le protocole HTTPS/IPPS ou l'authentification IEEE 802.1x.

- Pour les modèles DCP et MFC

  L'appareil Brother permet de stocker jusqu'à quatre certificats auto-signés ou jusqu'à quatre certificats émis par une CA. Les certificats stockés vous permettront d'utiliser le protocole HTTPS/IPPS, l'authentification IEEE 802.1x ou un PDF signé.

Vous pouvez également stocker jusqu'à quatre ou six (HL-S7000DN) certificats CA afin d'utiliser l'authentification IEEE 802.1x ainsi que SSL pour SMTP/POP3.

Nous vous recommandons de stocker un certificat de moins et de laisser le dernier libre pour pouvoir faire face à une éventuelle expiration de certificat. Par exemple, si vous souhaitez stocker un certificat CA, stockez trois certificats et conservez un emplacement de stockage de réserve. En cas de réémission du certificat, par exemple lors de son expiration, vous pouvez importer un nouveau certificat dans l'emplacement de réserve, puis supprimer le certificat arrivé à expiration afin d'éviter toute défaillance de la configuration.

Remarque

- Lorsque vous utilisez le protocole HTTPS/IPPS, IEEE 802.1x ou un PDF signé (pour les modèles DCP et MFC), vous devez choisir le certificat à employer.
- Lorsque vous utilisez les protocoles SSL pour les communications SMTP/POP3 (pour les modèles DCP et MFC), il n'est pas nécessaire de choisir le certificat. Le certificat qui convient sera déterminé automatiquement.

3 Gestion sécurisée de votre appareil réseau à l'aide de SSL/TLS

Pour une gestion sécurisée de votre appareil réseau, vous devez utiliser les utilitaires de gestion avec des protocoles de sécurité.

Gestion sécurisée à l'aide de la gestion via le Web (navigateur Web)

Nous vous conseillons d'utiliser le protocole HTTPS pour une gestion sécurisée. Pour utiliser ces protocoles, les paramètres d'appareil suivants sont nécessaires.

Remarque

- Le protocole HTTPS est activé par défaut.

  Vous pouvez modifier les paramètres du protocole HTTPS et le certificat à utiliser en cliquant sur **Réseau**, sur **Protocole**, puis sur **Paramètres du serveur HTTP** dans l'écran Gestion à partir du Web.
- Le certificat que vous avez installé sur l'appareil doit également l'être sur votre ordinateur. Consultez *Installation du certificat auto-signé ou pré-installé pour les utilisateurs de Windows Vista®, Windows® 7 et Windows Server® 2008 avec des droits d'administrateur* ➤➤ page 12 ou *Installation du certificat auto-signé ou pré-installé pour les utilisateurs de Windows® XP et Windows Server® 2003* ➤➤ page 14.

1. Lancez votre navigateur Web.
2. Tapez « https://adresse IP de l'appareil/ » dans votre navigateur. (Si vous utilisez le certificat que vous avez créé, tapez « https://Nom commun/ » dans votre navigateur. Où « Nom commun » est le nom commun que vous avez affecté au certificat, notamment une adresse IP, un nom de nœud ou un nom de domaine. Pour savoir comment attribuer un nom commun au certificat, consultez *Utilisation de certificats pour la sécurité de la machine* ➤➤ page 2.)

   ■ Par exemple :

   https://192.168.1.2/ (si le nom commun est l'adresse IP de l'appareil)
3. Aucun mot de passe n'est requis par défaut. Saisissez un mot de passe si vous en avez défini un, puis appuyez sur .

4 Impression sécurisée de documents à l’aide de SSL

Impression sécurisée de documents à l’aide d’IPPS pour Windows®

Nous vous conseillons d’utiliser le protocole IPPS pour une gestion sécurisée. Pour utiliser le protocole IPPS, les paramètres d’appareil suivants sont nécessaires.

Remarque

- Une communication à l’aide du protocole IPPS ne peut pas bloquer un accès non autorisé au serveur d’impression.
- Le certificat que vous avez installé sur l’appareil doit également l’être sur votre ordinateur. Consultez *Installation du certificat auto-signé ou pré-installé pour les utilisateurs de Windows Vista®, Windows® 7 et Windows Server® 2008 avec des droits d’administrateur* ➤➤ page 12 ou *Installation du certificat auto-signé ou pré-installé pour les utilisateurs de Windows® XP et Windows Server® 2003* ➤➤ page 14.
- Le protocole IPPS doit être activé. Réglage par défaut : activé. Vous pouvez modifier les paramètres du protocole IPPS et le certificat à utiliser en cliquant sur **Réseau**, sur **Protocole**, puis sur **Paramètres du serveur HTTP** dans l’écran Gestion à partir du Web.

Windows® XP et Windows Server® 2003

1. Cliquez sur **Démarrer**, puis choisissez **Imprimantes et télécopieurs**.
2. Cliquez sur **Ajouter une imprimante** pour lancer **Assistant Ajoute d'imprimante**.
3. Cliquez sur **Suivant** lorsque l’écran **Assistant Ajoute d'imprimante** s’affiche.
4. Choisissez **Une imprimante réseau ou une imprimante connectée à un autre ordinateur**.
5. Cliquez sur **Suivant**.
6. Choisissez **Se connecter à une imprimante sur Internet ou sur un réseau domestique ou d'entreprise**, puis saisissez le texte suivant dans le champ d’URL :
« https://adresse IP de l’appareil/ipp » (où « adresse IP de l’appareil » correspond à l’adresse IP ou au nom de nœud de l’appareil).

Remarque

- Il est important d'utiliser le préfixe « https:// », et non « http:// ». Sinon, l'impression via IPP ne sera pas sécurisée.
- Si vous avez modifié le fichier hosts sur votre ordinateur ou si vous utilisez un système DNS (Domain Name System), vous pouvez également entrer le nom DNS du serveur d'impression. Comme le serveur d'impression prend en charge les noms TCP/IP et NetBIOS, vous pouvez également entrer le nom NetBIOS du serveur d'impression. Le nom NetBIOS figure dans le rapport de configuration réseau. (Pour savoir comment imprimer le rapport de configuration réseau, consultez *Impression de la page Paramètres imprimante (Pour HL-5450DN(T))* ➤➤ page 29 ou *Impression du rapport de configuration réseau (pour les autres modèles)* ➤➤ page 29.) Le nom NetBIOS affecté correspond aux 15 premiers caractères du nom du nœud, et il apparaît par défaut sous la forme « BRNxxxxxxxxxxxx » pour un réseau filaire, ou « BRWxxxxxxxxxxxx » pour un réseau sans fil. (« xxxxxxxxxxxx » est l'Adresse MAC / Adresse Ethernet de votre machine.)

7 Lorsque vous cliquez sur **Suivant**, Windows® XP et Windows Server® 2003 établissent une connexion avec l'URL spécifiée.

- Si le pilote d'imprimante est déjà installé :

  L'écran de sélection d'imprimante s'affiche dans l'**Assistant Ajoute d'imprimante**.

  Passez à l'étape ⓫.

- Si le pilote d'imprimante N'est PAS encore installé :

  L'un des avantages du protocole d'impression IPP est qu'il détermine le nom de modèle de l'imprimante avec laquelle vous communiquez. Après une communication réussie, vous verrez automatiquement le nom de modèle de l'imprimante et vous n'aurez donc pas besoin d'indiquer à Windows® XP ou Windows Server® 2003 le type de pilote d'imprimante à utiliser.

  Passez à l'étape ❽.

Remarque

Si le pilote d'imprimante que vous êtes en train d'installer ne dispose pas d'un certificat numérique, un message d'avertissement s'affiche. Pour poursuivre l'installation, cliquez sur **Continuer**.

8 Cliquez sur **Disque fourni**. Vous serez ensuite invité à insérer le disque du pilote.

9 Cliquez sur **Parcourir** et sélectionnez le pilote d'imprimante Brother approprié sur le CD-ROM ou dans le partage réseau.
Cliquez sur **OK**.

10 Cliquez sur **OK**.

11 Sélectionnez votre appareil, puis cliquez sur **OK**.

12 Activez la case à cocher **Oui** si vous souhaitez utiliser cet appareil comme imprimante par défaut.
Cliquez sur **Suivant**.

13 Cliquez sur **Terminer**. L'imprimante est maintenant configurée et prête à imprimer. Pour tester la connexion de l'imprimante, imprimez une page de test.

Windows Vista®, Windows® 7 et Windows Server® 2008

1. (Windows Vista®)
   Cliquez sur le bouton , sur **Panneau de configuration**, **Matériel et audio**, puis sur **Imprimantes**.
   (Windows® 7)
   Cliquez sur le bouton , puis sur **Périphériques et imprimantes**.
   (Windows Server® 2008)
   Cliquez sur **Démarrer**, sur **Panneau de configuration**, sur **Matériel et audio**, puis sur **Imprimantes**.
2. Cliquez sur **Ajouter une imprimante**.
3. Choisissez **Ajouter une imprimante réseau, sans fil ou Bluetooth**.
4. Cliquez sur **L'imprimante que je veux n'set pas répertoriée**.
5. Choisissez **Sélectionner une imprimante partagée par nom**, puis saisissez le texte suivant dans le champ d'URL : « https://adresse IP de l'appareil/ipp » (où « adresse IP de l'appareil » correspond à l'adresse IP ou au nom de nœud de l'appareil).

Remarque

- Il est important d'utiliser le préfixe « https:// », et non « http:// ». Sinon, l'impression via IPP ne sera pas sécurisée.
- Si vous avez modifié le fichier hosts sur votre ordinateur ou si vous utilisez un système DNS (Domain Name System), vous pouvez également entrer le nom DNS du serveur d'impression. Comme le serveur d'impression prend en charge les noms TCP/IP et NetBIOS, vous pouvez également entrer le nom NetBIOS du serveur d'impression. Le nom NetBIOS figure dans le rapport de configuration réseau. (Pour savoir comment imprimer le rapport de configuration réseau, consultez *Impression de la page Paramètres imprimante (Pour HL-5450DN(T))* ➤➤ page 29 ou *Impression du rapport de configuration réseau (pour les autres modèles)* ➤➤ page 29.) Le nom NetBIOS affecté correspond aux 15 premiers caractères du nom du nœud, et il apparaît par défaut sous la forme « BRNxxxxxxxxxxxx » pour un réseau filaire, ou « BRWxxxxxxxxxxxx » pour un réseau sans fil. (« xxxxxxxxxxxx » est l'Adresse MAC / Adresse Ethernet de votre machine.)

6. Lorsque vous cliquez sur **Suivant**, Windows Vista® et Windows Server® 2008 établissent une connexion avec l'URL spécifiée.
   - Si le pilote d'imprimante est déjà installé :

     L'écran de sélection d'imprimante s'affiche dans l'Assistant Ajouter une imprimante. Cliquez sur **OK**.

     Si vous avez déjà installé le pilote d'imprimante approprié sur votre ordinateur, Windows Vista® et Windows Server® 2008 utiliseront automatiquement ce pilote. Dans ce cas, il vous suffira de préciser si vous souhaitez utiliser ce pilote par défaut pour terminer l'Assistant d'installation du pilote. Vous êtes maintenant prêt à imprimer.

     Passez à l'étape ⓫.

■ Si le pilote d'imprimante N'est PAS encore installé :

L'un des avantages du protocole d'impression IPP est qu'il détermine le nom de modèle de l'imprimante avec laquelle vous communiquez. Après une communication réussie, vous verrez automatiquement le nom de modèle de l'imprimante et vous n'aurez donc pas besoin d'indiquer à Windows Vista® et Windows Server® 2008 le type de pilote d'imprimante à utiliser.

Passez à l'étape ❼.

7 Si votre appareil ne figure pas sur la liste des imprimantes prises en charge, cliquez sur **Disque fourni**. Vous serez ensuite invité à insérer le disque du pilote.

8 Cliquez sur **Parcourir** et sélectionnez le pilote d'imprimante Brother approprié sur le CD-ROM ou dans le partage réseau. Cliquez sur **Ouvrir**.

9 Cliquez sur **OK**.

10 Spécifiez le nom de modèle de l'appareil. Cliquez sur **OK**.

Remarque

- Lorsque l'écran Contrôle de compte d'utilisateur apparaît, cliquez sur **Continuer**.
- Si le pilote d'imprimante que vous êtes en train d'installer ne dispose pas d'un certificat numérique, un message d'avertissement s'affiche. Pour poursuivre l'installation, cliquez sur **Installer ce pilote quand même**. L'**Ajouter une imprimante** s'achèvera ensuite.

11 L'écran **Entrer un nom d'imprimante** s'affiche dans l'Assistant **Ajouter une imprimante**. Activez la case à cocher **Définir en tant qu'imprimante par défaut** si vous souhaitez utiliser cet appareil comme imprimante par défaut, puis cliquez sur **Suivant**.

12 Pour tester la connexion de l'imprimante, cliquez sur **Imprimer une page de test**, puis sur **Terminer**. L'appareil est maintenant configuré et prêt à imprimer.

5 Envoi ou réception (pour les modèles DCP et MFC) sécurisés d’e-mails

Configuration à l’aide de la gestion via le Web (navigateur Web)

Vous pouvez configurer l’envoi sécurisé d’e-mails avec authentification de l’utilisateur ou l’envoi et la réception (pour les modèles DCP et MFC) d’e-mails à l’aide de SSL/TLS dans l’écran Gestion à partir du Web.

1. Lancez votre navigateur Web.
2. Tapez « http://adresse IP de l’appareil/ » dans votre navigateur (où « adresse IP de l’appareil » correspond à l’adresse IP ou au nom de nœud de l’appareil).
   - Par exemple :

     http://192.168.1.2/
3. Aucun mot de passe n’est requis par défaut. Saisissez un mot de passe si vous en avez défini un, puis appuyez sur →.
4. Cliquez sur **Réseau**.
5. Cliquez sur **Protocole**.
6. Cliquez sur l’option **Paramètres avancés** de **POP3/SMTP** et vérifiez que l’état de **POP3/SMTP** est **Activé**.
7. Vous pouvez configurer les paramètres du **POP3/SMTP** sur cette page.

Remarque

- Pour obtenir des compléments d’information, voir le texte d’aide dans la gestion via le Web.
- Vous pouvez aussi confirmer si les paramètres e-mail sont corrects après les avoir configurés en envoyant un e-mail de test.
- Si vous ne connaissez pas les paramètres du serveur POP3/SMTP, contactez votre administrateur système ou votre FAI (fournisseur d’accès Internet) pour obtenir ces informations.

8. Après la configuration, cliquez sur **Envoyer**. L’écran **Test de la configuration d'envoi des e-mails** ou **Test de la configuration d'envoi/réception des e-mails** s’affiche.
9. Suivez les consignes qui s’affichent à l’écran si vous souhaitez tester les paramètres actuels.

Envoi ou réception (pour les modèles DCP et MFC) sécurisés d’e-mails à l’aide de SSL/TLS

Cet appareil prend en charge les méthodes SSL/TLS pour l’envoi ou la réception (pour les modèles DCP et MFC) d’un e-mail via un serveur de messagerie exigeant une communication SSL/TLS sécurisée. Pour envoyer ou recevoir un e-mail via un serveur de messagerie utilisant une communication SSL/TLS, vous devez configurer correctement SMTP over SSL/TLS ou POP3 over SSL/TLS.

Vérification du certificat serveur

- Si vous choisissez SSL ou TLS pour **SMTP via SSL/TLS** ou **POP3 via SSL/TLS**, la case **Vérifier le certificat de serveur** exigeant la vérification du certificat serveur est automatiquement cochée.
  - Avant de vérifier le certificat serveur, vous devez importer le certificat CA émis par la CA qui a signé le certificat serveur. Contactez votre administrateur réseau ou votre FAI (fournisseur d’accès Internet) afin de déterminer si l’importation d’un certificat CA est nécessaire ou non. Pour importer le certificat, consultez *Importer et exporter un certificat CA* ➤➤ page 18.
  - Si vous ne devez pas vérifier le certificat serveur, décochez la case **Vérifier le certificat de serveur**.

Numéro de port

- Si vous choisissez SSL ou TLS, la valeur du **Port SMTP** ou du **Port POP3** est modifiée en fonction du protocole. Si vous souhaitez modifier manuellement le numéro de port, sélectionnez **SMTP via SSL/TLS** ou **POP3 via SSL/TLS**, puis entrez le numéro de port de votre choix.
- Vous devez configurer la méthode de communication POP3/SMTP en fonction du serveur de messagerie. Pour plus de détails sur les paramètres du serveur de messagerie, contactez votre administrateur réseau ou votre FAI (fournisseur d’accès Internet). Généralement, les services de messagerie Web sécurisés exigent les paramètres suivants :
  - **SMTP**
    - **Port SMTP** : 587
    - **Méthode d’authentification du serveur SMTP** : SMTP-AUTH
    - **SMTP over SSL/TLS** : TLS
  - **POP3**
    - **Port POP3** : 995
    - **POP3 over SSL/TLS** : SSL

6 Diagnostic des anomalies

Généralités

Ce chapitre explique comment régler les problèmes de réseau courants que vous pourriez éventuellement rencontrer en utilisant l'appareil Brother. Si ce chapitre ne vous permet pas de résoudre votre problème, veuillez consulter le Brother Solutions Center à l'adresse (http://solutions.brother.com/).

Visitez le Brother Solutions Center à l'adresse (http://solutions.brother.com/) et cliquez sur Manuels sur la page de votre modèle pour télécharger les autres manuels.

Identification de votre problème

Vérifiez que les éléments suivants sont configurés avant de lire ce chapitre.

Vérifiez d'abord les points suivants :
Le cordon d'alimentation CA est correctement connecté et l'appareil Brother est allumé.
Tous les éléments de protection ont été retirés de l'appareil.
Les cartouches de toner et le tambour ou de cartouches d'encre (HL-S7000DN) sont correctement installés.
Les capots avant et arrière sont bien fermés.
Le papier est correctement placé dans le bac à papier.
L'appareil est correctement connecté au réseau.

Accédez à la page correspondant à votre problème dans la liste ci-dessous

- Je ne peux pas imprimer le document via Internet avec IPPS.

  Consultez *Je ne peux pas imprimer le document via Internet avec IPPS.* ➤➤ page 28.
- Je souhaite vérifier que mes périphériques réseau fonctionnent correctement.

  Consultez *Je souhaite vérifier que mes périphériques réseau fonctionnent correctement.* ➤➤ page 28.

Je ne peux pas imprimer le document via Internet avec IPPS.

Question	Solution
Je ne peux pas communiquer avec mon appareil Brother à l'aide de SSL.	■ Procurez-vous un certificat valide et installez-le à nouveau sur l'appareil et sur l'ordinateur. ■ Vérifiez que le réglage du port de votre appareil est correct. Vous pouvez vérifier le réglage du port de votre appareil en cliquant sur **Réseau**, sur **Protocole**, puis sur **Paramètres du serveur HTTP** dans l'écran Gestion à partir du Web.

Je souhaite vérifier que mes périphériques réseau fonctionnent correctement.

Question	Solution
Votre appareil Brother est-il sous tension ?	Assurez-vous que vous avez bien vérifié toutes les instructions de la section *Vérifiez d'abord les points suivants :* ➤➤ page 27.
Où puis-je trouver les paramètres réseau de mon appareil Brother, tels que l'adresse IP ?	Imprimez le rapport de configuration réseau. Consultez *Impression de la page Paramètres imprimante (Pour HL-5450DN(T))* ➤➤ page 29 ou *Impression du rapport de configuration réseau (pour les autres modèles)* ➤➤ page 29.

Impression de la page Paramètres imprimante (Pour HL-5450DN(T))

Remarque

Nom du nœud : nom du nœud qui apparaît dans le rapport de configuration réseau. Le nom du nœud par défaut est « BRNxxxxxxxxxxxx ». (« xxxxxxxxxxxx » est l'Adresse MAC / Adresse Ethernet de votre machine.)

La page Paramètres imprimante imprime un rapport qui dresse la liste des paramètres actuels de l'imprimante, avec notamment les paramètres du serveur d'impression réseau.

Vous pouvez imprimer la page Paramètres imprimante en utilisant le bouton **Go** sur l'appareil.

1. Vérifiez que le capot avant est fermé et que le cordon d'alimentation est branché.
2. Mettez l'appareil sous tension et attendez que l'appareil passe à l'état Prêt.
3. Appuyez à trois reprises sur **Go** dans les 2 secondes. L'appareil imprime la page Paramètres imprimante actuelle.

Impression du rapport de configuration réseau (pour les autres modèles)

Remarque

Nom du nœud : nom du nœud qui apparaît dans le rapport de configuration réseau. Le nom du nœud par défaut est « BRNxxxxxxxxxxxx » pour un réseau filaire ou « BRWxxxxxxxxxxxx » pour un réseau sans fil. (« xxxxxxxxxxxx » est l'Adresse MAC / Adresse Ethernet de votre machine.)

Le rapport de configuration réseau est un rapport qui dresse la liste des paramètres réseau actuels, avec notamment les paramètres du serveur d'impression.

Pour HL-5470DW(T) et HL-6180DW(T)

1. Appuyez sur ▲ ou ▼ pour sélectionner `Info. appareil`.
   Appuyez sur **OK**.
2. Appuyez sur ▲ ou ▼ pour sélectionner `Impr conf réseau`.
   Appuyez sur **OK**.

Pour DCP-8110DN, DCP-8150DN, DCP-8155DN, MFC-8510DN, MFC-8710DW et MFC-8910DW

1. Appuyez sur **Menu**.
2. (Pour les modèles MFC) Appuyez sur ▲ ou ▼ pour sélectionner `Impr. rapports`.
   (Pour les modèles DCP) Appuyez sur ▲ ou ▼ pour sélectionner `Info. appareil`.
   Appuyez sur **OK**.
3. Appuyez sur ▲ ou ▼ pour sélectionner `Config Réseau`.
   Appuyez sur **OK**.
4. Appuyez sur **Marche**.

Pour DCP-8250DN et MFC-8950DW(T)

1. Appuyez sur `Menu`.
2. Appuyez sur ▲ ou ▼ pour afficher `Impr. rapports`, puis appuyez sur `Impr. rapports`.
3. Appuyez sur `Config Réseau`.
4. Appuyez sur **Marche**.

Pour HL-S7000DN

1. Appuyez sur **Menu**.
2. Appuyez sur ▲ ou sur ▼ pour choisir `Info. appareil`.
   Appuyez sur **OK**.
3. Appuyez sur ▲ ou sur ▼ pour choisir `Impr conf réseau`.
   Appuyez sur **OK**.

Remarque

Si l'**IP Address** indiquée dans le rapport de configuration réseau est **0.0.0.0**, attendez une minute et réessayez.

Termes et concepts relatifs aux réseaux

Aperçu technique de SSL

SSL (Secure Socket Layer) est une méthode de protection des données de la couche transport transitant sur un réseau local ou étendu via IPP (Internet Printing Protocol) afin d'empêcher les utilisateurs non autorisés de les lire.

Pour ce faire, elle utilise des protocoles d'authentification sous la forme de clés numériques de 2 types :

- Une clé publique, connue de tous ceux qui impriment.
- Une clé privée, connue uniquement de l'appareil utilisé pour décrypter les paquets et les rendre de nouveau lisibles par l'appareil.

La clé publique utilise le cryptage 1 024 bits ou 2 048 bits, et est incluse dans un certificat numérique. Ces certificats peuvent être auto-signés ou agréés par une CA (Certificate Authority).

En premier lieu, il existe trois différents types de clé : privée, publique et partagée.

La clé privée, connue uniquement de l'appareil, est associée à la clé publique, mais elle n'est pas incluse dans le certificat numérique des clients (expéditeurs). Lorsque l'utilisateur établit pour la première fois la connexion, l'appareil envoie la clé publique avec le certificat. Le PC client assume en toute confiance que cette clé publique provient de l'appareil muni du certificat. Le client génère la clé partagée, la code avec la clé publique, puis l'envoie à l'appareil. L'appareil code la clé partagée avec la clé privée. L'appareil et le client partagent alors la clé partagée en toute sécurité et ils établissent une connexion sécurisée pour le transfert des données d'impression.

Les données d'impression sont codées et décodées avec la clé partagée.

SSL n'empêche pas les utilisateurs non autorisés d'accéder aux paquets, mais il les rend illisibles sans clé privée (que seul l'appareil possède).

Elle peut être configurée sur les réseaux filaires et sans fil, et fonctionne avec d'autres outils de sécurité, tels que les pare-feu et les clés WPA, selon la configuration appropriée.

Termes liés aux réseaux

- SSL (Secure Socket Layer)

  Ce protocole de communication sécurisé crypte les données afin de bloquer les menaces de sécurité.

- IPP (Internet Printing Protocol)

  IPP est un protocole d'impression standard utilisé pour la gestion et l'administration de travaux d'impression. Il peut être utilisé localement ou globalement afin que n'importe quel utilisateur puisse imprimer sur le même appareil, où qu'il se trouve à travers le monde.

- IPPS

  Version du protocole d'impression Internet Printing Protocol (IPP Version 1.0) qui utilise le SSL.

- HTTPS

  Version du protocole Internet Hyper text Transfer Protocol (HTTP) qui utilise le SSL.

- CA (Certificate Authority)

  Une CA est une entité qui émet des certificats numériques (principalement des certificats X.509) et se porte garant du lien contraignant existant entre les données présentes dans un certificat.

- CSR (Certificate Signing Request)

  Un CSR est un message envoyé par un candidat à la CA afin de demander l'émission d'un certificat. Le CSR contient des informations identifiant le demandeur, la clé publique générée par le candidat ainsi que sa signature numérique.

- Certificat

  Un Certificat est l'information qui relie une clé publique et une identité. Le certificat peut être utilisé pour vérifier l'appartenance d'une clé publique à un individu. Son format est défini par la norme x.509.

- Public key cryptosystem

  Un Public key cryptosystem est une branche moderne de la cryptographie dans laquelle les algorithmes emploient une paire de clés (une clé publique et une clé privée) et utilisent un composant différent de la paire pour différentes étapes de l'algorithme.

- Shared key cryptosystem

  Un Shared key cryptosystem est une branche de la cryptographie dans laquelle les algorithmes emploient la même clé pour deux étapes différentes de l'algorithme (comme le cryptage et le décryptage).