Guide des fonctions de sécurité

Informations importantes pour la sécurité

- Le mot de passe par défaut pour gérer les paramètres de cet appareil se trouve en dessous de l'appareil et est indiqué par « **Pwd:** ». Nous vous conseillons de modifier immédiatement le mot de passe par défaut pour protéger votre appareil contre les accès non autorisés.
- Lorsque vous connectez votre appareil à un réseau extérieur tel qu'Internet, assurez-vous que votre environnement réseau est protégé par un pare-feu distinct ou par un autre moyen afin d'empêcher les fuites d'informations qui seraient la conséquence de paramètres inadéquats ou d'accès non autorisés par des tiers malveillants.
- Si un tel signal est disponible à proximité, le LAN sans fil vous permet d'établir une connexion au réseau local en toute liberté. Si toutefois les paramètres de sécurité ne sont pas configurés correctement, le signal pourra être intercepté par des tiers malveillants et entraîner, potentiellement :
  - Un vol d'informations personnelles ou confidentielles
  - Une transmission incorrecte d'informations à des parties se faisant passer pour les personnes spécifiées
  - Une divulgation du contenu de la communication transcrite interceptée

Renseignements connexes

- Réseau

Configurer des certificats pour assurer la sécurité de l’appareil

Vous devez configurer un certificat pour gérer votre appareil connecté à un réseau en toute sécurité à l'aide de SSL/TLS. Vous devez utiliser la Gestion à partir du Web pour configurer un certificat.

Aperçu des caractéristiques des certificats de sécurité

Votre appareil prend en charge l'utilisation de plusieurs certificats de sécurité, ce qui garantit la sécurité de l'authentification et de la communication avec l'appareil. Vous pouvez utiliser les fonctions de certificat de sécurité suivantes avec l'appareil :

Les fonctions prises en charge, les options et les paramètres peuvent varier en fonction du modèle.

- Communication SSL/TLS
- Authentification IEEE 802.1x
- IPSec

Votre appareil prend en charge ce qui suit :

- Certificat préinstallé

  Votre appareil possède un certificat préinstallé auto-signé. Ce certificat vous permet d'utiliser la communication SSL/TLS sans créer ou installer un certificat différent.

Le certificat auto-signé préinstallé protège votre communication jusqu'à un certain niveau. Pour accroître le niveau de sécurité, nous vous recommandons d'utiliser un certificat émis par une organisation digne de confiance.

- Certificat auto-signé

  Ce serveur d'impression émet son propre certificat. Ce certificat vous permet d'utiliser facilement la communication SSL/TLS sans créer ou installer un certificat différent d'une autorité de certification.
- Certificat d'une autorité de certification (CA)

  Il existe deux méthodes d'installation d'un certificat issue d'une autorité de certification. Si vous avez déjà un certificat d'une autorité de certification ou si vous souhaitez utiliser un certificat d'une autorité de certification externe approuvée :
  - Si vous utilisez une demande de signature de certificat (CSR) depuis ce serveur d'impression.
  - Si vous importez un certificat et une clé privée.
- Certification d'une autorité de certification (AC)

  Pour utiliser un certificat d'une autorité de certification qui identifie l'autorité de certification et possède sa propre clé privée, vous devez importer ce certificat depuis l'autorité de certification avant de configurer les fonctions de sécurité réseau.

- Si vous comptez utiliser la communication SSL/TLS, nous vous recommandons de contacter d'abord votre administrateur système.
- Si vous restaurez les paramètres d'usine par défaut du serveur d'impression, le certificat et la clé privée installés sont supprimés. Si vous souhaitez conserver le même certificat et la clé privée après la réinitialisation du serveur d'impression, exportez-les avant la réinitialisation, puis réinstallez-les.

Renseignements connexes

- Configurer des certificats pour assurer la sécurité de l'appareil

Sujets connexes :

- Configurez l'authentification IEEE 802.1x pour votre réseau à l'aide de la gestion à partir du Web (navigateur Web)

Comment créer et installer un certificat

Vous disposez de deux options pour le certificat de sécurité : utiliser un certificat auto-signé ou utiliser un certificat d’une autorité de certification (AC).

Option 1

Certificat auto-signé

1. Créez un certificat auto-signé à l’aide de la Gestion à partir du Web.
2. Installez le certificat auto-signé sur votre ordinateur.

Option 2

Certificat d’une autorité de certification

1. Créez une demande de signature de certificat (CSR) à l’aide de la Gestion à partir du Web.
2. Installez le certificat émis par l’autorité de certification sur votre appareil Brother à l’aide de la Gestion à partir du Web.
3. Installez le certificat sur votre ordinateur.

Renseignements connexes

- Configurer des certificats pour assurer la sécurité de l’appareil

Créer un certificat auto-signé

1. Démarrez votre navigateur Web.
2. Saisissez « https://adresse IP de l'appareil » dans la barre d'adresse de votre navigateur (où « adresse IP de l'appareil » correspond à l'adresse IP de votre appareil).

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil se trouve dans le rapport de configuration réseau.
3. Si nécessaire, saisissez le mot de passe dans le champ **Connexion**, puis cliquez sur **Connexion**.

> Le mot de passe par défaut pour gérer les paramètres de cet appareil se trouve au dos ou sur le fond de l'appareil. Il est indiqué par « **Pwd** ». Modifiez le mot de passe par défaut en suivant les instructions affichées à l'écran lors de la première connexion.

4. Dans la barre de navigation de gauche, cliquez sur **Réseau** > **Sécurité** > **Certificat**.

> Si la barre de navigation de gauche n'est pas visible, commencez la navigation à partir de ≡.

5. Cliquez sur **Créer un certificat auto signé**.
6. Entrez un **Nom commun** et une **Date de validité**.
   - La longueur du **Nom commun** doit être inférieure à 64 octets. Entrez un identifiant tel qu'une adresse IP, un nom de nœud et un nom de domaine à utiliser lorsque vous accédez à cet appareil par l'entremise de la communication SSL/TLS. Le nom de nœud s'affiche par défaut.
   - Un avertissement s'affiche si vous utilisez le protocole IPPS ou HTTPS et que vous entrez dans l'URL un nom différent du **Nom commun** qui a été utilisé pour le certificat auto-signé.
7. Sélectionnez votre réglage dans la liste déroulante **Algorithme de clé publique**.
8. Sélectionnez votre réglage dans la liste déroulante **Algorithme de chiffrement**.
9. Cliquez sur **Envoyer**.

Renseignements connexes

- Configurer des certificats pour assurer la sécurité de l'appareil

Créer une demande de signature de certificat (CSR) et installer un certificat d’une autorité de certification (CA)

Si vous avez déjà un certificat d’une autorité de certification externe (CA) approuvée, vous pouvez enregistrer le certificat et la clé privée sur l’appareil et les gérer à l’aide des fonctions d’importation et d’exportation. Si vous ne disposez pas d’un certificat d’une autorité de certification externe approuvée, créez une demande de signature de certificat (CSR), envoyez-la à une autorité de certification pour la faire authentifier, puis installez le certificat retourné sur votre appareil.

- Créer une demande de signature de certificat (CSR)
- Installer un certificat sur votre appareil

Créer une demande de signature de certificat (CSR)

Une demande de signature de certificat (CSR) est une requête envoyée à une autorité de certification (AC) afin d'authentifier les informations d'identification figurant dans le certificat.

Avant de créer la demande CSR, nous vous recommandons d'installer un certificat racine de l'autorité de certification sur votre ordinateur.

1. Démarrez votre navigateur Web.
2. Saisissez « https://adresse IP de l'appareil » dans la barre d'adresse de votre navigateur (où « adresse IP de l'appareil » correspond à l'adresse IP de votre appareil).

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil se trouve dans le rapport de configuration réseau.
3. Si nécessaire, saisissez le mot de passe dans le champ **Connexion**, puis cliquez sur **Connexion**.

   Le mot de passe par défaut pour gérer les paramètres de cet appareil se trouve au dos ou sur le fond de l'appareil. Il est indiqué par « **Pwd** ». Modifiez le mot de passe par défaut en suivant les instructions affichées à l'écran lors de la première connexion.
4. Dans la barre de navigation de gauche, cliquez sur **Réseau** > **Sécurité** > **Certificat**.

   Si la barre de navigation de gauche n'est pas visible, commencez la navigation à partir de ≡.
5. Cliquez sur **Créer un CSR**.
6. Saisissez un **Nom commun** (requis) et ajoutez d'autres informations sur votre **Organisation** (facultatif).

   - Vous devez fournir les détails de votre entreprise pour que l'autorité de certification puisse confirmer et vérifier votre identité pour les tiers.
   - La longueur du **Nom commun** doit être inférieure à 64 octets. Entrez un identifiant tel qu'une adresse IP, un nom de nœud et un nom de domaine à utiliser lorsque vous accédez à cet appareil par l'entremise de la communication SSL/TLS. Le nom de nœud s'affiche par défaut. Le **Nom commun** est obligatoire.
   - Un avertissement s'affiche si vous saisissez dans l'URL un nom différent du Nom commun qui a été utilisé pour le certificat.
   - La longueur des champs **Organisation**, **Unité d'organisation**, **Ville/localité** et **Département** doit être inférieure à 64 octets.
   - Le champ **Pays** doit contenir un code de pays ISO 3166 à deux caractères.
   - Si vous configurez une extension de certificat X.509v3, sélectionnez la case à cocher **Configurer la partition étendue**, puis sélectionnez **Automatique (Enregistrer IPv4)** ou **Manuel**.
7. Sélectionnez votre réglage dans la liste déroulante **Algorithme de clé publique**.
8. Sélectionnez votre réglage dans la liste déroulante **Algorithme de chiffrement**.
9. Cliquez sur **Envoyer**.

   La demande CSR s'affiche sur votre écran. Enregistrez la demande CSR dans un fichier ou copiez et collez-la dans un formulaire CSR en ligne mis à votre disposition par une autorité de certification.
10. Cliquez sur **Enregistrer**.

- Suivez la politique de votre autorité de certification concernant la méthode d'envoi d'une demande CSR.
- Si vous utilisez l'autorité de certification racine d'entreprise de Windows Server, nous vous recommandons d'utiliser le serveur Web pour le modèle de certificat afin de créer le certificat client en toute sécurité. Si vous créez un certificat client pour un environnement IEEE 802.1x avec l'authentification EAP-TLS, nous vous recommandons d'utiliser Utilisateur pour le modèle de certificat.

Renseignements connexes

- Créer une demande de signature de certificat (CSR) et installer un certificat d'une autorité de certification (CA)

Installer un certificat sur votre appareil

Lorsque vous recevez un certificat d'une autorité de certification (CA, Certificate Authority), suivez les étapes ci-dessous pour l'installer sur le serveur d'impression :

Seul un certificat émis avec la demande de signature de certificat (CSR, Certificate Signing Request) de votre appareil peut être installé sur l'appareil. Si vous souhaitez créer une nouvelle demande de signature de certificat (CSR), veillez à installer le certificat avant de créer cette demande. Ne créez une nouvelle demande CSR qu'après avoir installé le certificat sur l'appareil, faute de quoi la demande CSR créée avant l'installation de la nouvelle demande CSR ne sera pas valide.

1. Démarrez votre navigateur Web.
2. Saisissez « https://adresse IP de l'appareil » dans la barre d'adresse de votre navigateur (où « adresse IP de l'appareil » correspond à l'adresse IP de votre appareil).

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil se trouve dans le rapport de configuration réseau.
3. Si nécessaire, saisissez le mot de passe dans le champ **Connexion**, puis cliquez sur **Connexion**.

Le mot de passe par défaut pour gérer les paramètres de cet appareil se trouve au dos ou sur le fond de l'appareil. Il est indiqué par « **Pwd** ». Modifiez le mot de passe par défaut en suivant les instructions affichées à l'écran lors de la première connexion.

4. Dans la barre de navigation de gauche, cliquez sur **Réseau** > **Sécurité** > **Certificat**.

Si la barre de navigation de gauche n'est pas visible, commencez la navigation à partir de ≡.

5. Cliquez sur **Installer le certificat**.
6. Accédez au fichier contenant le certificat émis par l'autorité de certification, puis cliquez sur **Envoyer**.

   Le certificat est créé et enregistré dans la mémoire de l'appareil.

Pour utiliser la communication SSL/TLS, le certificat racine de l'autorité de certification doit être installé sur votre ordinateur. Communiquez avec votre administrateur réseau.

Renseignements connexes

- Créer une demande de signature de certificat (CSR) et installer un certificat d'une autorité de certification (CA)

Importer et exporter le certificat et la clé privée

Enregistrez le certificat et la clé privée sur votre appareil et gérez-les à l’aide des fonctions d’importation et d’exportation.

- Importer un certificat et une clé privée
- Exporter le certificat et la clé privée

Importer un certificat et une clé privée

1. Démarrez votre navigateur Web.
2. Saisissez « https://adresse IP de l'appareil » dans la barre d'adresse de votre navigateur (où « adresse IP de l'appareil » correspond à l'adresse IP de votre appareil).

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil se trouve dans le rapport de configuration réseau.
3. Si nécessaire, saisissez le mot de passe dans le champ **Connexion**, puis cliquez sur **Connexion**.

Le mot de passe par défaut pour gérer les paramètres de cet appareil se trouve au dos ou sur le fond de l'appareil. Il est indiqué par « **Pwd** ». Modifiez le mot de passe par défaut en suivant les instructions affichées à l'écran lors de la première connexion.

4. Dans la barre de navigation de gauche, cliquez sur **Réseau** > **Sécurité** > **Certificat**.

Si la barre de navigation de gauche n'est pas visible, commencez la navigation à partir de ≡.

5. Cliquez sur **Importer le certificat et la clé privée**.
6. Accédez à l'emplacement du fichier à importer, puis sélectionnez le fichier.
7. Saisissez le mot de passe si le fichier est crypté, puis cliquez sur **Envoyer**.

Le certificat et la clé privée sont importés sur votre appareil.

Renseignements connexes

- Importer et exporter le certificat et la clé privée

Exporter le certificat et la clé privée

1. Démarrez votre navigateur Web.
2. Saisissez « https://adresse IP de l'appareil » dans la barre d'adresse de votre navigateur (où « adresse IP de l'appareil » correspond à l'adresse IP de votre appareil).

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil se trouve dans le rapport de configuration réseau.
3. Si nécessaire, saisissez le mot de passe dans le champ **Connexion**, puis cliquez sur **Connexion**.

> Le mot de passe par défaut pour gérer les paramètres de cet appareil se trouve au dos ou sur le fond de l'appareil. Il est indiqué par « **Pwd** ». Modifiez le mot de passe par défaut en suivant les instructions affichées à l'écran lors de la première connexion.

4. Dans la barre de navigation de gauche, cliquez sur **Réseau** > **Sécurité** > **Certificat**.

> Si la barre de navigation de gauche n'est pas visible, commencez la navigation à partir de ≡.

5. Cliquez sur **Exporter** affiché avec **Liste des certificats**.
6. Entrez un mot de passe si vous souhaitez crypter le fichier.

   Si le mot de passe est laissé vide, la sortie ne sera pas cryptée.
7. Entrez le mot de passe de nouveau pour confirmer, puis cliquez sur **Envoyer**.
8. Cliquez sur **Enregistrer**.

Le certificat et la clé privée sont exportés vers votre ordinateur.

Vous pouvez également importer le certificat sur votre ordinateur.

Renseignements connexes

- Importer et exporter le certificat et la clé privée

Importer et exporter un certificat d'autorité de certification

Vous pouvez importer, exporter et enregistrer des certificats d’autorité de certification sur votre appareil Brother.

- Importer un certificat d'autorité de certification
- Exporter un certificat d'autorité de certification

Importer un certificat d'autorité de certification

1. Démarrez votre navigateur Web.
2. Saisissez « https://adresse IP de l'appareil » dans la barre d'adresse de votre navigateur (où « adresse IP de l'appareil » correspond à l'adresse IP de votre appareil).

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil se trouve dans le rapport de configuration réseau.
3. Si nécessaire, saisissez le mot de passe dans le champ **Connexion**, puis cliquez sur **Connexion**.

Le mot de passe par défaut pour gérer les paramètres de cet appareil se trouve au dos ou sur le fond de l'appareil. Il est indiqué par « **Pwd** ». Modifiez le mot de passe par défaut en suivant les instructions affichées à l'écran lors de la première connexion.

4. Dans la barre de navigation de gauche, cliquez sur **Réseau** > **Sécurité** > **Certificat AC**.

Si la barre de navigation de gauche n'est pas visible, commencez la navigation à partir de ≡.

5. Cliquez sur **Importer un certificat AC**.
6. Accédez au fichier que vous souhaitez importer.
7. Cliquez sur **Envoyer**.

Renseignements connexes

- Importer et exporter un certificat d'autorité de certification

Exporter un certificat d'autorité de certification

1. Démarrez votre navigateur Web.
2. Saisissez « https://adresse IP de l'appareil » dans la barre d'adresse de votre navigateur (où « adresse IP de l'appareil » correspond à l'adresse IP de votre appareil).

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil se trouve dans le rapport de configuration réseau.
3. Si nécessaire, saisissez le mot de passe dans le champ **Connexion**, puis cliquez sur **Connexion**.

Le mot de passe par défaut pour gérer les paramètres de cet appareil se trouve au dos ou sur le fond de l'appareil. Il est indiqué par « **Pwd** ». Modifiez le mot de passe par défaut en suivant les instructions affichées à l'écran lors de la première connexion.

4. Dans la barre de navigation de gauche, cliquez sur **Réseau** > **Sécurité** > **Certificat AC**.

Si la barre de navigation de gauche n'est pas visible, commencez la navigation à partir de ≡.

5. Sélectionnez le certificat que vous souhaitez exporter et cliquez sur **Exporter**.
6. Cliquez sur **Envoyer**.

Renseignements connexes

- Importer et exporter un certificat d'autorité de certification

Utiliser SSL/TLS

- Gérer votre appareil réseau en toute sécurité à l'aide de SSL/TLS
- Imprimer des documents en toute sécurité à l’aide de SSL/TLS
- Envoyer ou recevoir un courriel en toute sécurité en utilisant SSL/TLS

Gérer votre appareil réseau en toute sécurité à l'aide de SSL/TLS

- Configurer un certificat pour SSL/TLS et les protocoles disponibles
- Accéder à la Gestion à partir du Web à l’aide de SSL/TLS
- Installer le certificat autosigné pour les utilisateurs Windows disposant de droits d’administrateur
- Configurer des certificats pour assurer la sécurité de l’appareil

Configurer un certificat pour SSL/TLS et les protocoles disponibles

Configurez un certificat sur votre appareil à l'aide de la Gestion à partir du Web avant d'utiliser la communication SSL/TLS.

1. Démarrez votre navigateur Web.
2. Saisissez « https://adresse IP de l'appareil » dans la barre d'adresse de votre navigateur (où « adresse IP de l'appareil » correspond à l'adresse IP de votre appareil).

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil se trouve dans le rapport de configuration réseau.
3. Si nécessaire, saisissez le mot de passe dans le champ **Connexion**, puis cliquez sur **Connexion**.

Le mot de passe par défaut pour gérer les paramètres de cet appareil se trouve au dos ou sur le fond de l'appareil. Il est indiqué par « **Pwd** ». Modifiez le mot de passe par défaut en suivant les instructions affichées à l'écran lors de la première connexion.

4. Dans la barre de navigation de gauche, cliquez sur **Réseau** > **Réseau** > **Protocole**.

Si la barre de navigation de gauche n'est pas visible, commencez la navigation à partir de ≡.

5. Cliquez sur **Paramètres du serveur HTTP**.
6. Sélectionnez le certificat que vous souhaitez configurer à partir de la liste déroulante **Sélectionnez le certificat**.
7. Cliquez sur **Envoyer**.
8. Cliquez sur **Oui** pour redémarrer votre serveur d'impression.

Renseignements connexes

- Gérer votre appareil réseau en toute sécurité à l'aide de SSL/TLS

Sujets connexes :

- Imprimer des documents en toute sécurité à l'aide de SSL/TLS

Accéder à la Gestion à partir du Web à l'aide de SSL/TLS

Pour gérer votre appareil réseau en toute sécurité, vous devez utiliser des utilitaires de gestion avec des protocoles de sécurité.

- Pour utiliser le protocole HTTPS, HTTPS doit être activé sur votre appareil. Le protocole HTTPS est activé par défaut.
- Vous pouvez modifier les paramètres du protocole HTTPS à l'aide de l'écran de Gestion à partir du Web.

1. Démarrez votre navigateur Web.
2. Saisissez « https://adresse IP de l'appareil » dans la barre d'adresse de votre navigateur (où « adresse IP de l'appareil » correspond à l'adresse IP de votre appareil).

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil se trouve dans le rapport de configuration réseau.
3. Si nécessaire, saisissez le mot de passe dans le champ **Connexion**, puis cliquez sur **Connexion**.

   Le mot de passe par défaut pour gérer les paramètres de cet appareil se trouve au dos ou sur le fond de l'appareil. Il est indiqué par « **Pwd** ». Modifiez le mot de passe par défaut en suivant les instructions affichées à l'écran lors de la première connexion.
4. Vous pouvez maintenant accéder à l'appareil à l'aide du protocole HTTPS.

Renseignements connexes

- Gérer votre appareil réseau en toute sécurité à l'aide de SSL/TLS

Installer le certificat autosigné pour les utilisateurs Windows disposant de droits d’administrateur

- Les étapes suivantes s’appliquent à Microsoft Edge. Si vous utilisez un autre navigateur, consultez la documentation de votre navigateur ou son aide en ligne pour obtenir des instructions sur la procédure d'installation de certificats.
- Vous devez avoir créé votre certificat autosigné à l'aide de la gestion à partir du Web.

1. Cliquez avec le bouton droit de la souris sur l’icône **Microsoft Edge**, puis cliquez sur **Exécuter en tant qu’administrateur**.

   Si l’écran **Contrôle de compte d'utilisateur** s’affiche, cliquez sur **Oui**.
2. Saisissez « https://adresse IP de l’appareil » dans la barre d’adresse de votre navigateur (où « adresse IP de l’appareil » correspond à l’adresse IP de votre appareil).

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil se trouve dans le rapport de configuration réseau.
3. Si la connexion n’est pas privée, cliquez sur le bouton **Avancé**, puis passez à la page Web.
4. Si nécessaire, saisissez le mot de passe dans le champ **Connexion**, puis cliquez sur **Connexion**.

   Le mot de passe par défaut pour gérer les paramètres de cet appareil se trouve au dos ou sur le fond de l’appareil. Il est indiqué par « **Pwd** ». Modifiez le mot de passe par défaut en suivant les instructions affichées à l’écran lors de la première connexion.
5. Dans la barre de navigation de gauche, cliquez sur **Réseau** > **Sécurité** > **Certificat**.

   Si la barre de navigation de gauche n’est pas visible, commencez la navigation à partir de ≡.
6. Cliquez sur **Exporter**.
7. Pour chiffrer le fichier de sortie, saisissez un mot de passe dans le champ **Entrez un mot de passe**. Si le champ **Entrez un mot de passe** est vide, votre fichier exporté ne sera pas crypté.
8. Saisissez le mot de passe à nouveau dans le champ **Retapez le mot de passe**, puis cliquez sur **Envoyer**.
9. Cliquez sur le fichier téléchargé pour l’ouvrir.
10. Lorsque l’écran **Assistant Importation de certificat** s’affiche, cliquez sur **Suivant**.
11. Cliquez sur **Suivant**.
12. Si nécessaire, saisissez le mot de passe, puis cliquez sur **Suivant**.
13. Sélectionnez **Placer tous les certificats dans le magasin suivant**, puis cliquez sur **Parcourir...**.
14. Sélectionnez **Autorités de certification racines de confiance**, puis cliquez sur **OK**.
15. Cliquez sur **Suivant**.
16. Cliquez sur **Terminer**.
17. Cliquez sur **Oui**, si l’empreinte digitale (empreinte du pouce) est correcte.
18. Cliquez sur **OK**.

Renseignements connexes

- Gérer votre appareil réseau en toute sécurité à l'aide de SSL/TLS

Imprimer des documents en toute sécurité à l’aide de SSL/TLS

- Imprimer des documents à l’aide d’IPPS
- Configurer un certificat pour SSL/TLS et les protocoles disponibles
- Configurer des certificats pour assurer la sécurité de l’appareil

Imprimer des documents à l'aide d'IPPS

Pour imprimer des documents en toute sécurité avec le protocole IPP, utilisez le protocole IPPS.

1. Démarrez votre navigateur Web.
2. Saisissez « https://adresse IP de l'appareil » dans la barre d'adresse de votre navigateur (où « adresse IP de l'appareil » correspond à l'adresse IP de votre appareil).

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil se trouve dans le rapport de configuration réseau.
3. Si nécessaire, saisissez le mot de passe dans le champ **Connexion**, puis cliquez sur **Connexion**.

Le mot de passe par défaut pour gérer les paramètres de cet appareil se trouve au dos ou sur le fond de l'appareil. Il est indiqué par « **Pwd** ». Modifiez le mot de passe par défaut en suivant les instructions affichées à l'écran lors de la première connexion.

4. Dans la barre de navigation de gauche, cliquez sur **Réseau** > **Réseau** > **Protocole**.

Si la barre de navigation de gauche n'est pas visible, commencez la navigation à partir de ≡.

5. Assurez-vous que la case à cocher **IPP** est sélectionnée.

Si la case à cocher **IPP** n'est pas sélectionnée, sélectionnez la case à cocher **IPP**, puis cliquez sur **Envoyer**.

Redémarrez votre appareil pour activer la configuration.

Après le redémarrage de l'appareil, revenez à la page Web de l'appareil, saisissez le mot de passe, puis dans la barre de navigation de gauche, cliquez sur **Réseau** > **Réseau** > **Protocole**.

6. Cliquez sur **Paramètres du serveur HTTP**.
7. Sélectionnez la case à cocher **HTTPS** dans **IPP**, puis cliquez sur **Envoyer**.
8. Redémarrez votre appareil pour activer la configuration.

La communication à l'aide du protocole IPPS ne peut pas empêcher l'accès non autorisé au serveur d'impression.

Renseignements connexes

- Imprimer des documents en toute sécurité à l'aide de SSL/TLS

Utiliser SNMPv3

- Gérer votre appareil réseau en toute sécurité à l’aide de SNMPv3

Gérer votre appareil réseau en toute sécurité à l'aide de SNMPv3

Le protocole SNMPv3 (Simple Network Management Protocol version 3) assure l'authentification utilisateur et le cryptage des données afin de gérer les périphériques réseau en toute sécurité.

1. Démarrez votre navigateur Web.
2. Saisissez « https://Nom commun » dans la barre d'adresse de votre navigateur (où « Nom commun » est le nom commun que vous avez attribué au certificat; il pourrait s'agir de votre adresse IP, nom de nœud ou nom de domaine).
3. Si nécessaire, saisissez le mot de passe dans le champ **Connexion**, puis cliquez sur **Connexion**.

Le mot de passe par défaut pour gérer les paramètres de cet appareil se trouve au dos ou sur le fond de l'appareil. Il est indiqué par « **Pwd** ». Modifiez le mot de passe par défaut en suivant les instructions affichées à l'écran lors de la première connexion.

4. Dans la barre de navigation de gauche, cliquez sur **Réseau** > **Réseau** > **Protocole**.

Si la barre de navigation de gauche n'est pas visible, commencez la navigation à partir de ≡.

5. Assurez-vous que le paramètre **SNMP** est activé, puis cliquez sur **Paramètres avancés**.
6. Configurez les paramètres du mode SNMPv1/v2c.

Option	Description
Accès SNMP v1/v2c en lecture/écriture	Le serveur d'impression utilise la version 1 et la version 2c du protocole SNMP. Ce mode vous permet d'utiliser toutes les applications de votre appareil. Toutefois, il n'est pas sécurisé car il n'authentifie pas l'utilisateur et ne crypte pas les données.
Accès en lecture seule SNMP v1/v2c	Le serveur d'impression utilise l'accès en lecture seule de la version 1 et la version 2c du protocole SNMP.
Désactivé	Permet de désactiver la version 1 et la version 2c du protocole SNMP. Toutes les applications qui utilisent SNMPv1/v2c seront restreintes. Pour permettre l'utilisation des applications SNMPv1/v2c, utilisez le mode **Accès en lecture seule SNMP v1/v2c** ou **Accès SNMP v1/v2c en lecture/écriture**.

7. Configurez les paramètres du mode SNMPv3.

Option	Description
Activé	Le serveur d'impression utilise la version 3 du protocole SNMP. Pour gérer le serveur d'impression de manière sécurisée, utilisez le mode SNMPv3, puis configurez les paramètres.
Désactivé	Permet de désactiver la version 3 du protocole SNMP. Toutes les applications qui utilisent SNMPv3 seront restreintes. Pour permettre l'utilisation des applications SNMPv3, utilisez le mode SNMPv3.

8. Cliquez sur **Envoyer**.

Si votre appareil affiche les options de paramètre de protocole, sélectionnez les options souhaitées.

9. Redémarrez votre appareil pour activer la configuration.

Renseignements connexes

- Utiliser SNMPv3

Utiliser l’authentification IEEE 802.1x pour votre réseau

Qu’est-ce que l’authentification IEEE 802.1x?

IEEE 802.1x est une norme IEEE qui limite l’accès des appareils réseau non autorisés. Votre appareil Brother envoie une demande d’authentification à un serveur RADIUS (le serveur d’authentification) par le biais de votre point d’accès ou concentrateur de ports. Une fois votre demande vérifiée par le serveur RADIUS, votre appareil peut accéder au réseau.

Renseignements connexes

- Utiliser l’authentification IEEE 802.1x pour votre réseau

Configurez l'authentification IEEE 802.1x pour votre réseau à l'aide de la gestion à partir du Web (navigateur Web)

- Si vous configurez votre appareil en utilisant l'authentification EAP-TLS, vous devez installer le certificat client fourni par une autorité de certification avant de démarrer la configuration. Contactez votre administrateur de réseau à propos du certificat client. Si vous avez installé plusieurs certificats, nous vous recommandons de prendre note du nom du certificat que vous souhaitez utiliser.
- Avant de vérifier le certificat du serveur, vous devez importer le certificat d'autorité de certification émis par l'autorité de certification qui a signé le certificat du serveur. Contactez votre administrateur de réseau ou votre fournisseur d'accès Internet (FAI) pour vérifier s'il est nécessaire d'importer un certificat d'autorité de certification.

Vous pouvez également configurer l'authentification IEEE 802.1x à l'aide de l'assistant de configuration sans fil à partir du panneau de commande (Réseau sans fil).

1. Démarrez votre navigateur Web.
2. Saisissez « https://adresse IP de l'appareil » dans la barre d'adresse de votre navigateur (où « adresse IP de l'appareil » correspond à l'adresse IP de votre appareil).

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil se trouve dans le rapport de configuration réseau.
3. Si nécessaire, saisissez le mot de passe dans le champ **Connexion**, puis cliquez sur **Connexion**.

Le mot de passe par défaut pour gérer les paramètres de cet appareil se trouve au dos ou sur le fond de l'appareil. Il est indiqué par « **Pwd** ». Modifiez le mot de passe par défaut en suivant les instructions affichées à l'écran lors de la première connexion.

4. Dans la barre de navigation de gauche, cliquez sur **Réseau**.

Si la barre de navigation de gauche n'est pas visible, commencez la navigation à partir de ≡.

5. Effectuez l'une des opérations suivantes :
   - Pour le réseau câblé

     Cliquez sur **Câblé** > **État 802.1x authentification**.
   - Pour le réseau sans fil

     Cliquez sur **Sans fil** > **Sans fil (Entreprise)**.
6. Configurez les paramètres d'authentification IEEE 802.1x.

- Pour activer l'authentification IEEE 802.1x pour des réseaux câblés, sélectionnez **Activé** pour **État 802.1x câblé** à la page **État 802.1x authentification**.
- Si vous utilisez l'authentification **EAP-TLS**, vous devez sélectionner le certificat client installé (affiché avec le nom de certificat) pour la vérification à partir de la liste déroulante **Certificat client**.
- Si vous sélectionnez l'authentification **EAP-FAST**, **PEAP**, **EAP-TTLS** ou **EAP-TLS**, sélectionnez la méthode de vérification à partir de la liste déroulante **Vérification du certificat de serveur**. Vérifiez le certificat du serveur en utilisant, après importation dans l'appareil, le certificat d'autorité de certification émis par l'autorité de certification qui a signé le certificat du serveur.

Sélectionnez l'une des méthodes de vérification suivantes à partir de la liste déroulante **Vérification du certificat de serveur** :

Option	Description
Aucune vérification	Vous pouvez toujours faire confiance au certificat du serveur. La vérification n'est pas exécutée.
Cert. AC	Cette méthode de vérification permet de vérifier la fiabilité de l'autorité de certification du certificat du serveur en utilisant le certificat émis par l'autorité de certification qui a signé le certificat du serveur.
Cert. AC + ID serveur	Cette méthode de vérification permet de vérifier la valeur du nom commun [1] du certificat du serveur, en plus de la fiabilité de l'autorité de certification du certificat du serveur.

7. Lorsque vous terminez la configuration, cliquez sur **Envoyer**.

   Pour des réseaux câblés : Après la configuration, connectez votre appareil au réseau pris en charge par IEEE 802.1x. Après quelques minutes, imprimez le rapport de configuration réseau pour vérifier l'état **<Wired IEEE 802.1x>**.

Option	Description
Success	La fonction IEEE 802.1x câblée est activée et l'authentification a réussi.
Failed	La fonction IEEE 802.1x câblée est activée; toutefois, l'authentification a échoué.
Off	La fonction IEEE 802.1x câblée n'est pas disponible.

Renseignements connexes

- Utiliser l'authentification IEEE 802.1x pour votre réseau

Sujets connexes :

- Aperçu des caractéristiques des certificats de sécurité
- Configurer des certificats pour assurer la sécurité de l'appareil

1 La vérification du nom commun compare le nom commun du certificat de serveur à la chaîne de caractères configurée pour **ID serveur**. Avant d'utiliser cette méthode, contactez votre administrateur système à propos du nom commun du certificat du serveur, puis configurez la valeur **ID serveur**.

Méthodes d'authentification IEEE 802.1x

EAP-FAST

Le protocole EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secured Tunneling) a été mis au point par Cisco Systems, Inc. et utilise un nom d'utilisateur et un mot de passe pour l'authentification, ainsi que des algorithmes à clé symétrique pour créer un processus d'authentification en tunnel.

Votre appareil Brother prend en charge les méthodes d'authentification internes suivantes :

- EAP-FAST/NONE
- EAP-FAST/MS-CHAPv2
- EAP-FAST/GTC

EAP-MD5 (réseau câblé)

Le protocole EAP-MD5 (Extensible Authentication Protocol-Message Digest Algorithm 5) utilise un nom d'utilisateur et un mot de passe pour l'authentification Stimulation/Réponse.

PEAP

Le protocole PEAP (Protected Extensible Authentication Protocol) est une version de la méthode EAP développée par Cisco Systems, Inc., Microsoft Corporation et RSA Security. PEAP crée un tunnel SSL (Secure Sockets Layer)/TLS (Transport Layer Security) crypté entre un client et un serveur d'authentification pour l'envoi d'un nom d'utilisateur et d'un mot de passe. PEAP assure une authentification mutuelle entre le serveur et le client.

Votre appareil Brother prend en charge les méthodes d'authentification internes suivantes :

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

Le protocole EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security) a été mis au point par Funk Software et Certicom. Le protocole EAP-TTLS crée un tunnel SSL crypté similaire à celui de PEAP entre un client et un serveur d'authentification pour envoyer un nom d'utilisateur et un mot de passe. Le protocole EAP-TTLS procure une authentification mutuelle entre le serveur et le client.

Votre appareil Brother prend en charge les méthodes d'authentification internes suivantes :

- EAP-TTLS/CHAP
- EAP-TTLS/MS-CHAP
- EAP-TTLS/MS-CHAPv2
- EAP-TTLS/PAP

EAP-TLS

Le protocole EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) nécessite une authentification par certificat numérique au niveau du client et du serveur d'authentification.

Renseignements connexes

- Utiliser l'authentification IEEE 802.1x pour votre réseau