Guide des Fonctionnalités de Sécurité Réseau

Informations importantes pour la sécurité

- Le mot de passe par défaut pour gérer les paramètres de cet appareil se trouve au bas 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.
- Lors de la connexion de votre appareil à un réseau externe tel qu'Internet, assurez-vous que votre environnement réseau est protégé par un pare-feu distinct ou un autre moyen, de façon à éviter les fuites d'information résultant de paramètres inadéquats ou d'un accès non autorisé par des tiers malveillants.
- En cas de présence d'un signal à proximité, le réseau LAN sans fil (WLAN) vous permet de réaliser librement une connexion LAN. Toutefois, si les paramètres de sécurité ne sont pas correctement configurés, il est possible que le signal soit intercepté par des tiers malveillants, ce qui peut résulter en :
  - 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 intercepté

Information associée

- Réseau

Configurer des certificats pour la sécurité de l’appareil

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

Vue d'ensemble des fonctionnalités du certificat de sécurité

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

Les fonctions, options et paramètres pris en charge peuvent varier en fonction de votre modèle.

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

Votre appareil prend en charge les certificats suivants :

- Certificat préinstallé

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

Le certificat auto-signé pré-installé protège votre communication jusqu'à un certain niveau. Il est conseillé d'utiliser un certificat émis par une organisation fiable afin de garantir une meilleure sécurité.

- Certificat autosigné

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

  Il existe deux méthodes d'installation d'un certificat émis par une autorité de certification. Si vous avez déjà un certificat d'une autorité de certification ou si vous souhaitez utiliser le certificat d'une autorité de certification externe fiable :
  - Lors de l'utilisation d'une demande de signature de certificat (CSR) depuis ce serveur d'impression.
  - Lors de l'importation d'un certificat et d'une clé privée.
- Certificat d'autorité de certification (CA)

  Pour utiliser un certificat CA identifiant l'autorité de certification et possédant sa propre clé privée, vous devez importer ce certificat CA à partir de l'autorité de certification avant de configurer les fonctions de sécurité du réseau.

- Si vous comptez utiliser la communication SSL/TLS, nous vous recommandons de contacter d'abord votre administrateur système.
- Si vous restaurez les paramètres par défaut d'origine 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 de procéder à la réinitialisation et réinstallez-les par la suite.

Information associée

- Configurer des certificats pour la sécurité de l'appareil

Rubriques connexes:

- Configurer l'authentification IEEE 802.1x pour un réseau à l'aide de l'application Gestion à partir du Web (navigateur Web)

Comment créer et installer un certificat

Il existe deux façons de sélectionner un certificat de sécurité : utiliser un certificat auto-signé ou utiliser le certificat d’une autorité de certification (CA).

Option 1

Certificat auto-signé

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

Option 2

Certificat émis par une autorité de certification

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

Information associée

- Configurer des certificats pour la sécurité de l’appareil

Créer un certificat auto-signé

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

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil est indiquée sur le rapport de configuration du 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 la base de l'appareil et est indiqué par « **Pwd** ». Changez le mot de passe par défaut en suivant les instructions 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 à naviguer depuis ≡.

5. Cliquez sur **Créer un certificat auto signé**.
6. Saisissez un **Nom commun** et une **Date de validité**.
   - La longueur du **Nom commun** est inférieure à 64 octets. Saisissez un identifiant, comme une adresse IP, un nom de nœud ou un nom de domaine, à utiliser pour accéder à cet appareil via une communication SSL/TLS. Le nom de nœud est affiché par défaut.
   - Un avertissement s'affiche si vous utilisez le protocole IPPS ou HTTPS et si vous saisissez un nom dans l'URL différent du **Nom commun** utilisé pour le certificat.
7. Sélectionnez votre paramètre dans la liste déroulante **Algorithme de clé publique**.
8. Sélectionnez votre paramètre dans la liste déroulante **Algorithme de chiffrement**.
9. Cliquez sur **Envoyer**.

Information associée

- Configurer des certificats pour la sécurité de l'appareil

Créer une requête 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 (CA) externe fiable, vous pouvez enregistrer le certificat et la clé privée dans l’appareil et les gérer en les important et en les exportant. Si vous n’avez aucun certificat d’une autorité de certification externe fiable, créez un une demande de signature de certificat (CSR, Certificate Signing Request), envoyez-la à une autorité de certification et installez le certificat que vous allez recevoir, sur votre appareil.

- Créer une demande de signature de certificat (CSR, Certificate Signing Request)
- Installer un certificat sur votre appareil

Créer une demande de signature de certificat (CSR, Certificate Signing Request)

Une demande de signature de certificat (CSR, Certificate Signing Request) est une demande adressée à une autorité de certification pour authentifier les justificatifs d'identité contenus dans le certificat.

Il est conseillé d'installer un certificat racine de l'autorité de certification sur votre ordinateur avant de créer la demande CSR.

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

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil est indiquée sur le rapport de configuration du 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 la base de l'appareil et est indiqué par « **Pwd** ». Changez le mot de passe par défaut en suivant les instructions 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 à naviguer depuis ≡.

5. Cliquez sur **Créer un CSR**.
6. Saisissez un **Nom commun** (obligatoire) et ajoutez d'autres informations sur votre **Organisation** (facultatif).

- Les coordonnées de votre société sont nécessaires pour que l'autorité de certification puisse confirmer votre identité et la valider auprès d'un parti externe.
- La longueur du **Nom commun** doit être inférieure à 64 octets. Saisissez un identifiant, comme une adresse IP, un nom de nœud ou un nom de domaine, à utiliser pour accéder à cet appareil via une communication SSL/TLS. Le nom de nœud est affiché par défaut. Le **Nom commun** est obligatoire.
- Un avertissement s'affiche si vous saisissez un nom dans l'URL différent du nom commun 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 octets.
- Le **Pays** doit correspondre à un code de pays ISO 3166 de deux caractères.
- Si vous configurez une extension de certificat X.509v3, cochez la case **Configurer la partition étendue** et 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**.

   Le CSR s'affiche sur votre écran. Enregistrez le CSR sous forme de fichier et copiez-le ou collez-le dans un formulaire CSR en ligne fourni par une autorité de certification.
10. Cliquez sur **Enregistrer**.

- Suivez la procédure de votre autorité de certification pour lui envoyer une demande CSR.
- Si vous utilisez l’autorité de certification racine d’entreprise de Windows Server, il est conseillé d’utiliser le serveur Web pour le modèle de certificat afin de créer un certificat client sécurisé. Si vous créez un certificat client pour un environnement IEEE 802.1x avec l’authentification EAP-TLS, il est conseillé de sélectionner Utilisateur pour le modèle de certificat.

Information associée

- Créer une requête 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, suivez les étapes suivantes pour l'installer sur le serveur d'impression :

Seul un certificat émis avec une demande de signature de certificat (CSR) de cet appareil peut être installé sur l'appareil. Si vous voulez créer une autre demande CSR, assurez-vous que le certificat est installé avant de créer la nouvelle demande CSR. Créez une autre demande CSR uniquement après l'installation du certificat sur l'appareil ; à défaut, la demande CSR créée avant l'installation du nouveau certificat CSR ne sera pas valable.

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

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil est indiquée sur le rapport de configuration du 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 la base de l'appareil et est indiqué par « **Pwd** ». Changez le mot de passe par défaut en suivant les instructions 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 à naviguer depuis ☰.

5. Cliquez sur **Installer le certificat**.
6. Accédez au fichier qui contient le certificat émanant d'une autorité de certification, puis cliquez sur **Envoyer**.

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

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

Information associée

- Créer une requête 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 l’appareil et gérez-les en les important et en les exportant.

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

Importer un certificat et une clé privée

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

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil est indiquée sur le rapport de configuration du 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 la base de l'appareil et est indiqué par « **Pwd** ». Changez le mot de passe par défaut en suivant les instructions 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 à naviguer depuis ≡.

5. Cliquez sur **Importer le certificat et la clé privée**.
6. Recherchez et sélectionnez le fichier à importer.
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.

Information associée

- Importer et exporter le certificat et la clé privée

Exporter le certificat et la clé privée

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

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil est indiquée sur le rapport de configuration du 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 la base de l'appareil et est indiqué par « **Pwd** ». Changez le mot de passe par défaut en suivant les instructions 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 à naviguer depuis ≡.

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

   Si aucun mot de passe n'est saisi, le fichier n'est pas crypté.
7. Saisissez de nouveau le mot de passe pour confirmation, puis cliquez sur **Envoyer**.
8. Cliquez sur **Enregistrer**.

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

Vous pouvez également importer le certificat vers votre ordinateur.

Information associée

- 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. Lancez votre navigateur Web.
2. Saisissez « https://adresse IP de l'appareil » dans la barre d'adresse de votre navigateur (« adresse IP de l'appareil » correspondant à l'adresse IP de l'appareil).

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil est indiquée sur le rapport de configuration du 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 la base de l'appareil et est indiqué par « **Pwd** ». Changez le mot de passe par défaut en suivant les instructions 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 à naviguer depuis ≡.

5. Cliquez sur **Importer un certificat AC**.
6. Accédez jusqu'au fichier à importer.
7. Cliquez sur **Envoyer**.

Information associée

- Importer et exporter un certificat d'autorité de certification

Exporter un certificat d'autorité de certification

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

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil est indiquée sur le rapport de configuration du 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 la base de l'appareil et est indiqué par « **Pwd** ». Changez le mot de passe par défaut en suivant les instructions 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 à naviguer depuis ≡.

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

Information associée

- 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 avec le protocole SSL/TLS
- Envoyer ou recevoir un e-mail 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 Gestion à partir du Web à l’aide de SSL/TLS
- Installer le certificat auto-signé pour les utilisateurs Windows disposant de droits d’administration
- Configurer des certificats pour 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 Gestion à partir du Web avant d'utiliser la communication SSL/TLS.

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

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil est indiquée sur le rapport de configuration du 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 la base de l'appareil et est indiqué par « **Pwd** ». Changez le mot de passe par défaut en suivant les instructions 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 à naviguer depuis ≡.

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

Information associée

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

Rubriques connexes:

- Imprimer des documents en toute sécurité avec le protocole SSL/TLS

Accéder à 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 les 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 dans l'écran Gestion à partir du Web.

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

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil est indiquée sur le rapport de configuration du 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 la base de l'appareil et est indiqué par « **Pwd** ». Changez le mot de passe par défaut en suivant les instructions à l'écran lors de la première connexion.

4. Vous pouvez maintenant accéder à l'appareil avec le protocole HTTPS.

Information associée

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

Installer le certificat auto-signé pour les utilisateurs Windows disposant de droits d’administration

- La procédure suivante concerne Microsoft Edge. Si vous utilisez un autre navigateur Web, reportez-vous à la documentation ou à l'aide en ligne de ce navigateur Web pour obtenir des instructions relatives à l'installation des certificats.
- Assurez-vous d'avoir créé votre certificat auto-signé à l'aide de l’application Gestion à partir du Web.

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

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

   Par exemple :

   https://192.168.1.2

   L’adresse IP de votre appareil est indiquée sur le rapport de configuration du réseau.
3. Si votre connexion n'est pas privée, cliquez sur le bouton **Avancé**, puis continuez vers 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 la base de l’appareil et est indiqué par « **Pwd** ». Changez le mot de passe par défaut en suivant les instructions 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 à naviguer depuis ≡.
6. Cliquez sur **Exporter**.
7. Pour crypter 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 laissé vide, le fichier exporté ne sera pas crypté.
8. Retapez une nouvelle fois le mot de passe dans le champ **Retapez le mot de passe**, puis cliquez sur **Envoyer**.
9. Cliquez sur le fichier téléchargé pour l’ouvrir.
10. Lorsque **Assistant Importation de certificat** apparaît, cliquez sur **Suivant**.
11. Cliquez sur **Suivant**.
12. Si nécessaire, saisissez un 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**.

Information associée

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

Imprimer des documents en toute sécurité avec le protocole SSL/TLS

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

Imprimer des documents avec IPPS

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

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

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil est indiquée sur le rapport de configuration du 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 la base de l'appareil et est indiqué par « **Pwd** ». Changez le mot de passe par défaut en suivant les instructions 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 à naviguer depuis ≡.
5. Vérifiez que la case **IPP** est cochée.

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

   Redémarrez l'appareil pour activer la configuration.

   Après le redémarrage de l'appareil, retournez sur la page Web de l'appareil, entrez le mot de passe et, dans la barre de navigation de gauche, cliquez sur **Réseau** > **Réseau** > **Protocole**.
6. Cliquez sur **Paramètres du serveur HTTP**.
7. Cochez la case **HTTPS** dans la zone **IPP**, puis cliquez sur **Envoyer**.
8. Redémarrez l'appareil pour activer la configuration.

Une communication utilisant le protocole IPPS ne peut pas empêcher un accès non autorisé au serveur d'impression.

Information associée

- Imprimer des documents en toute sécurité avec le protocole SSL/TLS

Utiliser SNMPv3

- Gérer votre appareil réseau de façon sécurisée à l’aide de SNMPv3

Gérer votre appareil réseau de façon sécurisée 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. Lancez votre navigateur Web.
2. Saisissez « https://Nom commun » dans la barre d'adresse de votre navigateur (« Nom commun » remplace le nom commun que vous avez donné au certificat ; il peut s'agir d'une adresse IP, d'un nom de nœud ou d'un 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 la base de l'appareil et est indiqué par « **Pwd** ». Changez le mot de passe par défaut en suivant les instructions 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 à naviguer depuis ≡.

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. Dans ce mode, vous pouvez utiliser toutes les applications de votre appareil. Cependant il n'est pas sécurisé car il n'y a pas d'authentification des utilisateurs ni de cryptage des données.
Accès en lecture seule SNMP v1/v2c	Le serveur d'impression utilise l'accès en lecture de la version 1 et la version 2c du protocole SNMP.
Désactivé	Désactivez la version 1 et la version 2c du protocole SNMP. Toutes les applications utilisant SNMPv1/v2c seront limitées. Pour pouvoir utiliser les 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 façon sécurisée, utilisez le mode SNMPv3, puis configurez les paramètres.
Désactivé	Désactivez la version 3 du protocole SNMP. Toutes les applications utilisant SNMPv3 seront limitées. Pour pouvoir utiliser les applications SNMPv3, utilisez le mode SNMPv3.

8. Cliquez sur **Envoyer**.

Si votre appareil affiche les options de réglage du protocole, sélectionnez les options qui vous intéressent.

9. Redémarrez l'appareil pour activer la configuration.

Information associée

- Utiliser SNMPv3

Utiliser l'authentification IEEE 802.1x pour votre réseau

Présentation de l’authentification IEEE 802.1x

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

Information associée

- Utiliser l'authentification IEEE 802.1x pour votre réseau

Configurer l'authentification IEEE 802.1x pour un réseau à l'aide de l'application Gestion à partir du Web (navigateur Web)

- Si vous configurez votre appareil à l'aide de l'authentification EAP-TLS, vous devez installer le certificat client émis par une autorité de certification avant de démarrer la configuration. Contactez votre administrateur réseau au sujet du certificat client. Si vous avez installé plus d'un certificat, nous vous recommandons de noter le 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 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 depuis le panneau de commande (réseau sans fil).

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

   Par exemple :

   https://192.168.1.2

   L'adresse IP de votre appareil est indiquée sur le rapport de configuration du 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 la base de l'appareil et est indiqué par « **Pwd** ». Changez le mot de passe par défaut en suivant les instructions 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 à naviguer depuis ☰.

5. Effectuez l'une des actions 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 les réseaux câblés, sélectionnez **Activé** pour **État 802.1x câblé** sur la page **État 802.1x authentification**.
- Si vous utilisez l'authentification **EAP-TLS**, vous devez sélectionner le certificat client qui a été installé (indiqué par le nom du certificat) pour vérification dans la liste déroulante **Certificat client**.
- Si vous sélectionnez l'authentification **EAP-FAST**, **PEAP**, **EAP-TTLS** ou **EAP-TLS**, vous pouvez sélectionner la méthode de vérification dans la liste déroulante **Vérification du certificat de serveur**. Vérifiez le certificat du serveur à l'aide du certificat de l'autorité de certification, préalablement importé dans l'appareil, émis par l'autorité de certification qui a signé le certificat du serveur.

Sélectionnez une des méthodes de vérification suivantes dans la liste déroulante **Vérification du certificat de serveur** :

Option	Description
Aucune vérification	Le certificat du serveur est toujours fiable. La vérification n'est pas exécutée.
Cert. AC	Méthode de vérification de la fiabilité de l'autorité de certification du certificat du serveur à l'aide du certificat de l'autorité de certification émis par l'autorité de certification ayant signé le certificat du serveur.
Cert. AC + ID serveur	La méthode de vérification pour vérifier le nom commun [1] du certificat du serveur, en plus de la fiabilité de l'autorité de certification du certificat du serveur.

7. Lorsque vous avez terminé la configuration, cliquez sur **Envoyer**.

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

Option	Description
Success	La fonction IEEE 802.1x câblé est activée et l'authentification est réussie.
Failed	La fonction IEEE 802.1x câblé est activée, mais l'authentification a échoué.
Off	La fonction IEEE 802.1x câblé n'est pas disponible.

Information associée

- Utiliser l'authentification IEEE 802.1x pour votre réseau

Rubriques connexes:

- Vue d'ensemble des fonctionnalités du certificat de sécurité
- Configurer des certificats pour la sécurité de l'appareil

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

Méthodes d'authentification IEEE 802.1x

EAP-FAST

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

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

- EAP-FAST/AUCUN
- 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 effectuer une authentification de type « challenge-response ».

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) 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 interne suivantes :

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

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

Votre appareil Brother prend en charge les méthodes d'authentification interne 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 l'authentification d'un certificat numérique par un client et par un serveur d'authentification.

Information associée

- Utiliser l'authentification IEEE 802.1x pour votre réseau