Guide des Fonctionnalités de Sécurité Réseau

Table des matières

Introduction 1
Définition des remarques 2
Marques commerciales 3
Copyright 4
Avant d'utiliser les fonctions de sécurité réseau 5
Désactiver les protocoles inutiles 6
Sécurité du réseau 7
Configurer des certificats pour la sécurité de l'appareil 8
Vue d'ensemble des fonctionnalités du certificat de sécurité 9
Comment créer et installer un certificat 10
Créer un certificat auto-signé 11
Créer une requête de signature de certificat (CSR) et installer un certificat d'une autorité de certification (CA) 12
Importer et exporter le certificat et la clé privée 16
Importer et exporter un certificat d'autorité de certification 19
Utiliser SSL/TLS 22
Gérer votre appareil réseau en toute sécurité à l'aide de SSL/TLS 23
Imprimer des documents en toute sécurité avec le protocole SSL/TLS 27
Utiliser SNMPv3 29
Gérer votre appareil réseau de façon sécurisée à l'aide de SNMPv3 30
Utiliser IPsec 31
Introduction au protocole IPsec 32
Configurer une connexion IPsec à l'aide de Gestion à partir du Web 33
Configurer un modèle d'adresse IPsec à l'aide de Gestion à partir du Web 35
Configurer un modèle IPsec à l'aide de Gestion à partir du Web 37
Utiliser l'authentification IEEE 802.1x pour votre réseau 47
Présentation de l'authentification IEEE 802.1x 48
Configurer l'authentification IEEE 802.1x pour un réseau à l'aide de l'application Gestion à partir du Web (navigateur Web) 49
Méthodes d'authentification IEEE 802.1x 51
Authentification de l'utilisateur 52
Utiliser l'authentification Active Directory 53
Introduction à l'authentification Active Directory 54
Configurer l'authentification Active Directory à l'aide de Gestion à partir du Web 55
Se connecter pour modifier les réglages de l'appareil à l'aide du panneau de commande de l'appareil (authentification Active Directory) 57
Utiliser l'authentification LDAP 58
Introduction à l'authentification LDAP 59
Configurer l'authentification LDAP à l'aide de Gestion à partir du Web 60
Se connecter pour modifier les réglages de l'appareil à l'aide du panneau de commande de l'appareil (authentification LDAP) 61
Utiliser Verrouillage fonction sécurisée 3.0 62
Avant d'utiliser Secure Function Lock 3.0 63
Configurer Secure Function Lock 3.0 à l'aide de Gestion à partir du Web 64
Numérisation à l'aide de Secure Function Lock 3.0 65
Configurer le mode public pour Secure Function Lock 3.0 66

Configurer les réglages des écrans d’accueil personnels à l’aide de Gestion à partir du Web 67
Autres fonctions de Secure Function Lock 3.0 68
Enregistrer une nouvelle carte à CI à l'aide du panneau de commande de l’appareil 69
Enregistrer un lecteur de carte à puce externe 70
Envoyer ou recevoir un e-mail en toute sécurité 71
Configurer l'envoi et la réception d'e-mails à l'aide de Gestion à partir du Web 72
Envoyer un e-mail en utilisant l'authentification utilisateur 73
Envoyer ou recevoir un e-mail en toute sécurité en utilisant SSL/TLS 74
Enregistrer le journal d’impression sur le réseau 75
Vue d’ensemble de la fonction Enregistrement du journal d’impression sur le réseau 76
Configurer les paramètres de l’enregistrement du journal d’impression sur le réseau à l’aide de Gestion à partir du Web 77
Utiliser le réglage de la détection d’erreurs de l’enregistrement du journal d’impression sur le réseau 79
Utiliser l’enregistrement du journal d’impression sur le réseau avec Secure Function Lock 3.0 81

Introduction

- Définition des remarques
- Marques commerciales
- Copyright
- Avant d’utiliser les fonctions de sécurité réseau

Définition des remarques

Tout au long de ce guide, nous utilisons les conventions et symboles suivants :

IMPORTANT	IMPORTANT indique une situation potentiellement dangereuse qui, si elle n'est pas évitée, risque d'entraîner des dégâts matériels ou une perte de fonctionnalité de l'appareil.
REMARQUE	REMARQUE spécifie l'environnement d'exploitation, les conditions d'installation ou des conditions spéciales d'utilisation.
	Les icônes de conseils indiquent la présence de conseils utiles et d'informations supplémentaires.
Caractères gras	Le texte en gras identifie les boutons sur le panneau de commande de l'appareil ou sur l'écran de l'ordinateur.
Caractères en italique	Les caractères Italicized emphasizes un point important ou signalent un sujet connexe.

Information associée

- Introduction

Marques commerciales

Adobe® et Reader® sont des marques déposées ou des marques commerciales d'Adobe Systems Incorporated aux États-Unis et/ou dans d'autres pays.

Chaque société dont le nom du logiciel est mentionné dans ce manuel possède un Contrat de License logicielle propre à ses programmes propriétaires.

Tous les noms commerciaux et noms de produits d'autres sociétés apparaissant sur les produits Brother, les documents connexes et tout autre document sont des marques de commerce ou des marques déposées de ces sociétés respectives.

Information associée

- Introduction

Copyright

Information associée

- Introduction

Avant d’utiliser les fonctions de sécurité réseau

Votre appareil emploie certains des plus récents protocoles de sécurité réseau et de cryptage disponibles à ce jour. Ces fonctions réseau peuvent être intégrées à votre plan général de sécurité réseau pour vous aider à protéger vos données et empêcher un accès unauthorized à votre appareil.

Nous vous conseillons de désactiver les protocoles FTP et TFTP. L’accès à l’appareil via ces protocoles n’est pas sécurisé.

Information associée

- Introduction
  - Désactiver les protocoles inutiles

Désactiver les protocoles inutiles

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. Décochez toutes les cases de protocole inutiles pour les désactiver.
6. Cliquez sur **Envoyer**.
7. Redémarrez votre appareil Brother pour activer la configuration.

Information associée

- Avant d'utiliser les fonctions de sécurité réseau

Sécurité du réseau

- Configurer des certificats pour la sécurité de l’appareil
- Utiliser SSL/TLS
- Utiliser SNMPv3
- Utiliser IPsec
- Utiliser l'authentification IEEE 802.1x pour votre 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
- Comment créer et installer un certificat
- Créer un certificat auto-signé
- 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
- Importer et exporter un certificat d'autorité de certification

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 organization 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(Port 443)** 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 unauthorized 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 en toute sécurité, utilisez le mode SNMPv3.
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 IPsec

- Introduction au protocole IPsec
- Configurer une connexion IPsec à l’aide de Gestion à partir du Web
- Configurer un modèle d’adresse IPsec à l’aide de Gestion à partir du Web
- Configurer un modèle IPsec à l’aide de Gestion à partir du Web

Introduction au protocole IPsec

IPsec (Internet Protocol Security) est un protocole de sécurité qui utilise une fonction IP optionnelle visant à empêcher la manipulation de données et à assurer la protection des données transmises sous forme de paquets IP. IPsec crypte les données qui transitent sur un réseau, notamment les données d'impression envoyées depuis les ordinateurs vers une imprimante. Le cryptage des données s'effectuant au niveau de la couche réseau, les applications qui emploient un protocole de plus haut niveau exploitent IPsec sans que l'utilisateur ne s'en aperçoive.

IPsec prend en charge les fonctions suivantes :

- Transmissions IPsec

  En fonction des conditions de paramétrage IPsec, un ordinateur connecté au réseau envoie des données et en reçoit depuis un appareil spécifique à l'aide d'IPsec. Quand un appareil commence à communiquer via IPsec, les clés sont échangées d'abord par Internet Key Exchange (IKE), puis les données cryptées sont transmises à l'aide des clés.

  De plus, IPsec offre deux modes d'exploitation : le mode Transport et le mode Tunnel. Le mode Transport est surtout utilisé pour la communication entre les appareils, et le mode Tunnel est utilisé dans des environnements tels qu'un réseau privé virtuel (VPN, Virtual Private Network).

Pour les transmissions IPsec, les conditions ci-dessous sont requises :

- Un ordinateur pouvant communiquer à l'aide du protocole IPsec est connecté au réseau.
- Votre appareil est configuré pour les communications IPsec.
- L'ordinateur connecté à votre appareil est configuré pour des connexions IPsec.

- Paramètres IPsec

  Il s'agit des paramètres qui sont nécessaires pour les connexions utilisant le protocole IPsec. Ces paramètres peuvent être configurés à l'aide de l'application Gestion à partir du Web.

Pour configurer les paramètres IPsec, vous devez utiliser le navigateur d'un ordinateur connecté au réseau.

Information associée

- Utiliser IPsec

Configurer une connexion IPsec à l'aide de Gestion à partir du Web

Les conditions de connexion IPsec comptent deux **Modèle** types : **Adresse** et **IPsec**. Vous pouvez configurer 10 conditions de connexion au maximum.

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** > **IPsec**.

Si la barre de navigation de gauche n'est pas visible, commencez à naviguer depuis ☰.

5. Configurez les paramètres.

Option	Description
État	Active ou désactive Ipsec.
Mode de négociation	Sélectionnez **Mode de négociation** pour IKE Phase 1. IKE est un protocole qui est utilisé pour échanger des clés de cryptage pour exécuter les communications cryptées à l'aide du protocole IPsec. En mode **Principal**, le traitement est lent, mais la sécurité est élevée. En mode **Agressif**, la vitesse de traitement est plus rapide qu'en mode **Principal**, mais la sécurité est plus faible.
Tout le trafic non-IPsec	Sélectionnez l'action à effectuer pour les paquets non-IPsec. Si vous utilisez Web Services, vous devez sélectionner **Autoriser** pour **Tout le trafic non-IPsec**. Si vous sélectionnez **Abandonner**, il est impossible d'utiliser Web Services.
Broadcast/Multicast Bypass	Sélectionnez **Activé** ou **Désactivé**.
Bypass Protocol	Cochez les cases de l'option ou des options que vous souhaitez.
Règles	Cochez la case **Activé** pour activer le modèle. Si vous cochez plusieurs cases, les cases avec les valeurs les plus petites sont prioritaires en cas de conflits entre les paramètres des cases cochées. Cliquez sur la liste déroulante correspondante pour sélectionner le **Modèle d'adresse** à utiliser pour les conditions de connexion IPsec. Pour ajouter un **Modèle d'adresse**, cliquez sur **Ajouter un modèle**. Cliquez sur la liste déroulante correspondante pour sélectionner le **Modèle IPsec** à utiliser pour les conditions de connexion IPsec. Pour ajouter un **Modèle IPsec**, cliquez sur **Ajouter un modèle**.

6. Cliquez sur **Envoyer**.

   Si l'appareil doit être redémarré pour activer les nouveaux paramètres, l'écran de confirmation du redémarrage s'affiche.

   Si un élément n'est pas renseigné dans le modèle que vous avez activé dans le tableau **Règles**, un message d'erreur apparaît. Confirmez vos sélections et cliquez à nouveau sur **Envoyer**.

Information associée

- Utiliser IPsec

Rubriques connexes:

- Configurer des certificats pour la sécurité de l’appareil

Configurer un modèle d'adresse IPsec à l'aide de 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. Dans la barre de navigation de gauche, cliquez sur **Réseau** > **Sécurité** > **Modèle d'adresse IPsec**.

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

5. Cliquez sur le bouton **Supprimer** pour supprimer un **Modèle d'adresse**. Lorsqu'un **Modèle d'adresse** est en cours d'utilisation, sa suppression est impossible.
6. Cliquez sur le **Modèle d'adresse** à créer. Le **Modèle d'adresse IPsec** apparaît.
7. Configurez les paramètres.

Option	Description
Nom du modèle	Saisissez un nom pour le modèle (16 caractères maximum).
Adresse IP locale	• **Adresse IP** Spécifiez l'adresse IP. Sélectionnez **TOUTES les adresses IPv4**, **TOUTES les adresses IPv6**, **TOUTES les adresses IPv6 locales de lien** ou **Personnalisé** dans la liste déroulante. Si vous sélectionnez **Personnalisé** dans la liste déroulante, tapez l'adresse IP (IPv4 ou IPv6) dans la zone de texte. • **Plage d'adresses IP** Saisissez la première et la dernière adresse IP de la plage d'adresses IP dans les zones de texte. Si la première et la dernière adresses IP ne sont pas standardized pour IPv4 ou IPv6, ou si la dernière adresse IP est inférieure à la première adresse IP, une erreur se produit. • **Adresse IP / préfixe** Spécifiez l'adresse IP à l'aide d'une notation CIDR. Par exemple : 192.168.1.1/24 Le préfixe étant défini sous la forme d'un masque de sous-réseau 24 bits (255.255.255.0) pour 192.168.1.1, les adresses 192.168.1.### sont valides.
Adresse IP distante	• **Quelconque** Si vous sélectionnez **Quelconque**, toutes les adresses IP sont activées. • **Adresse IP** Saisissez l'adresse IP spécifiée (IPv4 ou IPv6) dans la zone de texte. • **Plage d'adresses IP** Saisissez la première et la dernière adresse IP de la plage d'adresses IP. Si la première et la dernière adresses IP ne sont

Option	Description
	pas standardized pour IPv4 ou IPv6, ou si la dernière adresse IP est inférieure à la première adresse IP, une erreur se produit. • **Adresse IP / préfixe** Spécifiez l'adresse IP à l'aide d'une notation CIDR. Par exemple : 192.168.1.1/24 Le préfixe étant défini sous la forme d'un masque de sous-réseau 24 bits (255.255.255.0) pour 192.168.1.1, les adresses 192.168.1.### sont valides.

8. Cliquez sur **Envoyer**.

Lorsque vous modifiez les paramètres du modèle en cours d'utilisation, redémarrez l'appareil pour activer la configuration.

Information associée

- Utiliser IPsec

Configurer un modèle IPsec à l'aide de 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. Dans la barre de navigation de gauche, cliquez sur **Réseau** > **Sécurité** > **Modèle IPsec**.

   Si la barre de navigation de gauche n'est pas visible, commencez à naviguer depuis ≡.
5. Cliquez sur le bouton **Supprimer** pour supprimer un **Modèle IPsec**. Lorsqu'un **Modèle IPsec** est en cours d'utilisation, sa suppression est impossible.
6. Cliquez sur le **Modèle IPsec** à créer. L'écran **Modèle IPsec** apparaît. Les champs de configuration diffèrent selon les paramètres que vous sélectionnez pour **Utiliser un modèle prédéfini** et **Internet Key Exchange (IKE)**.
7. Dans le champ **Nom du modèle**, saisissez un nom pour le modèle (jusqu'à 16 caractères).
8. Si vous avez sélectionné **Personnalisé** dans la liste déroulante **Utiliser un modèle prédéfini**, sélectionnez les options **Internet Key Exchange (IKE)** et modifiez les paramètres si nécessaire.
9. Cliquez sur **Envoyer**.

Information associée

- Utiliser IPsec
  - Réglages IKEv1 pour un modèle IPsec
  - Réglages IKEv2 pour un modèle IPsec
  - Réglages manuels pour un modèle IPsec

Réglages IKEv1 pour un modèle IPsec

Option	Description
Nom du modèle	Saisissez un nom pour le modèle (16 caractères maximum).
Utiliser un modèle prédéfini	Sélectionnez **Personnalisé**, **Sécurité élevée IKEv1** ou **Sécurité moyenne IKEv1**. Les éléments de paramétrage diffèrent selon le modèle sélectionné.
Internet Key Exchange (IKE)	IKE est un protocole de communication qui est utilisé pour échanger des clés de cryptage pour exécuter les communications cryptées à l'aide du protocole IPsec. Pour exécuter la communication cryptée pour cette fois uniquement, l'algorithme de cryptage qui est nécessaire pour le protocole IPsec est déterminé et les clés de cryptage sont partagées. Pour le protocole IKE, les clés de cryptage sont échangées à l'aide de la méthode d'échange de clés de Diffie-Hellman, et la communication cryptée qui est limitée au protocole IKE est exécutée. Si vous avez sélectionné **Personnalisé** dans **Utiliser un modèle prédéfini**, sélectionnez **IKEv1**.
Type d'authentification	• **Groupe Diffie-Hellman** Cette méthode d'échange de clés permet d'échanger des clés secrètes en toute sécurité sur un réseau non protégé. La méthode d'échange de clés de Diffie-Hellman utilise un problème du logarithme discret, et non pas une clé secrète, pour envoyer et recevoir des informations ouvertes qui ont été générées à l'aide d'un nombre aléatoire et d'une clé secrète. Sélectionnez **Groupe1**, **Groupe2**, **Groupe5** ou **Groupe14**. • **Cryptage** Sélectionnez **DES**, **3DES**, **AES-CBC 128** ou **AES-CBC 256**. • **Hachage** Sélectionnez **MD5**, **SHA1**, **SHA256**, **SHA384** ou **SHA512**. • **Durée de vie SA** Spécifiez la durée de vie SA IKE. Saisissez la durée (en secondes) et le nombre de kilo-octets (ko).
Sécurité d'encapsulation	• **Protocole** Sélectionnez **ESP**, **AH**, ou **AH+ESP**.

Option	Description
	- ESP est un protocole utilisé pour exécuter les communications cryptées à l'aide du protocole IPsec. Le protocole ESP crypte les données utiles (le contenu communiqué) et y ajoute des informations supplémentaires. Le paquet IP est composé d'un en-tête et des données utiles cryptées qui suivent l'en-tête. En plus des données cryptées, le paquet IP comprend également des informations concernant la méthode de cryptage et la clé de cryptage, les données d'authentification, etc. - Le protocole AH est la partie du protocole IPsec qui authentifie l'expéditeur et empêche la manipulation des données (en assurant l'intégrité des données). Dans le paquet IP, les données sont insérées immédiatement après l'en-tête. En outre, les paquets comprennent des valeurs de hachage, qui sont calculées à l'aide d'une équation du contenu communiqué, de la clé secrète et d'autres facteurs, de façon à empêcher la falsification de l'expéditeur et la manipulation des données. Contrairement au protocole ESP, le contenu communiqué n'est pas crypté, et les données sont envoyées et reçues sous forme de texte en clair. • **Cryptage (Non disponible pour l'option AH.)** Sélectionnez **DES**, **3DES**, **AES-CBC 128** ou **AES-CBC 256**. • **Hachage** Sélectionnez **Aucun**, **MD5**, **SHA1**, **SHA256**, **SHA384** ou **SHA512**. **Aucun** ne peut être sélectionné que si **ESP** est sélectionné pour **Protocole**. • **Durée de vie SA** Spécifiez la durée de vie SA IKE. Saisissez la durée (secondes) et le nombre de kilo-octets (Ko). • **Mode d'encapsulation** Sélectionnez **Transport** ou **Tunnel**. • **Adresse IP routeur distant** Spécifiez l'adresse IP (IPv4 ou IPv6) du routeur à distance. Spécifiez cette information seulement si le mode **Tunnel** est sélectionné. SA (Security Association) est une méthode de communication cryptée utilisant le protocole IPsec ou IPv6, qui échange et partage des informations, telles que la méthode de cryptage et la clé de cryptage, afin d'établir un canal de communication sécurisé avant que la communication ne commence. Le terme SA peut également désigner le canal de communication cryptée virtuel qui a été établi. La méthode SA utilisée pour le protocole IPsec établit la méthode de cryptage et les échanges de clés et assure l'authentification mutuelle selon la procédure standard IKE (Internet Key Exchange). De plus, elle est régulièrement mise à jour.
Perfect Forward Secrecy (PFS)	La confidentialité persistante assure qu'aucune clé n'est dérivée des clés antérieures qui ont été utilisées pour crypter les messages. En outre, si une clé utilisée pour crypter un message a été dérivée d'une clé parent, cette clé parent n'est pas utilisée pour dériver d'autres clés. Par conséquent, même si une clé est compromise, la perte de confidentialité sera limitée aux seuls messages qui ont été cryptés avec cette clé. Sélectionnez **Activé** ou **Désactivé**.

Option	Description
Méthode d'authentification	Sélectionnez la méthode d’authentification. Sélectionnez **Clé pré-partagée** ou **Certificats**.
Clé pré-partagée	Lors du cryptage d’une communication, la clé de cryptage est échangée et partagée par avance par un autre canal. Si vous avez sélectionné **Clé pré-partagée** en guise de **Méthode d'authentification**, saisissez la **Clé pré-partagée** (32 caractères maximum). • **Local/Type d'identifiant/Identifiant** Sélectionnez le type d’identifiant de l’expéditeur, puis saisissez l’identifiant. Sélectionnez **Adresse IPv4**, **Adresse IPv6**, **FQDN**, **Adresse e-mail** ou **Certificat** comme type. Si vous avez sélectionné **Certificat**, saisissez le nom commun du certificat dans le champ **ID**. • **Distant/Type d'identifiant/Identifiant** Sélectionnez le type d’identifiant du destinataire, puis saisissez l’identifiant. Sélectionnez **Adresse IPv4**, **Adresse IPv6**, **FQDN**, **Adresse e-mail** ou **Certificat** comme type. Si vous avez sélectionné **Certificat**, saisissez le nom commun du certificat dans le champ **ID**.
Certificat	Si vous avez sélectionné **Certificats** dans **Méthode d'authentification**, sélectionnez le certificat. Vous ne pouvez sélectionner que les certificats qui ont été créés dans la page **Certificat** de l’écran de configuration de la sécurité de l’application Gestion à partir du Web.

Information associée

- Configurer un modèle IPsec à l’aide de Gestion à partir du Web

Réglages IKEv2 pour un modèle IPsec

Option	Description
Nom du modèle	Saisissez un nom pour le modèle (16 caractères maximum).
Utiliser un modèle prédéfini	Sélectionnez **Personnalisé**, **Sécurité élevée IKEv2** ou **Sécurité moyenne IKEv2**. Les éléments de paramétrage diffèrent selon le modèle sélectionné.
Internet Key Exchange (IKE)	IKE est un protocole de communication qui est utilisé pour échanger des clés de cryptage pour exécuter les communications cryptées à l'aide du protocole IPsec. Pour exécuter la communication cryptée pour cette fois uniquement, l'algorithme de cryptage qui est nécessaire pour le protocole IPsec est déterminé et les clés de cryptage sont partagées. Pour le protocole IKE, les clés de cryptage sont échangées à l'aide de la méthode d'échange de clés de Diffie-Hellman, et la communication cryptée qui est limitée au protocole IKE est exécutée. Si vous avez sélectionné **Personnalisé** dans **Utiliser un modèle prédéfini**, sélectionnez **IKEv2**.
Type d'authentification	• **Groupe Diffie-Hellman** Cette méthode d'échange de clés permet d'échanger des clés secrètes en toute sécurité sur un réseau non protégé. La méthode d'échange de clés de Diffie-Hellman utilise un problème du logarithme discret, et non pas une clé secrète, pour envoyer et recevoir des informations ouvertes qui ont été générées à l'aide d'un nombre aléatoire et d'une clé secrète. Sélectionnez **Groupe1**, **Groupe2**, **Groupe5** ou **Groupe14**. • **Cryptage** Sélectionnez **DES**, **3DES**, **AES-CBC 128** ou **AES-CBC 256**. • **Hachage** Sélectionnez **MD5**, **SHA1**, **SHA256**, **SHA384** ou **SHA512**. • **Durée de vie SA** Spécifiez la durée de vie SA IKE. Saisissez la durée (en secondes) et le nombre de kilo-octets (ko).
Sécurité d'encapsulation	• **Protocole** Sélectionnez **ESP**. ESP est un protocole utilisé pour exécuter les communications cryptées à l'aide du protocole IPsec. Le protocole ESP crypte les données utiles (le contenu communiqué) et y ajoute des informations supplémentaires. Le paquet IP est composé d'un en-tête et des données utiles cryptées qui suivent l'en-tête. En plus des données cryptées, le paquet IP comprend également des informations concernant la méthode de cryptage et la clé de cryptage, les données d'authentification, etc. • **Cryptage** Sélectionnez **DES**, **3DES**, **AES-CBC 128** ou **AES-CBC 256**. • **Hachage** Sélectionnez **MD5**, **SHA1**, **SHA256**, **SHA384** ou **SHA512**. • **Durée de vie SA** Spécifiez la durée de vie SA IKE. Saisissez la durée (secondes) et le nombre de kilo-octets (Ko). • **Mode d'encapsulation** Sélectionnez **Transport** ou **Tunnel**.

Option	Description
	• **Adresse IP routeur distant** Spécifiez l'adresse IP (IPv4 ou IPv6) du routeur à distance. Spécifiez cette information seulement si le mode **Tunnel** est sélectionné. SA (Security Association) est une méthode de communication cryptée utilisant le protocole IPsec ou IPv6, qui échange et partage des informations, telles que la méthode de cryptage et la clé de cryptage, afin d'établir un canal de communication sécurisé avant que la communication ne commence. Le terme SA peut également désigner le canal de communication cryptée virtuel qui a été établi. La méthode SA utilisée pour le protocole IPsec établit la méthode de cryptage et les échanges de clés et assure l'authentification mutuelle selon la procédure standard IKE (Internet Key Exchange). De plus, elle est régulièrement mise à jour.
Perfect Forward Secrecy (PFS)	La confidentialité persistante assure qu'aucune clé n'est dérivée des clés antérieures qui ont été utilisées pour crypter les messages. En outre, si une clé utilisée pour crypter un message a été dérivée d'une clé parent, cette clé parent n'est pas utilisée pour dériver d'autres clés. Par conséquent, même si une clé est compromise, la perte de confidentialité sera limitée aux seuls messages qui ont été cryptés avec cette clé. Sélectionnez **Activé** ou **Désactivé**.
Méthode d'authentification	Sélectionnez la méthode d'authentification. Sélectionnez **Clé pré-partagée**, **Certificats**, **EAP - MD5** ou **EAP - MS-CHAPv2**. Le protocole d'authentification EAP est une extension du PPP. Si vous utilisez EAP avec IEEE802.1x, une clé différente est utilisée pour l'authentification de l'utilisateur lors de chaque session. Les réglages suivants ne sont nécessaires que si **EAP - MD5** ou **EAP - MS-CHAPv2** est sélectionné dans **Méthode d'authentification** : • **Mode** Sélectionnez **Mode serveur** ou **Mode client**. • **Certificat** Sélectionnez le certificat. • **Nom d'utilisateur** Saisissez le nom d'utilisateur (32 caractères maximum). • **Mot de passe** Saisissez le mot de passe (32 caractères maximum). Le mot de passe doit être saisi une deuxième fois pour confirmation.
Clé pré-partagée	Lors du cryptage d'une communication, la clé de cryptage est échangée et partagée par avance par un autre canal. Si vous avez sélectionné **Clé pré-partagée** en guise de **Méthode d'authentification**, saisissez la **Clé pré-partagée** (32 caractères maximum). • **Local/Type d'identifiant/Identifiant** Sélectionnez le type d'identifiant de l'expéditeur, puis saisissez l'identifiant. Sélectionnez **Adresse IPv4**, **Adresse IPv6**, **FQDN**, **Adresse e-mail** ou **Certificat** comme type. Si vous avez sélectionné **Certificat**, saisissez le nom commun du certificat dans le champ **ID**.

Option	Description
	• **Distant/Type d'identifiant/Identifiant** Sélectionnez le type d’identifiant du destinataire, puis saisissez l’identifiant. Sélectionnez **Adresse IPv4**, **Adresse IPv6**, **FQDN**, **Adresse e-mail** ou **Certificat** comme type. Si vous avez sélectionné **Certificat**, saisissez le nom commun du certificat dans le champ **ID**.
Certificat	Si vous avez sélectionné **Certificats** dans **Méthode d'authentification**, sélectionnez le certificat. Vous ne pouvez sélectionner que les certificats qui ont été créés dans la page **Certificat** de l’écran de configuration de la sécurité de l’application Gestion à partir du Web.

Information associée

- Configurer un modèle IPsec à l’aide de Gestion à partir du Web

Réglages manuels pour un modèle IPsec

Option	Description
Nom du modèle	Saisissez un nom pour le modèle (16 caractères maximum).
Utiliser un modèle prédéfini	Sélectionnez **Personnalisé**.
Internet Key Exchange (IKE)	IKE est un protocole de communication qui est utilisé pour échanger des clés de cryptage pour exécuter les communications cryptées à l'aide du protocole IPsec. Pour exécuter la communication cryptée pour cette fois uniquement, l'algorithme de cryptage qui est nécessaire pour le protocole IPsec est déterminé et les clés de cryptage sont partagées. Pour le protocole IKE, les clés de cryptage sont échangées à l'aide de la méthode d'échange de clés de Diffie-Hellman, et la communication cryptée qui est limitée au protocole IKE est exécutée. Sélectionnez **Manuel**.
Clé d'authentification (ESP, AH)	Saisissez les valeurs pour **Entrée/Sortie**. Ces réglages sont nécessaires si **Personnalisé** est sélectionné pour **Utiliser un modèle prédéfini**, si **Manuel** est sélectionné pour **Internet Key Exchange (IKE)** et si tout autre réglage que **Aucun** est sélectionné pour **Hachage** dans la section **Sécurité d'encapsulation**. Le nombre de caractères que vous pouvez définir varie selon le paramètre sélectionné pour **Hachage** dans la section **Sécurité d'encapsulation**. Si la longueur de la clé d'authentification sélectionnée diffère de l'algorithme de hachage sélectionné, une erreur se produit. • **MD5** : 128 bits (16 octets) • **SHA1** : 160 bits (20 octets) • **SHA256** : 256 bits (32 octets) • **SHA384** : 384 bits (48 octets) • **SHA512** : 512 bits (64 octets) Lorsque vous spécifiez la clé en code ASCII, entourez les caractères par des guillemets doubles (").
Clé de code (ESP)	Saisissez les valeurs pour **Entrée/Sortie**. Ces réglages sont nécessaires si **Personnalisé** est sélectionné pour **Utiliser un modèle prédéfini**, **Manuel** est sélectionné pour **Internet Key Exchange (IKE)**, et **ESP** est sélectionné pour **Protocole** dans **Sécurité d'encapsulation**. Le nombre de caractères que vous pouvez définir varie selon le paramètre sélectionné pour **Cryptage** dans la section **Sécurité d'encapsulation**. Si la longueur de la clé de code diffère de l'algorithme de cryptage sélectionné, une erreur se produit. • **DES** : 64 bits (8 octets) • **3DES** : 192 bits (24 octets) • **AES-CBC 128** : 128 bits (16 octets) • **AES-CBC 256** : 256 bits (32 octets) Lorsque vous spécifiez la clé en code ASCII, entourez les caractères par des guillemets doubles (").
SPI	Ces paramètres sont utilisés pour identifier les informations de sécurité. En général, un hôte dispose de plusieurs associations de sécurité (SA, Security Associations) pour plusieurs types de communication IPsec. Il faut donc identifier la SA applicable lorsqu'un paquet IP est reçu. Le

Option	Description
	paramètre SPI, qui identifie la SA, est inclus dans l'en-tête d'authentification AH (Authentication Header) et dans l'en-tête ESP (Encapsulating Security Payload). Ces réglages sont nécessaires si **Personnalisé** est sélectionné pour **Utiliser un modèle prédéfini** et si **Manuel** est sélectionné pour **Internet Key Exchange (IKE)**. Saisissez les valeurs pour **Entrée/Sortie**. (3 à 10 caractères)
Sécurité d'encapsulation	• **Protocole** Sélectionnez **ESP** ou **AH**. - ESP est un protocole utilisé pour exécuter les communications cryptées à l'aide du protocole IPsec. Le protocole ESP crypte les données utiles (le contenu communiqué) et y ajoute des informations supplémentaires. Le paquet IP est composé d'un en-tête et des données utiles cryptées qui suivent l'en-tête. En plus des données cryptées, le paquet IP comprend également des informations concernant la méthode de cryptage et la clé de cryptage, les données d'authentification, etc. - Le protocole AH est la partie du protocole IPsec qui authentifie l'expéditeur et empêche la manipulation des données (assure l'intégrité des données). Dans le paquet IP, les données sont insérées immédiatement après l'en-tête. En outre, les paquets comprennent des valeurs de hachage, qui sont calculées à l'aide d'une équation du contenu communiqué, de la clé secrète et d'autres facteurs, de façon à empêcher la falsification de l'expéditeur et la manipulation des données. Contrairement au protocole ESP, le contenu communiqué n'est pas crypté, et les données sont envoyées et reçues sous forme de texte en clair. • **Cryptage (Non disponible pour l'option AH.)** Sélectionnez **DES**, **3DES**, **AES-CBC 128** ou **AES-CBC 256**. • **Hachage** Sélectionnez **Aucun**, **MD5**, **SHA1**, **SHA256**, **SHA384** ou **SHA512**. **Aucun** ne peut être sélectionné que si **ESP** est sélectionné pour **Protocole**. • **Durée de vie SA** Spécifiez la durée de vie SA IKE. Saisissez la durée (secondes) et le nombre de kilo-octets (Ko). • **Mode d'encapsulation** Sélectionnez **Transport** ou **Tunnel**. • **Adresse IP routeur distant** Spécifiez l'adresse IP (IPv4 ou IPv6) du routeur à distance. Spécifiez cette information seulement si le mode **Tunnel** est sélectionné. SA (Security Association) est une méthode de communication cryptée utilisant le protocole IPsec ou IPv6, qui échange et partage des informations, telles que la méthode de cryptage et la clé de cryptage, afin d'établir un canal de communication sécurisé avant que la communication ne commence. Le terme SA peut également désigner le canal de communication cryptée virtuel qui a été établi. La méthode SA utilisée pour le protocole IPsec établit la méthode de cryptage et les échanges de clés et assure l'authentification mutuelle selon la procédure standard IKE (Internet Key Exchange). De plus, elle est régulièrement mise à jour.

Information associée

- Configurer un modèle IPsec à l’aide de Gestion à partir du Web

Utiliser l'authentification IEEE 802.1x pour votre réseau

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

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 unauthorized. 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 **Cablé** > **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 tunneled.

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

Authentification de l’utilisateur

- Utiliser l’authentification Active Directory
- Utiliser l’authentification LDAP
- Utiliser Verrouillage fonction sécurisée 3.0

Utiliser l’authentification Active Directory

- Introduction à l’authentification Active Directory
- Configurer l’authentification Active Directory à l’aide de Gestion à partir du Web
- Se connecter pour modifier les réglages de l’appareil à l’aide du panneau de commande de l’appareil (authentification Active Directory)

Introduction à l’authentification Active Directory

L’authentification Active Directory restreint l’utilisation de votre appareil. Si l’authentification Active Directory est activée, le panneau de commande de l’appareil est bloqué. Il est impossible de modifier les réglages de l’appareil sans saisir le nom d’utilisateur et le mot de passe.

L’authentification Active Directory offre les fonctions suivantes :

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

- L’enregistrement des données d’impression entrantes
- L’enregistrement des données des fax réceptionnés
- Obtient l’adresse e-mail auprès du serveur Active Directory en fonction de votre nom d’utilisateur, lors de l’envoi des données numérisées vers un serveur de messagerie.

  Pour utiliser cette fonction, sélectionnez l’option **Oui** pour le paramètre **Obtenir adresse e-mail** et la méthode d’authentification **LDAP + kerberos** ou **LDAP + NTLMv2**. Votre adresse e-mail de l’appareil est considérée comme l’expéditeur si l’appareil envoie des données numérisées à un serveur de messagerie ou comme le destinataire si vous voulez envoyer des données numérisées à votre adresse e-mail.

Lorsque l’authentification Active Directory est activée, votre appareil enregistre toutes les données des fax réceptionnés. Après avoir ouvert une session, l’appareil imprime les données des fax enregistrés.

Vous pouvez modifier les paramètres d’authentification Active Directory à l’aide de l’application Gestion à partir du Web.

Information associée

- Utiliser l’authentification Active Directory

Configurer l'authentification Active Directory à l'aide de Gestion à partir du Web

L'authentification Active Directory prend en charge l'authentification Kerberos et l'authentification NTLMv2. Vous devez configurer le protocole SNTP (serveur de synchronisation du réseau) et la configuration du serveur DNS pour l'authentification.

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 **Administrateur** > **Fonction de restrictions utilisateur** ou **Gestion des restrictions**.

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

5. Sélectionnez **Authentification Active Directory**.
6. Cliquez sur **Envoyer**.
7. Cliquez sur **Authentification Active Directory**.
8. Configurez les paramètres suivants.

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

Option	Description
Stockage de données de réception Fax	Sélectionnez cette option pour enregistrer les données des fax réceptionnés. Vous pouvez imprimer toutes les données des fax réceptionnés après vous être connecté à l'appareil.
Mémoriser l'ID utilisateur	Sélectionnez cette option pour enregistrer votre nom d'utilisateur.
Adresse serveur Active Directory	Saisissez l'adresse IP ou le nom de serveur (ad.exemple.com, par exemple) du serveur Active Directory.
Nom de domaine Active Directory	Saisissez le nom de domaine Active Directory.
Protocole et méthode d'authentification	Sélectionnez le protocole et la méthode d'authentification.
SSL/TLS	Sélectionnez l'option **SSL/TLS**.
Port serveur LDAP	Saisissez le numéro du port à connecter au serveur Active Directory via LDAP (uniquement disponible pour la méthode d'authentification **LDAP + kerberos** ou **LDAP + NTLMv2**).

Option	Description
Racine de recherche LDAP	Saisissez la racine de recherche LDAP (disponible seulement pour la méthode d'authentification **LDAP + kerberos** ou **LDAP + NTLMv2**).
Obtenir adresse e-mail	Sélectionnez cette option pour obtenir l'adresse e-mail de l'utilisateur connecté auprès du serveur Active Directory. (disponible uniquement pour la méthode d'authentification **LDAP + kerberos** ou **LDAP + NTLMv2**)
Obtenir le répertoire de base de l'utilisateur	Sélectionnez cette option pour obtenir votre répertoire d'accueil en tant que destination Numérisation vers réseau. (disponible uniquement pour la méthode d'authentification **LDAP + kerberos** ou **LDAP + NTLMv2**)

9. Cliquez sur **Envoyer**.

Information associée

- Utiliser l'authentification Active Directory

Se connecter pour modifier les réglages de l’appareil à l’aide du panneau de commande de l’appareil (authentification Active Directory)

Lorsque l’authentification Active Directory est activée, vous devez saisir vos nom d’utilisateur et mot de passe à l’aide du panneau de commande pour débloquer celui-ci.

1. Sur le panneau de commande de l’appareil, saisissez votre nom d’utilisateur et votre mot de passe pour vous connecter.
2. Lorsque l’authentification aboutit, le panneau de commande de l’appareil est débloqué.

Information associée

- Utiliser l’authentification Active Directory

Utiliser l’authentification LDAP

- Introduction à l’authentification LDAP
- Configurer l’authentification LDAP à l’aide de Gestion à partir du Web
- Se connecter pour modifier les réglages de l’appareil à l’aide du panneau de commande de l’appareil (authentification LDAP)

Introduction à l’authentification LDAP

L’authentification LDAP restreint l’utilisation de votre appareil. Si l’authentification LDAP est activée, le panneau de commande de l’appareil est bloqué. Il est impossible de modifier les réglages de l’appareil sans saisir le nom d’utilisateur et le mot de passe.

L’authentification LDAP offre les fonctions suivantes :

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

- L’enregistrement des données d’impression entrantes
- L’enregistrement des données des fax réceptionnés
- Obtient l’adresse e-mail auprès du serveur LDAP en fonction de votre nom d’utilisateur, lors de l’envoi des données numérisées vers un serveur de messagerie.

  Pour utiliser cette fonction, sélectionnez l’option **Oui** pour le réglage **Obtenir adresse e-mail**. Votre adresse e-mail de l’appareil est considérée comme l’expéditeur si l’appareil envoie des données numérisées à un serveur de messagerie ou comme le destinataire si vous voulez envoyer des données numérisées à votre adresse e-mail.

Lorsque l’authentification LDAP est activée, votre appareil enregistre toutes les données des fax réceptionnés. Après avoir ouvert une session, l’appareil imprime les données des fax enregistrés.

Vous pouvez modifier les paramètres d’authentification LDAP à l’aide de l’application Gestion à partir du Web.

Information associée

- Utiliser l’authentification LDAP

Configurer l'authentification LDAP à l'aide de 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. Dans la barre de navigation de gauche, cliquez sur **Administrateur** > **Fonction de restrictions utilisateur** ou **Gestion des restrictions**.

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

5. Sélectionnez **Authentification LDAP**.
6. Cliquez sur **Envoyer**.
7. Cliquez sur le menu **Authentification LDAP**.
8. Configurez les paramètres suivants.

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

Option	Description
Stockage de données de réception Fax	Sélectionnez cette option pour enregistrer les données des fax réceptionnés. Vous pouvez imprimer toutes les données des fax réceptionnés après vous être connecté à l'appareil.
Mémoriser l'ID utilisateur	Sélectionnez cette option pour enregistrer votre nom d'utilisateur.
Adresse du serveur LDAP	Saisissez l'adresse IP ou le nom de serveur (ad.exemple.com, par exemple) du serveur LDAP.
SSL/TLS	Sélectionnez l'option **SSL/TLS** pour utiliser LDAP sur SSL/TLS.
Port serveur LDAP	Saisissez le numéro de port serveur LDAP.
Racine de recherche LDAP	Saisissez le répertoire racine de recherche LDAP.
Attribut nom (Clé de recherche)	Saisissez l'attribut à utiliser comme clé de recherche.
Obtenir adresse e-mail	Sélectionnez cette option pour obtenir l'adresse e-mail de l'utilisateur connecté auprès du serveur LDAP.
Obtenir le répertoire de base de l'utilisateur	Sélectionnez cette option pour obtenir votre répertoire d'accueil en tant que destination Numérisation vers réseau.

9. Cliquez sur **Envoyer**.

Information associée

- Utiliser l'authentification LDAP

Se connecter pour modifier les réglages de l’appareil à l’aide du panneau de commande de l’appareil (authentification LDAP)

Lorsque l’authentification LDAP est activée, le panneau de commande de l’appareil reste verrouillé tant que vous n’avez pas spécifié vos nom d’utilisateur et mot de passe sur le panneau de commande.

1. Sur le panneau de commande de l’appareil, saisissez votre nom d’utilisateur et votre mot de passe pour vous connecter.
2. Lorsque l’authentification aboutit, le panneau de commande de l’appareil est débloqué.

Information associée

- Utiliser l’authentification LDAP

Utiliser Verrouillage fonction sécurisée 3.0

La fonction Verrouillage fonction sécurisée 3.0 renforce la sécurité en limitant les fonctions disponibles sur votre appareil.

- Avant d’utiliser Secure Function Lock 3.0
- Configurer Secure Function Lock 3.0 à l’aide de Gestion à partir du Web
- Numérisation à l’aide de Secure Function Lock 3.0
- Configurer le mode public pour Secure Function Lock 3.0
- Configurer les réglages des écrans d’accueil personnels à l’aide de Gestion à partir du Web
- Autres fonctions de Secure Function Lock 3.0
- Enregistrer une nouvelle carte à CI à l'aide du panneau de commande de l’appareil
- Enregistrer un lecteur de carte à puce externe

Avant d’utiliser Secure Function Lock 3.0

Utilisez Verrouillage fonction sécurisée pour configurer des mots de passe, définir des limites de pages selon les utilisateurs spécifiques et donner accès à une partie ou à la totalité des fonctions énumérées ici.

Vous pouvez configurer et modifier les paramètres suivants de Verrouillage fonction sécurisée 3.0 à l’aide de l’application Gestion à partir du Web :

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

- **Imprimer**
- **Copie**
- **Numérisation**
- **Fax**
- **Support**
- **Web Connect**
- **Applications**
- **Limites de pages**
- **Compteurs de pages**
- **ID carte (ID NFC)**

Modèles à écran tactile LCD :

Lorsque Verrouillage fonction sécurisée est activé, l'appareil bascule automatiquement en mode public et certaines fonctions de l'appareil sont limitées aux utilisateurs authorized seulement. Pour accéder aux fonctions limitées de l'appareil, appuyez sur , sélectionnez votre nom d’utilisateur et votre mot de passe.

Information associée

- Utiliser Verrouillage fonction sécurisée 3.0

Configurer Secure Function Lock 3.0 à l'aide de 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. Dans la barre de navigation de gauche, cliquez sur **Administrateur** > **Fonction de restrictions utilisateur** ou **Gestion des restrictions**.

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

5. Sélectionnez **Verrouill. fonction sécurisée**.
6. Cliquez sur **Envoyer**.
7. Cliquez sur le menu **Fonctions restreintes**.
8. Configurez les paramètres de gestion des restrictions par utilisateur ou par groupe.
9. Cliquez sur **Envoyer**.
10. Cliquez sur le menu **Liste des utilisateurs**.
11. Configurez la liste des utilisateurs.
12. Cliquez sur **Envoyer**.

Vous pouvez également modifier les paramètres de verrouillage de la liste d'utilisateurs dans le menu **Verrouill. fonction sécurisée**.

Information associée

- Utiliser Verrouillage fonction sécurisée 3.0

Numérisation à l’aide de Secure Function Lock 3.0

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

Configuration des restrictions de numérisation (pour les administrateurs)

Verrouillage fonction sécurisée 3.0 permet à un administrateur de limiter les utilisateurs qui sont autorisés à numériser. Lorsque la fonction de numérisation est désactivée pour le profil de l’utilisateur Public, seuls les utilisateurs pour lesquels l’option **Numérisation** est cochée pourront effectuer des numérisations.

Utilisation de la fonction Numérisation (pour les utilisateurs restreints)

- Pour numériser à l’aide du panneau de commande de l’appareil :

  Les utilisateurs restreints doivent entrer leurs mots de passe sur le panneau de commande de l'appareil pour accéder au mode de numérisation.
- Pour numériser depuis un ordinateur :

  Les utilisateurs restreints doivent entrer leurs mots de passe sur le panneau de commande de l'appareil avant de pouvoir numériser depuis leur ordinateur. Si le mot de passe n'est pas entré sur le panneau de commande de l'appareil, un message d'erreur s'affiche sur l'ordinateur de l'utilisateur.

Si l'appareil prend en charge l'authentification par carte à CI, les utilisateurs auxquels des restrictions s'appliquent peuvent également accéder au mode Numériser en mettant en contact le symbole NFC sur le panneau de commande de l'appareil avec leurs cartes à CI enregistrées.

Information associée

- Utiliser Verrouillage fonction sécurisée 3.0

Configurer le mode public pour Secure Function Lock 3.0

Utilisez l'écran Secure Function Lock pour configurer le mode public qui limite les fonctions disponibles pour les utilisateurs publics. Les utilisateurs publics n'ont pas besoin d'entrer de mot de passe pour accéder aux fonctionnalités disponibles via les paramètres du mode public.

Le mode public inclut les travaux d'impression envoyés via Brother iPrint&Scan et Brother Mobile Connect.

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 **Administrateur** > **Fonction de restrictions utilisateur** ou **Gestion des restrictions**.

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

5. Sélectionnez **Verrouill. fonction sécurisée**.
6. Cliquez sur **Envoyer**.
7. Cliquez sur le menu **Fonctions restreintes**.
8. Dans la ligne **Mode public**, cochez une case pour autoriser la fonction indiquée ou décochez une case pour la restreindre.
9. Cliquez sur **Envoyer**.

Information associée

- Utiliser Verrouillage fonction sécurisée 3.0

Configurer les réglages des écrans d’accueil personnels à l’aide de Gestion à partir du Web

En tant qu’administrateur, vous pouvez spécifier les onglets que les utilisateurs peuvent afficher sur leurs écrans d’accueil personnels. Ces onglets permettent un accès rapide aux raccourcis favorite des utilisateurs, qu’ils peuvent affecter aux onglets de leur écran d’accueil personnel à partir du panneau de commande de l’appareil.

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

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 **Administrateur** > **Fonction de restrictions utilisateur** ou **Gestion des restrictions**.

Si la barre de navigation de gauche n’est pas visible, commencez à naviguer depuis ≡.

5. Sélectionnez **Verrouill. fonction sécurisée**.
6. Dans le champ **Paramètres d’onglet**, sélectionnez **Personnel** pour les noms d’onglet que vous souhaitez utiliser pour votre écran d’accueil personnel.
7. Cliquez sur **Envoyer**.
8. Cliquez sur le menu **Fonctions restreintes**.
9. Configurez les paramètres de gestion des restrictions par utilisateur ou par groupe.
10. Cliquez sur **Envoyer**.
11. Cliquez sur le menu **Liste des utilisateurs**.
12. Configurez la liste des utilisateurs.
13. Sélectionnez **Liste des utilisateurs/Fonctions restreintes** dans la liste déroulante pour chaque utilisateur.
14. Sélectionnez le nom de l’onglet dans la liste déroulante **Écran d'accueil** pour chaque utilisateur.
15. Cliquez sur **Envoyer**.

Information associée

- Utiliser Verrouillage fonction sécurisée 3.0

Autres fonctions de Secure Function Lock 3.0

Configurez les fonctionnalités suivantes dans l'écran Secure Function Lock :

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

Réinitialiser tous les compteurs

Cliquez sur **Réinitialiser tous les compteurs**, dans la colonne **Compteurs de pages**, afin de réinitialiser le compteur de pages.

Exporter vers un fichier CSV

Cliquez sur **Exporter vers un fichier CSV**, pour exporter le compteur de pages actuel et le dernier compteur de pages, en incluant les informations **Liste des utilisateurs/Fonctions restreintes** en tant que fichier CSV.

ID carte (ID NFC)

Cliquez sur le menu **Liste des utilisateurs**, puis saisissez un identifiant de carte d'utilisateur dans le champ **ID carte (ID NFC)**. Vous pouvez utiliser votre carte à CI pour vous authentifier.

Sortie

Si une unité de boîte aux lettres est installée sur votre appareil, sélectionnez le bac de sortie pour chaque utilisateur dans la liste déroulante.

Enregistrement dernier compteur

Cliquez sur **Enregistrement dernier compteur**, si vous souhaitez que l'appareil mémorise le nombre de pages une fois le compteur réinitialisé.

Initialisation auto du compteur

Cliquez sur **Initialisation auto du compteur** pour configurer l'intervalle temporel souhaité entre chaque réinitialisation du compteur de pages. Choisissez un intervalle quotidien, hebdomadaire ou mensuel.

Information associée

- Utiliser Verrouillage fonction sécurisée 3.0

Enregistrer une nouvelle carte à CI à l'aide du panneau de commande de l’appareil

Vous pouvez enregistrer des cartes à circuit intégré (cartes CI) sur votre appareil.

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

1. Mettez une carte à circuit intégré (carte à CI) enregistrée en contact avec le symbole NFC (Near-Field Communication) situé sur le panneau de commande de l’appareil.
2. Appuyez sur votre identifiant utilisateur au niveau de l’écran LCD.
3. Appuyez sur le bouton d’enregistrement de carte.
4. Touchez le symbole NFC avec une nouvelle carte à CI.

   Le numéro de la nouvelle carte à CI est alors enregistré sur l’appareil.
5. Appuyez sur le bouton OK.

Information associée

- Utiliser Verrouillage fonction sécurisée 3.0

Enregistrer un lecteur de carte à puce externe

Lorsque vous connectez un lecteur de carte à CI (circuit imprimé) externe, utilisez Gestion à partir du Web pour l’enregistrer. Votre appareil prend en charge les lecteurs de carte à puce externes prenant en charge le pilote HID.

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 **Administrateur** > **Lecteur externe de carte**.

Si la barre de navigation de gauche n’est pas visible, commencez à naviguer depuis ☰.

5. Entrez les informations nécessaires, puis cliquez sur **Envoyer**.
6. Redémarrez votre appareil Brother pour activer la configuration.
7. Connectez le lecteur de carte à votre appareil.
8. Mettez la carte en contact avec le lecteur de cartes lors de l'utilisation de l'authentification par carte.

Information associée

- Utiliser Verrouillage fonction sécurisée 3.0

Envoyer ou recevoir un e-mail en toute sécurité

- Configurer l'envoi et la réception d'e-mails à l'aide de Gestion à partir du Web
- Envoyer un e-mail en utilisant l'authentification utilisateur
- Envoyer ou recevoir un e-mail en toute sécurité en utilisant SSL/TLS

Configurer l'envoi et la réception d'e-mails à l'aide de Gestion à partir du Web

- La réception d'e-mails est disponible uniquement pour certains modèles.
- Il est conseillé d'utiliser l'application Gestion à partir du Web pour configurer l'envoi sécurisé d'e-mails en utilisant l'authentification utilisateur, ou l'envoi et la réception d'e-mails à l'aide de SSL/TLS (modèles pris en charge uniquement).

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. Dans le champ **Client POP3/IMAP4/SMTP**, cliquez sur **Paramètres avancés** et assurez-vous que **Client POP3/IMAP4/SMTP** est en mode **Activé**.

- Les protocoles disponibles peuvent varier en fonction de votre appareil.
- Si l'écran de sélection **Méthode d'authentification** s'affiche, sélectionnez votre méthode d'authentification et suivez les instructions à l'écran.

6. Configurez les paramètres **Client POP3/IMAP4/SMTP**.
   - Vérifiez que les paramètres de la messagerie électronique sont corrects après les avoir configurés en envoyant un e-mail de test.
   - Si vous ignorez les paramètres du serveur POP3/IMAP4/SMTP, contactez l'administrateur réseau ou votre fournisseur d'accès Internet (FAI).
7. Lorsque vous avez terminé, cliquez sur **Envoyer**.

   La boîte de dialogue **Tester la configuration de l'envoi et de la réception des e-mails** s'affiche.
8. Suivez les instructions de la boîte de dialogue pour tester les paramètres actuels.

Information associée

- Envoyer ou recevoir un e-mail en toute sécurité

Rubriques connexes:

- Envoyer ou recevoir un e-mail en toute sécurité en utilisant SSL/TLS

Envoyer un e-mail en utilisant l'authentification utilisateur

Votre appareil envoie des e-mails via un serveur de messagerie nécessitant une authentification utilisateur. Cette méthode empêche que des utilisateurs unauthorized accèdent au serveur de messagerie.

Vous pouvez envoyer une notification par e-mail, des rapports par e-mail et des I-Fax (disponibles uniquement sur certains modèles) via l'authentification utilisateur.

- Les protocoles disponibles peuvent varier en fonction de votre appareil.
- Il est conseillé d'utiliser l'application Gestion à partir du Web pour configurer l'authentification SMTP.

Paramètres du serveur de messagerie

Vous devez configurer la méthode d'authentification SMTP de votre appareil pour qu'elle corresponde à la méthode utilisée par votre serveur de messagerie. Pour des détails sur les paramètres du serveur de messagerie, contactez votre administrateur réseau ou votre fournisseur d'accès Internet (FAI).

Pour activer l'authentification serveur SMTP à l'aide de Gestion à partir du Web, sélectionnez votre méthode d'authentification sous **Méthode d'authentification sur le serveur** au niveau de l'écran **Client POP3/IMAP4/SMTP**.

Information associée

- Envoyer ou recevoir un e-mail en toute sécurité

Envoyer ou recevoir un e-mail en toute sécurité en utilisant SSL/TLS

Votre appareil prend en charge les méthodes de communication SSL/TLS. Pour utiliser un serveur de messagerie utilisant la communication SSL/TLS, vous devez configurer les paramètres suivants.

- La réception d'e-mails est disponible uniquement pour certains modèles.
- Il est conseillé d'utiliser l'application Gestion à partir du Web pour configurer SSL/TLS.

Vérifier le certificat de serveur

Sous **SSL/TLS**, si vous choisissez **SSL** ou **TLS**, la case **Vérifier le certificat de serveur** est automatiquement cochée.

- 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.
- Si vous n'avez pas besoin de vérifier le certificat de serveur, désélectionnez la case **Vérifier le certificat de serveur**.

Numéro de port

Si vous sélectionnez **SSL** ou **TLS**, la valeur **Port** sera modifiée en fonction du protocole utilisé. Pour modifier manuellement le numéro de port, saisissez ce dernier après avoir sélectionné les paramètres de **SSL/TLS**.

Vous devez configurer la méthode de communication de votre appareil pour qu'elle corresponde à celle utilisée par votre serveur de messagerie. Pour des détails sur les paramètres du serveur de messagerie, contactez votre administrateur réseau ou votre FAI.

Les services de messagerie Web sécurisés exigent généralement les paramètres suivants :

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

SMTP	**Port**	587
	Méthode d'authentification sur le serveur	**SMTP-AUTH**
	SSL/TLS	**TLS**
POP3	**Port**	995
	SSL/TLS	**SSL**
IMAP4	**Port**	993
	SSL/TLS	**SSL**

Information associée

- Envoyer ou recevoir un e-mail en toute sécurité

Rubriques connexes:

- Configurer l'envoi et la réception d'e-mails à l'aide de Gestion à partir du Web
- Configurer des certificats pour la sécurité de l'appareil

Enregistrer le journal d’impression sur le réseau

- Vue d’ensemble de la fonction Enregistrement du journal d’impression sur le réseau
- Configurer les paramètres de l’enregistrement du journal d’impression sur le réseau à l’aide de Gestion à partir du Web
- Utiliser le réglage de la détection d’erreurs de l’enregistrement du journal d’impression sur le réseau
- Utiliser l’enregistrement du journal d’impression sur le réseau avec Secure Function Lock 3.0

Vue d’ensemble de la fonction Enregistrement du journal d’impression sur le réseau

La fonction Enregistrement du journal d’impression sur le réseau vous permet d’enregistrer le fichier du journal d’impression depuis votre appareil sur un serveur réseau utilisant le protocole CIFS (Common Internet File System). Vous pouvez enregistrer l’identifiant, le type de travail d’impression, le nom d’utilisateur, la date, l’heure et le nombre de pages imprimées pour chaque travail d’impression. CIFS est un protocole exécuté en plus du protocole TCP/IP pour permettre aux ordinateurs connectés à un réseau de partager des fichiers via un intranet ou l’Internet.

Les fonctions d’impression suivantes sont enregistrées dans le journal d’impression :

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

- Travaux d’impression depuis votre ordinateur
- Impression USB directe
- Copie
- Fax reçu
- Impression Web Connect

- La fonction d’enregistrement du journal d’impression sur le réseau prend en charge les authentifications Kerberos et NTLMv2. Vous devez configurer le protocole SNTP (serveur de synchronisation horaire du réseau) ou définir correctement la date, l’heure et le fuseau horaire sur le panneau de commande pour l’authentification.
- Vous pouvez sélectionner TXT ou CSV pour le type de fichier lors de l’enregistrement d’un fichier sur le serveur.

Information associée

- Enregistrer le journal d’impression sur le réseau

Configurer les paramètres de l’enregistrement du journal d’impression sur le réseau à l’aide de 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. Dans la barre de navigation de gauche, cliquez sur **Administrateur** > **Enreg journal d'impr sur réseau**.

Si la barre de navigation de gauche n’est pas visible, commencez à naviguer depuis ≡.

5. Dans le champ **Imprimer le journal**, cliquez sur **Oui**.
6. Configurez les paramètres suivants.

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

Option	Description
Chemin d'accès au dossier réseau	Saisissez le dossier de destination dans lequel votre journal d’impression sera enregistré sur le serveur CIFS (par exemple : \\ComputerName\SharedFolder).
Nom de fichier	Saisissez le nom du fichier à utiliser pour le journal d’impression (32 caractères maximum).
Type de fichier	Sélectionnez l’option **TXT** ou **CSV** comme type de fichier pour le journal d’impression.
Origine de l'horloge du journal	Sélectionnez la source de temps pour le journal d’impression.
Méthode d'authentification	Sélectionnez la méthode d’authentification nécessaire pour accéder au serveur CIFS : **Auto**, **Kerberos**, ou **NTLMv2**. Kerberos est un protocole d’authentification qui permet à des périphériques ou des individus de prouver leur identité de façon sécurisée aux serveurs de réseau en utilisant une connexion unique. NTLMv2 est la méthode d’authentification utilisée par Windows pour la connexion aux serveurs. • **Auto** : si vous sélectionnez **Auto**, NTLMv2 servira de méthode d’authentification. • **Kerberos** : sélectionnez l’option **Kerberos** pour utiliser uniquement l’authentification Kerberos. • **NTLMv2** : sélectionnez l’option **NTLMv2** pour utiliser uniquement l’authentification NTLMv2.

Option	Description
	• Pour les authentifications **Kerberos** et **NTLMv2**, vous devez également configurer les paramètres de **Date et Heure** ou le protocole SNTP (serveur de synchronisation réseau) et le serveur DNS. • Vous pouvez aussi configurer les paramètres Date et Heure depuis le panneau de commande de l'appareil.
Nom d'utilisateur	Saisissez le nom d'utilisateur pour l'authentification (96 caractères maximum). Si le nom d'utilisateur fait partie d'un domaine, saisissez-le comme suit (au choix) : utilisateur@domaine ou domaine\utilisateur.
Mot de passe	Saisissez le mot de passe pour l'authentification (32 caractères maximum).
Adresse du serveur Kerberos (si nécessaire)	Saisissez l'adresse de l'hôte centre de distribution de clés (par exemple, kerberos.exemple.com ; 64 caractères maximum) ou l'adresse IP (par exemple, 192.168.56.189).
Réglage de la détection d'erreurs	Choisissez la mesure à prendre si le journal d'impression ne peut être enregistré sur le serveur à cause d'une erreur réseau.

7. Dans le champ **État de la connexion**, confirmez l'état du dernier journal.

Vous pouvez également confirmer l'état d'erreur sur l'écran LCD de votre appareil.

8. Cliquez sur **Envoyer** pour afficher la page **Test Journal impressions > Réseau**.

   Pour tester les paramètres, cliquez sur **Oui**, puis passez à l'étape suivante.

   Si vous ne voulez pas tester vos réglages, cliquez sur **Non**. Vos réglages seront automatiquement soumis.
9. L'appareil va tester vos réglages.
10. Si vos réglages sont acceptés, le message **Test OK** apparaît sur la page.

    Si le message **Test: Erreur** s'affiche, vérifiez tous les réglages, puis cliquez sur **Envoyer** pour afficher de nouveau la page de test.

Information associée

- Enregistrer le journal d'impression sur le réseau

Utiliser le réglage de la détection d'erreurs de l'enregistrement du journal d'impression sur le réseau

Servez-vous des paramètres de détection d'erreurs pour déterminer l'action à entreprendre si le journal d'impression ne peut pas être enregistré sur le serveur à cause d'une erreur réseau.

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 **Administrateur** > **Enreg journal d'impr sur réseau**.

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

5. Dans la section **Réglage de la détection d'erreurs**, sélectionnez l'option **Annuler l'impression** ou **Ignorer Journal & Impr**.

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

Option	Description
Annuler l'impression	Si vous sélectionnez l'option **Annuler l'impression**, les travaux d'impression sont canceled lorsque le journal d'impression ne peut pas être enregistré sur le serveur. Même si vous sélectionnez l'option **Annuler l'impression**, votre appareil imprime les fax réceptionnés.

Ignorer Journal & Impr	Si vous sélectionnez l'option **Ignorer Journal & Impr**, l'appareil imprime les documents même si le journal d'impression ne peut pas être enregistré sur le serveur.
	Lorsque la fonction d'enregistrement du journal d'impression est rétablie, le journal d'impression est enregistré comme suit :
	`Id, Type, Job Name, User Name, Date, Time, Print Pages`
	`1, Print(xxxxxxx), "Document01.doc", "user01", 03/03/20xx, 14:01:32, 52`
	`2, Print(xxxxxxx), "Document02.doc", "user01", 03/03/20xx, 14:45:30, ?` (a)
	`3, <Error>, ?, ?, ?, ?, ?` (b)
	`4, Print(xxxxxxx), "Report01.xls", "user02", 03/03/20xx, 19:30:40, 4`
	a. Si le journal d'impression ne peut être enregistré à la fin de l'impression, le nombre de pages imprimées ne sera pas enregistré.
	b. Si le journal ne peut être enregistré au début et à la fin de l'impression, le journal d'impression du travail n'est pas enregistré. Lorsque la fonction est rétablie, l'erreur est signalée dans le journal d'impression.

6. Cliquez sur **Envoyer** pour afficher la page **Test Journal impressions > Réseau**.

   Pour tester les paramètres, cliquez sur **Oui**, puis passez à l'étape suivante.

Si vous ne voulez pas tester vos réglages, cliquez sur **Non**. Vos réglages seront automatiquement soumis.

7. L’appareil va tester vos réglages.
8. Si vos réglages sont acceptés, le message **Test OK** apparaît sur la page.

   Si le message **Test: Erreur** s’affiche, vérifiez tous les réglages, puis cliquez sur **Envoyer** pour afficher de nouveau la page de test.

Information associée

- Enregistrer le journal d’impression sur le réseau

Utiliser l’enregistrement du journal d’impression sur le réseau avec Secure Function Lock 3.0

Lorsque la fonction Verrouillage fonction sécurisée 3.0 est activée, les noms des utilisateurs enregistrés pour la copie, la réception de fax, l’impression Web Connect et l’impression USB directe sont consignés dans le rapport d’enregistrement du journal d’impression sur le réseau. Lorsque l’authentification Active Directory est activée, le nom de l’utilisateur est consigné dans le rapport d’enregistrement du journal d’impression sur le réseau :

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

```
Id, Type, Job Name, User Name, Date, Time, Print Pages
1, Copy, -, -, 04/04/20xx, 09:05:12, 3
2, Fax, -, -, 04/04/20xx, 09:45:30, 5
3, Copy, -, "Bob", 04/04/20xx, 10:20:30, 4
4, Fax, -, "Bob", 04/04/20xx, 10:35:12, 3
5, USB Direct, -, "John", 04/04/20xx, 11:15:43, 6
```

Information associée

- Enregistrer le journal d’impression sur le réseau

brother

Brother Earth

www.brotherearth.com

FRE
Version 0