# Guide des fonctions de sécurité

# Table des matières

**Introduction ..... 1**
Définitions des Remarques ..... 2
Marques de commerce ..... 3
Droits d’auteur et de copie ..... 4
Avant d’utiliser les fonctions de sécurité du réseau ..... 5
Désactiver les protocoles inutiles ..... 6
**Sécurité du réseau ..... 7**
Configurer des certificats pour assurer la sécurité de l’appareil ..... 8
Aperçu des caractéristiques des certificats de sécurité ..... 9
Comment créer et installer un certificat ..... 10
Créer un certificat auto-signé ..... 11
Créer une demande 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 à l’aide de SSL/TLS ..... 27
Utiliser SNMPv3 ..... 29
Gérer votre appareil réseau en toute sécurité à l’aide de SNMPv3 ..... 30
Utiliser IPsec ..... 31
Présentation d’IPsec ..... 32
Configurer IPsec à l’aide de la Gestion à partir du Web ..... 33
Configurer un modèle d’adresse IPsec à l’aide de la Gestion à partir du Web ..... 35
Configurer un modèle IPsec à l’aide de la Gestion à partir du Web ..... 37
Utiliser l’authentification IEEE 802.1x pour votre réseau ..... 47
Qu’est-ce que l’authentification IEEE 802.1x? ..... 48
Configurez l’authentification IEEE 802.1x pour votre réseau à l’aide de la 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
Présentation de l’authentification Active Directory ..... 54
Configurer l’authentification Active Directory à l’aide de la Gestion à partir du Web ..... 55
Ouvrir une session pour modifier les paramètres de l’appareil à l’aide du panneau de commande de l’appareil (Authentification Active Directory) ..... 57
Utiliser l’authentification LDAP ..... 58
Présentation de l’authentification LDAP ..... 59
Configurer l’authentification LDAP à l’aide de la Gestion à partir du Web ..... 60
Ouvrir une session pour modifier les paramètres de l’appareil à l’aide du panneau de commande de l’appareil (Authentification LDAP) ..... 61
Utiliser la fonctionnalité Verrouillage sécuritaire des fonctions 3.0 ..... 62
Avant d’utiliser le verrouillage sécuritaire des fonctions 3.0 ..... 63
Configurer le verrouillage sécuritaire des fonctions 3.0 à l’aide de la Gestion à partir du Web ..... 64
Numériser à l’aide du verrouillage sécuritaire des fonctions 3.0 ..... 65
Configurer le mode public pour le verrouillage sécuritaire des fonctions 3.0 ..... 66

Configurer les paramètres d’écran d’accueil personnel à l’aide de la Gestion à partir du Web ..... 67
Fonctionnalités supplémentaires du verrouillage sécuritaire des fonctions 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 IC externe ..... 70
**Envoyer ou recevoir un courriel en toute sécurité ..... 71**
Configurer l'envoi ou la réception de courriels à l'aide de la gestion à partir du Web ..... 72
Envoyer un courriel en utilisant l'authentification utilisateur ..... 73
Envoyer ou recevoir un courriel en toute sécurité en utilisant SSL/TLS ..... 74
**Enregistrer le journal d’impression sur le réseau ..... 75**
Aperçu de la fonction d’enregistrement du journal d’impression sur le réseau ..... 76
Configurer les paramètres d’enregistrement du journal d’impression sur le réseau à l’aide de la Gestion à partir du Web ..... 77
Utiliser le paramètre de détection d’erreur de l’enregistrement du journal d’impression sur le réseau ..... 79
Utiliser l’enregistrement du journal d’impression sur le réseau avec le verrouillage sécuritaire des fonctions 3.0 ..... 81

# Introduction


- Définitions des Remarques
- Marques de commerce
- Droits d’auteur et de copie
- Avant d’utiliser les fonctions de sécurité du réseau

# Définitions des Remarques

Le présent guide de l'utilisateur utilise les symboles et conventions suivants :

| | |
|---|---|
| **IMPORTANT** | IMPORTANT signale une situation potentiellement dangereuse susceptible d'entraîner des dommages matériels ou une perte de fonctionnalité du produit. |
| **REMARQUE** | REMARQUE précise l'environnement d'exploitation, les conditions d'installation ou des conditions d'utilisation spéciales. |
|  | Les icônes de conseils offrent des trucs pratiques et de l'information supplémentaire. |
| **Caractères gras** | Les caractères gras identifient les boutons sur le panneau de commande de l'appareil ou sur l'écran de l'ordinateur. |
| *Caractères italiques* | Les caractères italiques mettent en valeur un point important ou signalent un sujet connexe. |

## Renseignements connexes

- Introduction

# Marques de commerce

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

Chaque société dont un logiciel est mentionné dans ce manuel possède un contrat de licence de logiciel spécifique à ses propres programmes.

**Tous les noms de marque et de produit de compagnies apparaissant sur les produits Brother, dans les documents connexes et la documentation sont tous des marques de commerce ou des marques déposées de ces compagnies respectives.**

## Renseignements connexes

- Introduction

# Droits d’auteur et de copie



## Renseignements connexes

- Introduction

# Avant d’utiliser les fonctions de sécurité du réseau

Votre appareil emploie quelques-uns des protocoles de sécurité et de cryptage les plus récents actuellement disponibles. Ces fonctions réseau peuvent être intégrées au plan de sécurité global de votre réseau de façon à contribuer à la protection de vos données et à empêcher tout accès non autorisé à l’appareil.

Il est conseillé de désactiver les protocoles FTP et TFTP. L'accès à l'appareil en utilisant ces protocoles n'est pas sécurisé.

## Renseignements connexes

- Introduction
  - Désactiver les protocoles inutiles

# Désactiver les protocoles inutiles

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

   Par exemple :

   https://192.168.1.2

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

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

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

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

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

## Renseignements connexes

- Avant d’utiliser les fonctions de sécurité du réseau

# Sécurité du réseau

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

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


- Aperçu des caractéristiques des certificats de sécurité
- Comment créer et installer un certificat
- Créer un certificat auto-signé
- Créer une demande de signature de certificat (CSR) et installer un certificat d’une autorité de certification (CA)
- Importer et exporter le certificat et la clé privée
- Importer et exporter un certificat d'autorité de certification

# Aperçu des caractéristiques des certificats de sécurité

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

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

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

Votre appareil prend en charge ce qui suit :

- Certificat préinstallé

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

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

- Certificat auto-signé

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

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

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

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

## Renseignements connexes

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

**Sujets connexes :**

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

# Comment créer et installer un certificat

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

## Option 1

### Certificat auto-signé

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

## Option 2

### Certificat d’une autorité de certification

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

## Renseignements connexes

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

# Créer un certificat auto-signé

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

   Par exemple :

   https://192.168.1.2

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

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

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

## Renseignements connexes

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

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

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

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

# Créer une demande de signature de certificat (CSR)

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

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

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

   Par exemple :

   https://192.168.1.2

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

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

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

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

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

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

## Renseignements connexes

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

# Installer un certificat sur votre appareil

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

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

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

   Par exemple :

   https://192.168.1.2

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

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

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

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

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

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

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

## Renseignements connexes

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

# Importer et exporter le certificat et la clé privée

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

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

# Importer un certificat et une clé privée

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

   Par exemple :

   https://192.168.1.2

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

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

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

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

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

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

## Renseignements connexes

- Importer et exporter le certificat et la clé privée

# Exporter le certificat et la clé privée

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

   Par exemple :

   https://192.168.1.2

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

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

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

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

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

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

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

Vous pouvez également importer le certificat sur votre ordinateur.

## Renseignements connexes

- Importer et exporter le certificat et la clé privée

# Importer et exporter un certificat d'autorité de certification

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

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

# Importer un certificat d'autorité de certification

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

   Par exemple :

   https://192.168.1.2

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

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

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

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

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

## Renseignements connexes

- Importer et exporter un certificat d'autorité de certification

# Exporter un certificat d'autorité de certification

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

   Par exemple :

   https://192.168.1.2

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

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

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

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

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

## Renseignements connexes

- Importer et exporter un certificat d'autorité de certification

# Utiliser SSL/TLS

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

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

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

# Configurer un certificat pour SSL/TLS et les protocoles disponibles

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

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

   Par exemple :

   https://192.168.1.2

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

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

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

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

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

## Renseignements connexes

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

**Sujets connexes :**

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

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

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

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

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

   Par exemple :

   https://192.168.1.2

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

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

## Renseignements connexes

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

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

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

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

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

   Par exemple :

   https://192.168.1.2

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

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

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

## Renseignements connexes

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

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

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

# Imprimer des documents à l'aide d'IPPS

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

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

   Par exemple :

   https://192.168.1.2

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

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

   Si la barre de navigation de gauche n'est pas visible, commencez la navigation à partir de ≡.
5. Assurez-vous que la case à cocher **IPP** est sélectionnée.

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

   Redémarrez votre appareil pour activer la configuration.

   Après le redémarrage de l'appareil, revenez à la page Web de l'appareil, saisissez le mot de passe, puis dans la barre de navigation de gauche, cliquez sur **Réseau** > **Réseau** > **Protocole**.
6. Cliquez sur **Paramètres du serveur HTTP**.
7. Sélectionnez la case à cocher **HTTPS(Port 443)** dans **IPP**, puis cliquez sur **Envoyer**.
8. Redémarrez votre appareil pour activer la configuration.

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

## Renseignements connexes

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

# Utiliser SNMPv3

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

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

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

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

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

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

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

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

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

7. Configurez les paramètres du mode SNMPv3.

| Option | Description |
|---|---|
| **Activé** | Le serveur d'impression utilise la version 3 du protocole SNMP. Pour gérer le serveur d'impression en toute sécurité, utilisez le mode SNMPv3. |
| **Désactivé** | Permet de désactiver la version 3 du protocole SNMP.<br>Toutes les applications qui utilisent SNMPv3 seront restreintes. Pour permettre l'utilisation des applications SNMPv3, utilisez le mode SNMPv3. |

8. Cliquez sur **Envoyer**.

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

9. Redémarrez votre appareil pour activer la configuration.

## Renseignements connexes

- Utiliser SNMPv3

# Utiliser IPsec


- Présentation d’IPsec
- Configurer IPsec à l’aide de la Gestion à partir du Web
- Configurer un modèle d’adresse IPsec à l’aide de la Gestion à partir du Web
- Configurer un modèle IPsec à l’aide de la Gestion à partir du Web

# Présentation d’IPsec

IPsec (Internet Protocol Security) est un protocole de sécurité qui se sert d'une fonction facultative de protocole Internet pour empêcher la manipulation et assurer la confidentialité des données transmises par paquets IP. IPsec chiffre les données transportées sur le réseau, telles que les données d'impression envoyées à partir d'un ordinateur vers une imprimante. Comme les données sont cryptées au niveau de la couche réseau, les applications qui emploient un protocole de niveau supérieur font appel à IPsec même si l’utilisateur n’en est pas conscient.

IPsec prend en charge les fonctions suivantes :

- Transmissions IPsec

  Selon les conditions de configuration IPsec, l’ordinateur connecté au réseau envoie des données à un appareil spécifié et en reçoit de celui-ci à l’aide du protocole IPsec. Lorsque les appareils commencent à communiquer en utilisant IPsec, des clés sont d’abord échangées à l’aide d’IKE (Internet Key Exchange), puis les données chiffrées sont transmises à l’aide de ces clés.

  De plus, IPsec utilise deux modes de fonctionnement : le mode Transport et le mode Tunnel. Le mode Transport sert principalement pour les communications entre les appareils, tandis que le mode Tunnel est utilisé dans des environnements tels qu’un réseau privé virtuel (VPN).

Pour les transmissions IPsec, les conditions suivantes doivent être remplies :

- Un ordinateur capable de communiquer à l’aide du protocole IPsec est connecté au réseau.
- Votre appareil est configuré pour la communication IPsec.
- L’ordinateur connecté à votre appareil est configuré pour les connexions IPsec.

- Paramètres IPsec

  Les paramètres qui sont nécessaires pour les connexions utilisant IPsec. Vous pouvez utiliser la Gestion à partir du Web pour configurer ces paramètres.

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

## Renseignements connexes

- Utiliser IPsec

# Configurer IPsec à l'aide de la Gestion à partir du Web

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

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

   Par exemple :

   https://192.168.1.2

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

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

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

| Option | Description |
|---|---|
| **État** | Permet d'activer ou de désactiver IPsec. |
| **Mode de négociation** | Sélectionnez **Mode de négociation** pour IKE Phase 1. IKE est un protocole qui permet d'échanger des clés de cryptage pour assurer les communications cryptées à l'aide d'IPsec.<br>Dans le mode **Principal**, la vitesse de traitement est lente, mais la sécurité est élevée. Dans le mode **Agressif**, la vitesse de traitement est plus rapide que dans le mode **Principal**, mais la sécurité est plus faible. |
| **Tout le trafic non-IPsec** | Sélectionnez l'action à effectuer pour les paquets non-IPsec.<br>Lorsque vous utilisez Web Services, vous devez sélectionner **Autoriser** pour **Tout le trafic non-IPsec**. Si vous sélectionnez **Abandonner**, il n'est pas possible d'utiliser Web Services. |
| **Raccourci de diffusion/multidiffusion** | Sélectionnez **Activé** ou **Désactivé**. |
| **Raccourci du protocole** | Sélectionnez les cases à cocher de l'option ou des options souhaitées. |
| **Règles** | Sélectionnez la case à cocher **Activé** pour activer le modèle. Lorsque vous sélectionnez plusieurs cases à cocher, les cases affichant les numéros les plus bas reçoivent la priorité en cas de conflit entre les paramètres des cases sélectionnées.<br>Cliquez sur la liste déroulante correspondante pour sélectionner le **Modèle d'adresse** utilisé pour les conditions de connexion IPsec. Pour ajouter un **Modèle d'adresse**, cliquez sur **Ajouter un modèle**.<br>Cliquez sur la liste déroulante correspondante pour sélectionner le **Modèle IPsec** utilisé pour les conditions de connexion IPsec. Pour ajouter un **Modèle IPsec**, cliquez sur **Ajouter un modèle**. |

6. Cliquez sur **Envoyer**.

   Si l'appareil nécessite un redémarrage pour activer les nouveaux paramètres, l'écran de confirmation du redémarrage s'affichera.

   Si le modèle activé dans le tableau **Règles** contient un élément vide, un message d'erreur s'affiche. Confirmez vos choix, puis cliquez de nouveau sur **Envoyer**.

## Renseignements connexes

- Utiliser IPsec

**Sujets connexes :**

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

# Configurer un modèle d’adresse IPsec à l’aide de la Gestion à partir du Web

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

   Par exemple :

   https://192.168.1.2

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

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

4. 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 la navigation à partir de ≡.

5. Cliquez sur le bouton **Supprimer** pour supprimer un **Modèle d'adresse**. Lorsqu’un **Modèle d'adresse** est en cours d’utilisation, vous ne pouvez pas le supprimer.
6. Cliquez sur le **Modèle d'adresse** que vous souhaitez créer. Le **Modèle d'adresse IPsec** apparaît.
7. Configurez les paramètres.

| Option | Description |
|---|---|
| **Nom du modèle** | Saisissez un nom pour le modèle (jusqu’à 16 caractères). |
| **Adresse IP locale** | • **Adresse IP**<br>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.<br>Si vous sélectionnez **Personnalisé** dans la liste déroulante, saisissez l’adresse IP (IPv4 ou IPv6) dans la zone de texte.<br>• **Plage d'adresses IP**<br>Saisissez les adresses IP de début et de fin pour la plage d’adresses IP dans les zones de texte. Si les adresses IP de début et de fin ne sont pas normalisées pour IPv4 ou IPv6, ou que l’adresse IP de fin est inférieure à l’adresse de début, une erreur se produira.<br>• **Adresse IP / préfixe**<br>Spécifiez l’adresse IP en utilisant une notation CIDR.<br>Par exemple : 192.168.1.1/24<br>Comme le préfixe est spécifié 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**<br>Si vous sélectionnez **Quelconque**, toutes les adresses IP sont activées.<br>• **Adresse IP**<br>Saisissez l’adresse IP spécifiée (IPv4 ou IPv6) dans la zone de texte.<br>• **Plage d'adresses IP**<br>Saisissez les première et dernière adresses IP de la plage d’adresses IP. Si les première et dernière adresses IP ne sont pas |

| Option | Description |
| --- | --- |
| | normalisées pour IPv4 ou IPv6, ou si la dernière adresse IP est inférieure à la première, une erreur se produira.<br>• **Adresse IP / préfixe**<br>Spécifiez l'adresse IP en utilisant une notation CIDR.<br>Par exemple : 192.168.1.1/24<br>Comme le préfixe est spécifié 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 actuellement utilisé, redémarrez votre appareil pour activer la configuration.

## Renseignements connexes

- Utiliser IPsec

# Configurer un modèle IPsec à l'aide de la Gestion à partir du Web

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

   Par exemple :

   https://192.168.1.2

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

   Le mot de passe par défaut pour gérer les paramètres de cet appareil se trouve au dos ou sur le fond de l'appareil. Il est indiqué par « **Pwd** ». Modifiez le mot de passe par défaut en suivant les instructions affichées à l'écran lors de la première connexion.
4. 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 la navigation à partir de ≡.
5. Cliquez sur le bouton **Supprimer** pour supprimer un **Modèle IPsec**. Lorsqu'un **Modèle IPsec** est en cours d'utilisation, vous ne pouvez pas le supprimer.
6. Cliquez sur le **Modèle IPsec** que vous souhaitez créer. L'écran **Modèle IPsec** s'affiche. Les champs de configuration varient selon les paramètres **Utiliser un modèle prédéfini** et **Internet Key Exchange (IKE)** que vous sélectionnez.
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)**, puis modifiez les paramètres, si nécessaire.
9. Cliquez sur **Envoyer**.

## Renseignements connexes

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

# Paramètres IKEv1 pour un modèle IPsec

| Option | Description |
|---|---|
| **Nom du modèle** | Saisissez un nom pour le modèle (jusqu'à 16 caractères). |
| **Utiliser un modèle prédéfini** | Sélectionnez **Personnalisé**, **Sécurité élevée IKEv1** ou **Sécurité moyenne IKEv1**. Les éléments des paramètres varient selon le modèle sélectionné. |
| **Internet Key Exchange (IKE)** | IKE est un protocole de communication qui permet d'échanger des clés de cryptage pour assurer les communications cryptées à l'aide d'IPsec. Pour assurer des communications cryptées à ce moment uniquement, l'algorithme de cryptage nécessaire pour IPsec est déterminé et les clés de cryptage sont partagées. Pour IKE, les clés de cryptage sont échangées à l'aide de la méthode d'échange de clés Diffie-Hellman et la communication cryptée limitée à IKE est assurée.<br>Si vous avez sélectionné **Personnalisé** dans **Utiliser un modèle prédéfini**, sélectionnez **IKEv1**. |
| **Type d'authentification** | • **Groupe Diffie-Hellman**<br>Cette méthode d'échange de clés permet d'échanger des clés secrètes de manière sécurisée sur un réseau non protégé. La méthode d'échange de clés Diffie-Hellman utilise un problème de logarithme discret, et non la clé secrète, pour envoyer et recevoir des informations ouvertes générées à l'aide d'un nombre aléatoire et de la clé secrète.<br>Sélectionnez **Groupe1**, **Groupe2**, **Groupe5** ou **Groupe14**.<br>• **Cryptage**<br>Sélectionnez **DES**, **3DES**, **AES-CBC 128** ou **AES-CBC 256**.<br>• **Hachage**<br>Sélectionnez **MD5**, **SHA1**, **SHA256**, **SHA384** ou **SHA512**.<br>• **Durée de vie SA**<br>Spécifiez la durée de vie IKE SA.<br>Saisissez la durée (secondes) et le nombre de kilo-octets (Ko). |
| **Sécurité d'encapsulation** | • **Protocole**<br>Sélectionnez **ESP**, **AH** ou **AH+ESP**.<br>- ESP est un protocole permettant d'assurer des communications cryptées à l'aide d'IPsec. ESP crypte la charge active (les contenus communiqués) et ajoute des informations supplémentaires. Le paquet IP comprend l'en-tête et la charge active cryptée, laquelle vient après l'en-tête. En plus des données cryptées, le paquet IP inclut également des informations relatives à la méthode de cryptage et à la clé de cryptage, les données d'authentification et d'autres informations.<br>- AH, une partie intégrante du protocole IPsec, authentifie l'expéditeur et empêche la manipulation (afin d'assurer l'intégrité) des données. Dans le paquet IP, les données sont insérées immédiatement après l'en-tête. De plus, les paquets incluent des valeurs de hachage, qui sont calculées à l'aide d'une équation provenant des contenus communiqués, de la clé secrète et autres, afin d'empêcher la falsification de l'expéditeur et la manipulation des données. Contrairement au protocole ESP, les contenus communiqués ne sont pas cryptés et les données sont envoyées et reçues sous forme de texte ordinaire. |

| Option | Description |
|---|---|
| | • **Cryptage (Non disponible pour l'option AH.)**<br>Sélectionnez **DES**, **3DES**, **AES-CBC 128** ou **AES-CBC 256**.<br>• **Hachage**<br>Sélectionnez **Aucun**, **MD5**, **SHA1**, **SHA256**, **SHA384** ou **SHA512**.<br>**Aucun** peut être sélectionné uniquement lorsque **ESP** est sélectionné pour **Protocole**.<br>• **Durée de vie SA**<br>Spécifiez la durée de vie IKE SA.<br>Saisissez la durée (secondes) et le nombre de kilo-octets (Ko).<br>• **Mode d'encapsulation**<br>Sélectionnez **Transport** ou **Tunnel**.<br>• **Adresse IP routeur distant**<br>Saisissez l'adresse IP (IPv4 ou IPv6) du routeur distant. Entrez uniquement cette information lorsque le mode **Tunnel** est sélectionné.<br>SA (Security Association) est une méthode de communication cryptée utilisant IPsec ou IPv6 et permettant d'échanger et de partager des informations, telles que la méthode de cryptage et la clé de cryptage, afin d'établir un canal de communication sécurisé avant le début de la communication. SA peut également désigner un canal de communication virtuel crypté préalablement établi. Le SA utilisé pour IPsec établit la méthode de cryptage, échange les clés et assure l'authentification mutuelle selon la procédure standard IKE (Internet Key Exchange). De plus, le SA est régulièrement mis à jour. |
| **Confidentialité de transmission parfaite (PFS)** | PFS ne dérive pas les clés des clés précédentes qui ont été utilisées pour crypter des messages. De plus, si une clé utilisée pour crypter un message est dérivée d'une clé parente, cette clé parente n'est pas utilisée pour dériver d'autres clés. Par conséquent, même si une clé est compromise, le dommage est limité uniquement aux messages qui ont été cryptés à l'aide de cette clé.<br>Sélectionnez **Activé** ou **Désactivé**. |
| **Méthode d'authentification** | Sélectionnez la méthode d'authentification. Sélectionnez **Clé pré-partagée** ou **Certificats**. |
| **Clé pré-partagée** | Lors du cryptage de la communication, la clé de cryptage est échangée et partagée avant l'utilisation d'un autre canal.<br>Si vous avez sélectionné **Clé pré-partagée** pour la **Méthode d'authentification**, saisissez la **Clé pré-partagée** (jusqu'à 32 caractères).<br>• **Local/Type d'identifiant/Identifiant**<br>Sélectionnez le type d'identifiant de l'expéditeur, puis saisissez l'identifiant.<br>Sélectionnez **Adresse IPv4**, **Adresse IPv6**, **FQDN**, **Adresse de courriel** ou **Certificat** pour le type.<br>Si vous sélectionnez **Certificat**, saisissez le nom commun du certificat dans le champ **ID**.<br>• **Distant/Type d'identifiant/Identifiant**<br>Sélectionnez le type d'identifiant du destinataire, puis saisissez l'identifiant.<br>Sélectionnez **Adresse IPv4**, **Adresse IPv6**, **FQDN**, **Adresse de courriel** ou **Certificat** pour le type.<br>Si vous sélectionnez **Certificat**, saisissez le nom commun du certificat dans le champ **ID**. |

| Option | Description |
| --- | --- |
| **Certificat** | Si vous avez sélectionné **Certificats** pour **Méthode d'authentification**, sélectionnez le certificat.<br><br>Vous pouvez uniquement sélectionner les certificats créés à l'aide de la page **Certificat** de l'écran de configuration de sécurité de la gestion à partir du Web. |

## Renseignements connexes

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

# Paramètres IKEv2 pour un modèle IPsec

| Option | Description |
|---|---|
| **Nom du modèle** | Saisissez un nom pour le modèle (jusqu'à 16 caractères). |
| **Utiliser un modèle prédéfini** | Sélectionnez **Personnalisé**, **Sécurité élevée IKEv2** ou **Sécurité moyenne IKEv2**. Les éléments des paramètres varient selon le modèle sélectionné. |
| **Internet Key Exchange (IKE)** | IKE est un protocole de communication qui permet d'échanger des clés de cryptage pour assurer les communications cryptées à l'aide d'IPsec. Pour assurer des communications cryptées à ce moment uniquement, l'algorithme de cryptage nécessaire pour IPsec est déterminé et les clés de cryptage sont partagées. Pour IKE, les clés de cryptage sont échangées à l'aide de la méthode d'échange de clés Diffie-Hellman et la communication cryptée limitée à IKE est assurée.<br>Si vous avez sélectionné **Personnalisé** dans **Utiliser un modèle prédéfini**, sélectionnez **IKEv2**. |
| **Type d'authentification** | • **Groupe Diffie-Hellman**<br>Cette méthode d'échange de clés permet d'échanger des clés secrètes de manière sécurisée sur un réseau non protégé. La méthode d'échange de clés Diffie-Hellman utilise un problème de logarithme discret, et non la clé secrète, pour envoyer et recevoir des informations ouvertes générées à l'aide d'un nombre aléatoire et de la clé secrète.<br>Sélectionnez **Groupe1**, **Groupe2**, **Groupe5** ou **Groupe14**.<br>• **Cryptage**<br>Sélectionnez **DES**, **3DES**, **AES-CBC 128** ou **AES-CBC 256**.<br>• **Hachage**<br>Sélectionnez **MD5**, **SHA1**, **SHA256**, **SHA384** ou **SHA512**.<br>• **Durée de vie SA**<br>Spécifiez la durée de vie IKE SA.<br>Saisissez la durée (secondes) et le nombre de kilo-octets (Ko). |
| **Sécurité d'encapsulation** | • **Protocole**<br>Sélectionnez **ESP**.<br>ESP est un protocole permettant d'assurer des communications cryptées à l'aide d'IPsec. ESP crypte la charge active (les contenus communiqués) et ajoute des informations supplémentaires. Le paquet IP comprend l'en-tête et la charge active cryptée, laquelle vient après l'en-tête. En plus des données cryptées, le paquet IP inclut également des informations relatives à la méthode de cryptage et à la clé de cryptage, les données d'authentification et d'autres informations.<br>• **Cryptage**<br>Sélectionnez **DES**, **3DES**, **AES-CBC 128** ou **AES-CBC 256**.<br>• **Hachage**<br>Sélectionnez **MD5**, **SHA1**, **SHA256**, **SHA384** ou **SHA512**.<br>• **Durée de vie SA**<br>Spécifiez la durée de vie IKE SA.<br>Saisissez la durée (secondes) et le nombre de kilo-octets (Ko).<br>• **Mode d'encapsulation**<br>Sélectionnez **Transport** ou **Tunnel**. |

| Option | Description |
| --- | --- |
| | • **Adresse IP routeur distant**<br>Saisissez l'adresse IP (IPv4 ou IPv6) du routeur distant. Entrez uniquement cette information lorsque le mode **Tunnel** est sélectionné.<br>SA (Security Association) est une méthode de communication cryptée utilisant IPsec ou IPv6 et permettant d'échanger et de partager des informations, telles que la méthode de cryptage et la clé de cryptage, afin d'établir un canal de communication sécurisé avant le début de la communication. SA peut également désigner un canal de communication virtuel crypté préalablement établi. Le SA utilisé pour IPsec établit la méthode de cryptage, échange les clés et assure l'authentification mutuelle selon la procédure standard IKE (Internet Key Exchange). De plus, le SA est régulièrement mis à jour. |
| **Confidentialité de transmission parfaite (PFS)** | PFS ne dérive pas les clés des clés précédentes qui ont été utilisées pour crypter des messages. De plus, si une clé utilisée pour crypter un message est dérivée d'une clé parente, cette clé parente n'est pas utilisée pour dériver d'autres clés. Par conséquent, même si une clé est compromise, le dommage est limité uniquement aux messages qui ont été cryptés à l'aide de cette clé.<br>Sélectionnez **Activé** ou **Désactivé**. |
| **Méthode d'authentification** | Sélectionnez la méthode d'authentification. Sélectionnez **Clé pré-partagée**, **Certificats**, **EAP - MD5**, ou **EAP - MS-CHAPv2**.<br>EAP est un protocole d'authentification constituant une extension de PPP. En utilisant EAP avec IEEE802.1x, une clé différente est utilisée pour l'authentification de l'utilisateur pendant chaque session.<br>Les paramètres suivants sont nécessaires uniquement lorsque **EAP - MD5** ou **EAP - MS-CHAPv2** est sélectionné dans **Méthode d'authentification** :<br>• **Mode**<br>Sélectionnez **Mode serveur** ou **Mode client**.<br>• **Certificat**<br>Sélectionnez le certificat.<br>• **Nom d'utilisateur**<br>Saisissez le nom d'utilisateur (jusqu'à 32 caractères).<br>• **Mot de passe**<br>Saisissez le mot de passe (jusqu'à 32 caractères). Vous devez entrer le mot de passe deux fois pour le confirmer. |
| **Clé pré-partagée** | Lors du cryptage de la communication, la clé de cryptage est échangée et partagée avant l'utilisation d'un autre canal.<br>Si vous avez sélectionné **Clé pré-partagée** pour la **Méthode d'authentification**, saisissez la **Clé pré-partagée** (jusqu'à 32 caractères).<br>• **Local/Type d'identifiant/Identifiant**<br>Sélectionnez le type d'identifiant de l'expéditeur, puis saisissez l'identifiant.<br>Sélectionnez **Adresse IPv4**, **Adresse IPv6**, **FQDN**, **Adresse de courriel** ou **Certificat** pour le type.<br>Si vous sélectionnez **Certificat**, saisissez le nom commun du certificat dans le champ **ID**. |

| Option | Description |
| --- | --- |
| | • **Distant/Type d'identifiant/Identifiant**<br>Sélectionnez le type d’identifiant du destinataire, puis saisissez l’identifiant.<br>Sélectionnez **Adresse IPv4**, **Adresse IPv6**, **FQDN**, **Adresse de courriel** ou **Certificat** pour le type.<br>Si vous sélectionnez **Certificat**, saisissez le nom commun du certificat dans le champ **ID**. |
| **Certificat** | Si vous avez sélectionné **Certificats** pour **Méthode d'authentification**, sélectionnez le certificat.<br>Vous pouvez uniquement sélectionner les certificats créés à l’aide de la page **Certificat** de l’écran de configuration de sécurité de la gestion à partir du Web. |

## Renseignements connexes

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

# Paramètres manuels pour un modèle IPsec

| Option | Description |
|---|---|
| **Nom du modèle** | Saisissez un nom pour le modèle (jusqu'à 16 caractères). |
| **Utiliser un modèle prédéfini** | Sélectionnez **Personnalisé**. |
| **Internet Key Exchange (IKE)** | IKE est un protocole de communication qui permet d'échanger des clés de cryptage pour assurer les communications cryptées à l'aide d'IPsec. Pour assurer des communications cryptées à ce moment uniquement, l'algorithme de cryptage nécessaire pour IPsec est déterminé et les clés de cryptage sont partagées. Pour IKE, les clés de cryptage sont échangées à l'aide de la méthode d'échange de clés Diffie-Hellman et la communication cryptée limitée à IKE est assurée.<br>Sélectionnez **Manuel**. |
| **Clé d'authentification (ESP, AH)** | Saisissez les valeurs **Entrée/Sortie**.<br>Ces paramètres sont nécessaires lorsque **Personnalisé** est sélectionné pour **Utiliser un modèle prédéfini**, que **Manuel** est sélectionné pour **Internet Key Exchange (IKE)** et qu'un paramètre autre que **Aucun** est sélectionné pour **Hachage** dans la section **Sécurité d'encapsulation**.<br>Le nombre de caractères que vous pouvez définir varie selon le paramètre sélectionné pour **Hachage** dans la section **Sécurité d'encapsulation**.<br>Si la longueur de la clé d'authentification spécifiée est différente de l'algorithme de hachage sélectionné, une erreur se produira.<br>• **MD5** : 128 bits (16 octets)<br>• **SHA1** : 160 bits (20 octets)<br>• **SHA256** : 256 bits (32 octets)<br>• **SHA384** : 384 bits (48 octets)<br>• **SHA512** : 512 bits (64 octets)<br>Lorsque vous spécifiez la clé en code ASCII, encadrez les caractères à l'aide de guillemets doubles (« »). |
| **Clé de code (ESP)** | Saisissez les valeurs **Entrée/Sortie**.<br>Ces paramètres sont nécessaires lorsque **Personnalisé** est sélectionné pour **Utiliser un modèle prédéfini**, que **Manuel** est sélectionné pour **Internet Key Exchange (IKE)** et que **ESP** est sélectionné pour **Protocole**, dans **Sécurité d'encapsulation**.<br>Le nombre de caractères que vous pouvez définir varie selon le paramètre sélectionné pour **Cryptage** dans la section **Sécurité d'encapsulation**.<br>Si la longueur de la clé de code spécifiée est différente de l'algorithme de cryptage sélectionné, une erreur se produira.<br>• **DES** : 64 bits (8 octets)<br>• **3DES** : 192 bits (24 octets)<br>• **AES-CBC 128** : 128 bits (16 octets)<br>• **AES-CBC 256** : 256 bits (32 octets)<br>Lorsque vous spécifiez la clé en code ASCII, encadrez les caractères à l'aide de guillemets doubles (« »). |
| **SPI** | Ces paramètres permettent d'identifier les informations de sécurité. En général, un hôte utilise plusieurs SA (Security Associations – Associations de sécurité) pour différents types de communication IPsec. Par conséquent, il est nécessaire d'identifier le SA applicable |

| Option | Description |
|---|---|
| | lors de la réception d'un paquet IPsec. Le paramètre SPI, qui identifie le SA, est inclus dans l'en-tête AH (Authentication Header – En-tête d'authentification) et ESP (Encapsulating Security Payload – Charge active de sécurité d'encapsulation).<br>Ces paramètres sont nécessaires lorsque **Personnalisé** est sélectionné pour **Utiliser un modèle prédéfini** et que **Manuel** est sélectionné pour **Internet Key Exchange (IKE)**.<br>Entrez les valeurs **Entrée/Sortie**. (3 à 10 caractères) |
| **Sécurité d'encapsulation** | • **Protocole**<br>Sélectionnez **ESP** ou **AH**.<br>- ESP est un protocole permettant d'assurer des communications cryptées à l'aide d'IPsec. ESP crypte la charge active (les contenus communiqués) et ajoute des informations supplémentaires. Le paquet IP comprend l'en-tête et la charge active cryptée, laquelle vient après l'en-tête. En plus des données cryptées, le paquet IP inclut également des informations relatives à la méthode de cryptage et à la clé de cryptage, les données d'authentification et d'autres informations.<br>- AH, une partie intégrante du protocole IPsec, authentifie l'expéditeur et empêche la manipulation des données (afin d'assurer l'intégrité des données). Dans le paquet IP, les données sont insérées immédiatement après l'en-tête. De plus, les paquets incluent des valeurs de hachage, qui sont calculées à l'aide d'une équation provenant des contenus communiqués, de la clé secrète et autres, afin d'empêcher la falsification de l'expéditeur et la manipulation des données. Contrairement au protocole ESP, les contenus communiqués ne sont pas cryptés et les données sont envoyées et reçues sous forme de texte ordinaire.<br>• **Cryptage (Non disponible pour l'option AH.)**<br>Sélectionnez **DES**, **3DES**, **AES-CBC 128** ou **AES-CBC 256**.<br>• **Hachage**<br>Sélectionnez **Aucun**, **MD5**, **SHA1**, **SHA256**, **SHA384** ou **SHA512**.<br>**Aucun** peut être sélectionné uniquement lorsque **ESP** est sélectionné pour **Protocole**.<br>• **Durée de vie SA**<br>Spécifiez la durée de vie IKE SA.<br>Saisissez la durée (secondes) et le nombre de kilo-octets (Ko).<br>• **Mode d'encapsulation**<br>Sélectionnez **Transport** ou **Tunnel**.<br>• **Adresse IP routeur distant**<br>Saisissez l'adresse IP (IPv4 ou IPv6) du routeur distant. Entrez uniquement cette information lorsque le mode **Tunnel** est sélectionné. |

| Option | Description |
| --- | --- |
| | SA (Security Association) est une méthode de communication cryptée utilisant IPsec ou IPv6 et permettant d'échanger et de partager des informations, telles que la méthode de cryptage et la clé de cryptage, afin d'établir un canal de communication sécurisé avant le début de la communication. SA peut également désigner un canal de communication virtuel crypté préalablement établi. Le SA utilisé pour IPsec établit la méthode de cryptage, échange les clés et assure l'authentification mutuelle selon la procédure standard IKE (Internet Key Exchange). De plus, le SA est régulièrement mis à jour. |

## Renseignements connexes

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

# Utiliser l’authentification IEEE 802.1x pour votre réseau


- Qu’est-ce que l’authentification IEEE 802.1x?
- Configurez l’authentification IEEE 802.1x pour votre réseau à l’aide de la gestion à partir du Web (navigateur Web)
- Méthodes d’authentification IEEE 802.1x

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

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

## Renseignements connexes

- Utiliser l’authentification IEEE 802.1x pour votre réseau

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

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

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

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

   Par exemple :

   https://192.168.1.2

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

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

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

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

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

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

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

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

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

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

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

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

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

## Renseignements connexes

- Utiliser l'authentification IEEE 802.1x pour votre réseau

**Sujets connexes :**

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

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

# Méthodes d'authentification IEEE 802.1x

**EAP-FAST**

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

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

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

**EAP-MD5 (réseau câblé)**

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

**PEAP**

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

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

- PEAP/MS-CHAPv2
- PEAP/GTC

**EAP-TTLS**

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

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

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

**EAP-TLS**

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

## Renseignements connexes

- Utiliser l'authentification IEEE 802.1x pour votre réseau

# Authentification de l’utilisateur


- Utiliser l’authentification Active Directory
- Utiliser l’authentification LDAP
- Utiliser la fonctionnalité Verrouillage sécuritaire des fonctions 3.0

# Utiliser l’authentification Active Directory


- Présentation de l’authentification Active Directory
- Configurer l’authentification Active Directory à l’aide de la Gestion à partir du Web
- Ouvrir une session pour modifier les paramètres de l’appareil à l’aide du panneau de commande de l’appareil (Authentification Active Directory)

# Présentation de l’authentification Active Directory

L’authentification Active Directory limite l’utilisation de votre appareil. Lorsque l’authentification Active Directory est activée, le panneau de commande de l’appareil est verrouillé. Vous ne pouvez pas modifier les paramètres de l’appareil avant d’avoir entré un nom d’utilisateur et un mot de passe.

L’authentification Active Directory propose les fonctions suivantes :

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

- Enregistrement des données d’impression entrantes
- Enregistrement des données de télécopie entrantes
- Obtention de l’adresse électronique à partir du serveur Active Directory en fonction de votre nom d’utilisateur lors de l’envoi de données numérisées à un serveur de messagerie.

  Pour utiliser cette fonction, sélectionnez l’option **Activé** du paramètre **Obtenir l'adresse courriel** et la méthode d’authentification **LDAP + kerberos** ou **LDAP + NTLMv2**. Votre adresse électronique est définie en tant qu’expéditeur lorsque l’appareil envoie des données numérisées à un serveur de messagerie, ou en tant que destinataire si vous souhaitez envoyer des données numérisées à votre adresse électronique.

Lorsque l’authentification Active Directory est activée, votre appareil enregistre toutes les données de télécopie entrantes. Après l’ouverture d’une session, l’appareil imprime les données de télécopie enregistrées.

Vous pouvez modifier les paramètres d’authentification Active Directory en utilisant la Gestion à partir du Web.

## Renseignements connexes

- Utiliser l’authentification Active Directory

# Configurer l'authentification Active Directory à l'aide de la 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 temps du réseau) et la configuration du serveur DNS pour l'authentification.

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

   Par exemple :

   https://192.168.1.2

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

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

4. Dans la barre de navigation de gauche, cliquez sur **Administrateur** > **Fonction de restriction d'utilisateur** ou **Gestion des restrictions**.

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

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

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

| Option | Description |
|---|---|
| **Stockage des données RX de télécopie** | Sélectionnez cette option pour enregistrer des données de télécopie entrantes. Vous pouvez imprimer toutes les données de télécopie entrantes après l'ouverture d'une session sur l'appareil. |
| **Mémoriser l'ID utilisateur** | Sélectionnez cette option pour enregistrer votre nom d'utilisateur. |
| **Adresse du serveur Active Directory** | Saisissez l'adresse IP ou le nom de serveur (par exemple : ad.exemple.com) du serveur Active Directory. |
| **Nom de domaine du 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 du serveur LDAP** | Saisissez le numéro de port pour connecter le serveur Active Directory via LDAP (disponible uniquement pour la méthode d'authentification **LDAP + kerberos** ou **LDAP + NTLMv2**). |

| Option | Description |
| --- | --- |
| **Racine de recherche LDAP** | Saisissez la racine de recherche LDAP (disponible uniquement pour la méthode d'authentification **LDAP + kerberos** ou **LDAP + NTLMv2**). |
| **Obtenir l'adresse courriel** | Sélectionnez cette option pour obtenir l'adresse électronique de l'utilisateur connecté à partir 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 personnel en tant que destination Numérisation vers réseau. (disponible uniquement pour la méthode d'authentification **LDAP + kerberos** ou **LDAP + NTLMv2**) |

9. Cliquez sur **Envoyer**.

## Renseignements connexes

- Utiliser l'authentification Active Directory

# Ouvrir une session pour modifier les paramètres de l’appareil à l’aide du panneau de commande de l’appareil (Authentification Active Directory)

Lorsque l’authentification Active Directory est activée, le panneau de commande de l’appareil est verrouillé jusqu’à ce que vous entriez votre nom d’utilisateur et le mot de passe sur le panneau de commande de l’appareil.

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

## Renseignements connexes

- Utiliser l’authentification Active Directory

# Utiliser l’authentification LDAP

- Présentation de l’authentification LDAP
- Configurer l’authentification LDAP à l’aide de la Gestion à partir du Web
- Ouvrir une session pour modifier les paramètres de l’appareil à l’aide du panneau de commande de l’appareil (Authentification LDAP)

# Présentation de l’authentification LDAP

L’authentification LDAP limite l’utilisation de votre appareil. Lorsque l’authentification LDAP est activée, le panneau de commande de l’appareil est verrouillé. Vous ne pouvez pas modifier les paramètres de l’appareil avant d’avoir entré un nom d’utilisateur et un mot de passe.

L’authentification LDAP propose les fonctions suivantes :

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

- Enregistrement des données d’impression entrantes
- Enregistrement des données de télécopie entrantes
- Obtention de l’adresse électronique à partir du serveur LDAP en fonction de votre nom d’utilisateur lors de l’envoi de données numérisées à un serveur de messagerie.

  Pour utiliser cette fonction, sélectionnez l’option **Activé** du paramètre **Obtenir l'adresse courriel**. Votre adresse électronique est définie en tant qu’expéditeur lorsque l’appareil envoie des données numérisées à un serveur de messagerie, ou en tant que destinataire si vous souhaitez envoyer des données numérisées à votre adresse électronique.

Lorsque l’authentification LDAP est activée, votre appareil enregistre toutes les données de télécopie entrantes. Après l’ouverture d’une session, l’appareil imprime les données de télécopie enregistrées.

Vous pouvez modifier les paramètres d’authentification LDAP en utilisant la Gestion à partir du Web.

## Renseignements connexes

- Utiliser l’authentification LDAP

# Configurer l'authentification LDAP à l'aide de la Gestion à partir du Web

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

   Par exemple :

   https://192.168.1.2

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

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

4. Dans la barre de navigation de gauche, cliquez sur **Administrateur** > **Fonction de restriction d'utilisateur** ou **Gestion des restrictions**.

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

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

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

| Option | Description |
|---|---|
| **Stockage des données RX de télécopie** | Sélectionnez cette option pour enregistrer des données de télécopie entrantes. Vous pouvez imprimer toutes les données de télécopie entrantes après l'ouverture d'une session sur 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 (par exemple : ldap.exemple.com) du serveur LDAP. |
| **SSL/TLS** | Sélectionnez l'option **SSL/TLS** pour utiliser LDAP sur SSL/TLS. |
| **Port du serveur LDAP** | Saisissez le numéro de port du serveur LDAP. |
| **Racine de recherche LDAP** | Saisissez le répertoire racine de recherche LDAP. |
| **Attribut nom (Clé de recherche)** | Saisissez l'attribut que vous souhaitez utiliser comme clé de recherche. |
| **Obtenir l'adresse courriel** | Sélectionnez cette option pour obtenir l'adresse électronique de l'utilisateur connecté à partir du serveur LDAP. |
| **Obtenir le répertoire de base de l'utilisateur** | Sélectionnez cette option pour obtenir votre répertoire personnel en tant que destination Numérisation vers réseau. |

9. Cliquez sur **Envoyer**.

## Renseignements connexes

- Utiliser l'authentification LDAP

# Ouvrir une session pour modifier les paramètres 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 est verrouillé jusqu’à ce que vous entriez votre nom d’utilisateur et le mot de passe sur le panneau de commande de l’appareil.

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

## Renseignements connexes

- Utiliser l’authentification LDAP

# Utiliser la fonctionnalité Verrouillage sécuritaire des fonctions 3.0

La fonctionnalité Verrouillage sécuritaire des fonctions 3.0 renforce la sécurité en limitant les fonctions disponibles sur votre appareil.


- Avant d’utiliser le verrouillage sécuritaire des fonctions 3.0
- Configurer le verrouillage sécuritaire des fonctions 3.0 à l’aide de la Gestion à partir du Web
- Numériser à l’aide du verrouillage sécuritaire des fonctions 3.0
- Configurer le mode public pour le verrouillage sécuritaire des fonctions 3.0
- Configurer les paramètres d’écran d’accueil personnel à l’aide de la Gestion à partir du Web
- Fonctionnalités supplémentaires du verrouillage sécuritaire des fonctions 3.0
- Enregistrer une nouvelle carte à CI à l’aide du panneau de commande de l’appareil
- Enregistrer un lecteur de carte IC externe

# Avant d’utiliser le verrouillage sécuritaire des fonctions 3.0

Utilisez la fonctionnalité Verrouillage sécuritaire des fonctions pour configurer des mots de passe, fixer des limites de page spécifiques selon les utilisateurs et donner accès à l'ensemble ou à une partie des fonctions répertoriées ici.

Vous pouvez configurer et modifier les paramètres suivants de Verrouillage sécuritaire des fonctions 3.0 à l’aide de la Gestion à partir du Web :

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

- **Imprimer**
- **Copie**
- **Numériser**
- **Fax**
- **Support**
- **Connect. Web**
- **Applis**
- **Limites de page**
- **Compteurs de pages**
- **ID carte (ID NFC)**

Modèles à écran tactile ACL :

Lorsque Verrouillage sécuritaire des fonctions est activé, l’appareil entre automatiquement en mode public et l’accès à certaines de ses fonctions est réservé aux utilisateurs autorisés uniquement. Pour accéder aux fonctions à accès restreint de l’appareil, appuyez sur , sélectionnez votre nom d’utilisateur et entrez votre mot de passe.

## Renseignements connexes

- Utiliser la fonctionnalité Verrouillage sécuritaire des fonctions 3.0

# Configurer le verrouillage sécuritaire des fonctions 3.0 à l'aide de la Gestion à partir du Web

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

   Par exemple :

   https://192.168.1.2

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

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

4. Dans la barre de navigation de gauche, cliquez sur **Administrateur** > **Fonction de restriction d'utilisateur** ou **Gestion des restrictions**.

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

5. Sélectionnez **Verrouillage sécuritaire des fonctions**.
6. Cliquez sur **Envoyer**.
7. Cliquez sur le menu **Fonctions restreintes**.
8. Configurez les paramètres pour gérer les restrictions par utilisateur ou par groupe.
9. Cliquez sur **Envoyer**.
10. Cliquez sur le menu **Liste d'utilisateurs**.
11. Configurez la liste des utilisateurs.
12. Cliquez sur **Envoyer**.

Vous pouvez également modifier les paramètres de blocage par liste d'utilisateurs dans le menu **Verrouillage sécuritaire des fonctions**.

## Renseignements connexes

- Utiliser la fonctionnalité Verrouillage sécuritaire des fonctions 3.0

# Numériser à l’aide du verrouillage sécuritaire des fonctions 3.0

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

## Configuration des restrictions de numérisation (pour les administrateurs)

Verrouillage sécuritaire des fonctions 3.0 permet à un administrateur de limiter l’accès à la fonction de numérisation à certains utilisateurs. Lorsque la fonction de numérisation est désactivée pour le paramètre d'utilisateurs publics, seuls les utilisateurs dont la case **Numériser** est cochée pourront effectuer des numérisations.

## Utilisation de la fonction de numérisation (pour les utilisateurs restreints)

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

  Les utilisateurs restreints doivent entrer leur mot de passe sur le panneau de commande de l'appareil pour accéder au mode de numérisation.
- Pour numériser à partir d’un ordinateur :

  Les utilisateurs restreints doivent entrer leur mot de passe sur le panneau de commande de l'appareil pour pouvoir effectuer une numérisation à partir de 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 disposant d'un accès restreint pourront également accéder au mode Numériser en approchant leurs cartes à CI enregistrées du symbole NFC sur le panneau de commande de l'appareil.

## Renseignements connexes

- Utiliser la fonctionnalité Verrouillage sécuritaire des fonctions 3.0

# Configurer le mode public pour le verrouillage sécuritaire des fonctions 3.0

Utilisez l'écran de verrouillage sécuritaire des fonctions pour configurer le mode public qui limite les fonctions disponibles pour les utilisateurs publics. Les utilisateurs publics ne seront pas obligés d'entrer un mot de passe pour accéder aux fonctions rendues accessibles par les paramètres du mode public.

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

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

   Par exemple :

   https://192.168.1.2

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

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

4. Dans la barre de navigation de gauche, cliquez sur **Administrateur** > **Fonction de restriction d'utilisateur** ou **Gestion des restrictions**.

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

5. Sélectionnez **Verrouillage sécuritaire des fonctions**.
6. Cliquez sur **Envoyer**.
7. Cliquez sur le menu **Fonctions restreintes**.
8. Sur la ligne **Mode public**, cochez une case pour autoriser la fonction indiquée, ou décochez une case pour l'interdire.
9. Cliquez sur **Envoyer**.

## Renseignements connexes

- Utiliser la fonctionnalité Verrouillage sécuritaire des fonctions 3.0

# Configurer les paramètres d'écran d'accueil personnel à l'aide de la Gestion à partir du Web

En tant qu'administrateur, vous pouvez spécifier quels onglets les utilisateurs peuvent afficher sur leurs écrans de page d'accueil. Ces onglets fournissent un accès rapide aux raccourcis favoris des utilisateurs qu'ils peuvent affecter à leurs onglets personnels d'écran d'accueil à partir du panneau de commande de l'appareil.

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

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

   Par exemple :

   https://192.168.1.2

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

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

4. Dans la barre de navigation de gauche, cliquez sur **Administrateur** > **Fonction de restriction d'utilisateur** ou **Gestion des restrictions**.

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

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

## Renseignements connexes

- Utiliser la fonctionnalité Verrouillage sécuritaire des fonctions 3.0

# Fonctionnalités supplémentaires du verrouillage sécuritaire des fonctions 3.0

Configurez les fonctions suivantes dans l’écran de verrouillage sécuritaire des fonctions :

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

**Réinitialiser tous les compteurs**

Cliquez sur **Réinitialiser tous les compteurs**, dans la colonne **Compteurs de pages**, pour remettre à zéro le compteur de pages.

**Exporter vers un fichier CSV**

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

**ID carte (ID NFC)**

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

**Sortie**

Lorsque l’unité 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 après la remise à zéro du compteur.

**Initialisation auto du compteur**

Cliquez sur **Initialisation auto du compteur** pour configurer l'intervalle souhaité entre les remises à zéro du compteur de pages. Choisissez un intervalle quotidien, hebdomadaire ou mensuel.

## Renseignements connexes

- Utiliser la fonctionnalité Verrouillage sécuritaire des fonctions 3.0

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

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

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

1. Touchez le symbole NFC (Near-Field Communication) sur le panneau de commande de l’appareil avec une carte à circuit intégré (carte à CI) enregistrée.
2. Appuyez sur votre identifiant d'utilisateur sur l’écran ACL.
3. Appuyez sur le bouton Enregistrer carte.
4. Touchez le symbole NFC avec une nouvelle carte à CI.

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

## Renseignements connexes

- Utiliser la fonctionnalité Verrouillage sécuritaire des fonctions 3.0

# Enregistrer un lecteur de carte IC externe

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

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

   Par exemple :

   https://192.168.1.2

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

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

4. Dans la barre de navigation de gauche, cliquez sur **Administrateur** > **Lecteur de carte externe**.

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

5. Saisissez les informations requises, puis cliquez sur **Envoyer**.
6. Redémarrez votre appareil Brother pour activer la configuration.
7. Connectez le lecteur de carte à votre appareil.
8. Pour utiliser l'authentification par carte, touchez le lecteur de carte avec la carte.

## Renseignements connexes

- Utiliser la fonctionnalité Verrouillage sécuritaire des fonctions 3.0

# Envoyer ou recevoir un courriel en toute sécurité


- Configurer l'envoi ou la réception de courriels à l'aide de la gestion à partir du Web
- Envoyer un courriel en utilisant l'authentification utilisateur
- Envoyer ou recevoir un courriel en toute sécurité en utilisant SSL/TLS

# Configurer l'envoi ou la réception de courriels à l'aide de la gestion à partir du Web

- La réception de courriels n'est disponible que sur certains modèles.
- Il est conseillé d'utiliser la gestion à partir du Web pour configurer l'envoi sécurisé de courriels en utilisant l'authentification utilisateur, ou l'envoi et la réception de courriels à l'aide de SSL/TLS (modèles compatibles uniquement).

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

   Par exemple :

   https://192.168.1.2

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

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

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

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

5. Dans le champ **Client POP3/IMAP4/SMTP**, cliquez sur **Paramètres avancés** et vérifiez que le statut de **Client POP3/IMAP4/SMTP** est **Activé**.

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

6. Configurez les paramètres **Client POP3/IMAP4/SMTP**.
   - Vérifiez si les paramètres de courriel sont corrects après la configuration en envoyant un courriel de test.
   - Si vous ne connaissez pas les paramètres du serveur POP3/IMAP4/SMTP, contactez votre 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 réception/d'envoi de courriel** s'affiche.
8. Suivez les instructions de la boîte de dialogue pour tester les paramètres actuels.

## Renseignements connexes

- Envoyer ou recevoir un courriel en toute sécurité

**Sujets connexes :**

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

# Envoyer un courriel en utilisant l'authentification utilisateur

Votre appareil envoie les courriels par l'intermédiaire d'un serveur de messagerie exigeant une authentification de l'utilisateur. Cette méthode empêche que des utilisateurs non autorisés n'accèdent au serveur de messagerie.

Vous pouvez envoyer des notifications de courriels, des rapports de courriels ainsi que des I-Fax (fonctionnalité disponible sur certains modèles uniquement).

- Les protocoles disponibles peuvent varier en fonction de l'appareil.
- Il est conseillé d'utiliser la 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 plus de détails sur les paramètres du serveur de messagerie, contactez votre administrateur de réseau ou votre fournisseur d'accès Internet (FAI).

Pour activer l'authentification du serveur SMTP à l'aide de la gestion à partir du Web, sélectionnez votre méthode d'authentification sous **Méthode d'authentification du serveur** dans l'écran **Client POP3/IMAP4/SMTP**.

## Renseignements connexes

- Envoyer ou recevoir un courriel en toute sécurité

# Envoyer ou recevoir un courriel 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 de courriels n'est disponible que sur certains modèles.
- Il est conseillé d'utiliser la Gestion à partir du Web pour configurer SSL/TLS.

## Vérifier le certificat du serveur

Sous **SSL/TLS**, si vous choisissez **SSL** ou **TLS**, la case à cocher **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, décochez 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 le numéro de port après avoir sélectionné les paramètres de **SSL/TLS**.

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

Dans la plupart des cas, les services Webmail sécurisés nécessitent les paramètres suivants :

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

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

## Renseignements connexes

- Envoyer ou recevoir un courriel en toute sécurité

**Sujets connexes :**

- Configurer l'envoi ou la réception de courriels à l'aide de la gestion à partir du Web
- Configurer des certificats pour assurer la sécurité de l'appareil

# Enregistrer le journal d’impression sur le réseau


- Aperçu de la fonction d’enregistrement du journal d’impression sur le réseau
- Configurer les paramètres d’enregistrement du journal d’impression sur le réseau à l’aide de la Gestion à partir du Web
- Utiliser le paramètre de détection d’erreur de l’enregistrement du journal d’impression sur le réseau
- Utiliser l’enregistrement du journal d’impression sur le réseau avec le verrouillage sécuritaire des fonctions 3.0

# Aperçu de la fonction d’enregistrement du journal d’impression sur le réseau

La fonction d’enregistrement du journal d’impression sur le réseau vous permet d’enregistrer le fichier du journal d’impression de votre appareil sur un serveur réseau à l’aide du protocole CIFS (Common Internet File System). Pour chaque tâche d’impression, vous pouvez consigner l’identifiant, le type de tâche d’impression, le nom de la tâche, le nom d’utilisateur, la date, l’heure et le nombre de pages imprimées. CIFS est un protocole fonctionnant sur TCP/IP qui permet aux ordinateurs d’un réseau de partager des fichiers via Intranet ou Internet.

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

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

- Tâches d’impression depuis votre ordinateur
- Impression directe USB
- Copie
- Télécopie reçue
- Impression Web Connect

- La fonction d’enregistrement du journal d’impression sur le réseau prend en charge l’authentification Kerberos et l’authentification NTLMv2. Vous devez configurer le protocole SNTP (serveur de temps du réseau) ou régler correctement la date, l’heure et le fuseau horaire sur le panneau de commande pour l’authentification.
- Vous pouvez régler le type de fichier à TXT ou CSV lorsque vous enregistrez un fichier sur le serveur.

## Renseignements connexes

- Enregistrer le journal d’impression sur le réseau

# Configurer les paramètres d'enregistrement du journal d'impression sur le réseau à l'aide de la Gestion à partir du Web

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

   Par exemple :

   https://192.168.1.2

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

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

4. 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 la navigation à partir de ≡.

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

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

| Option | Description |
|---|---|
| **Chemin d'accès au dossier réseau** | Saisissez le dossier de destination où votre journal d'impression sera enregistré sur le serveur CIFS (exemple: \\NomOrdinateur\DossierPartagé). |
| **Nom de fichier** | Saisissez le nom de fichier à utiliser pour le journal d'impression (avec 32 caractères maximum). |
| **Type fichier** | Sélectionnez l'option **TXT** ou **CSV** pour le type de fichier du journal d'impression. |
| **Origine de l'horloge du journal** | Sélectionnez la source de synchronisation pour le journal d'impression. |
| **Méthode d'authentification** | Sélectionnez la méthode d'authentification requise pour accéder au serveur CIFS : **Auto**, **Kerberos** ou **NTLMv2**. Kerberos est un protocole d'authentification qui permet aux appareils et aux personnes de prouver leur identité en toute sécurité aux serveurs du réseau à l'aide d'une identification unique. NTLMv2 est la méthode d'authentification utilisée par Windows pour se connecter aux serveurs.<br>• **Auto** : Si vous sélectionnez **Auto**, la méthode d'authentification NTLMv2 sera utilisée.<br>• **Kerberos** : Sélectionnez l'option **Kerberos** pour utiliser l'authentification Kerberos exclusivement.<br>• **NTLMv2** : Sélectionnez l'option **NTLMv2** pour utiliser l'authentification NTLMv2 exclusivement. |

| Option | Description |
| --- | --- |
| | • Pour l’authentification **Kerberos** et **NTLMv2**, vous devez également configurer les paramètres **Date et Heure** ou le protocole SNTP (serveur de temps du réseau) et le serveur DNS.<br>• Vous pouvez également configurer la date et l'heure à partir du panneau de commande de l'appareil. |
| **Nom utilisateur** | Saisissez le nom d’utilisateur pour l’authentification (avec 96 caractères maximum).<br>Si le nom d’utilisateur fait partie d’un domaine, entrez-le sous l’un des formats suivants : utilisateur@domaine ou domaine\utilisateur. |
| **Mot de passe** | Saisissez le mot de passe pour l’authentification (avec 32 caractères maximum). |
| **Adresse du serveur Kerberos** (si nécessaire) | Saisissez l’adresse d’hôte du centre de distribution de clés (KDC) (par exemple : kerberos.exemple.com; avec 64 caractères maximum) ou l’adresse IP (par exemple : 192.168.56.189). |
| **Réglage de la détection d'erreurs** | Choisissez la mesure devant être prise lorsque le journal d’impression ne peut pas être enregistré sur le serveur en raison d’une erreur de réseau. |

7. Dans le champ **État de la connexion**, confirmez le plus récent état du journal.

Vous pouvez également confirmer l’état d’erreur à l’écran ACL de votre appareil.

8. Cliquez sur **Envoyer** pour afficher la page **Test d'impression du journal au réseau**.

   Pour tester vos paramètres, cliquez sur **Oui**, puis passez à l’étape suivante.

   Pour sauter le test, cliquez sur **Non**. Vos paramètres seront soumis automatiquement.
9. L’appareil testera vos paramètres.
10. Si vos paramètres sont acceptés, **Test OK** s’affiche à l’écran.

    Si **Erreur de test** s’affiche, vérifiez tous les paramètres, puis cliquez sur **Envoyer** pour afficher à nouveau la page Test.

## Renseignements connexes

- Enregistrer le journal d’impression sur le réseau

# Utiliser le paramètre de détection d'erreur de l'enregistrement du journal d'impression sur le réseau

Utilisez les paramètres de détection d'erreur pour déterminer la mesure à prendre lorsque le journal d'impression ne peut pas être enregistré sur le serveur en raison d'une erreur de réseau.

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

   Par exemple :

   https://192.168.1.2

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

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

4. Dans la barre de navigation de gauche, cliquez sur **Administrateur** > **Enreg journal d'impr sur réseau**.

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

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

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

| Option | Description |
|---|---|
| **Annuler l'impression** | Si vous sélectionnez l'option **Annuler l'impression**, les tâches d'impression sont annulées lorsque le journal d'impression ne peut pas être enregistré sur le serveur.<br>Même si vous sélectionnez l'option **Annuler l'impression**, votre appareil peut imprimer une télécopie reçue. |
| **Ignorer Journal et Impr** | Si vous sélectionnez l'option **Ignorer Journal et Impr**, l'appareil imprime la documentation même si le journal d'impression ne peut pas être enregistré sur le serveur.<br>Lorsque la fonction d'enregistrement du journal d'impression reprend son fonctionnement normal, le journal d'impression est enregistré comme suit :<br>`Id, Type, Job Name, User Name, Date, Time, Print Pages`<br>`1, Print(xxxxxxx), "Document01.doc", "user01", 03/03/20xx, 14:01:32, 52`<br>`2, Print(xxxxxxx), "Document02.doc", "user01", 03/03/20xx, 14:45:30, ?` (a)<br>`3, <Error>, ?, ?, ?, ?, ?` (b)<br>`4, Print(xxxxxxx), "Report01.xls", "user02", 03/03/20xx, 19:30:40, 4`<br>a. Si le journal d'impression ne peut pas être enregistré à la fin de l'impression, le nombre de pages imprimées n'est pas enregistré.<br>b. Si le journal d'impression ne peut pas être enregistré au début et à la fin de l'impression, le journal d'impression de la tâche n'est pas enregistré. Lorsque la fonction reprend son fonctionnement normal, l'erreur est signalée dans le journal d'impression. |

6. Cliquez sur **Envoyer** pour afficher la page **Test d'impression du journal au réseau**.

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

   Pour sauter le test, cliquez sur **Non**. Vos paramètres seront soumis automatiquement.
7. L'appareil testera vos paramètres.
8. Si vos paramètres sont acceptés, **Test OK** s'affiche à l'écran.

   Si **Erreur de test** s'affiche, vérifiez tous les paramètres, puis cliquez sur **Envoyer** pour afficher à nouveau la page Test.

## Renseignements connexes

- Enregistrer le journal d'impression sur le réseau

# Utiliser l’enregistrement du journal d’impression sur le réseau avec le verrouillage sécuritaire des fonctions 3.0

Lorsque la fonction Verrouillage sécuritaire des fonctions 3.0 est activée, les noms des utilisateurs enregistrés pour la copie, la réception de télécopie, l’impression Web Connect et l’impression directe USB sont consignés dans le rapport de la fonction 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 de la fonction d’enregistrement du journal d’impression sur le réseau :

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

## Renseignements connexes

- Enregistrer le journal d’impression sur le réseau

brother

Brother Earth

www.brotherearth.com

CAN-FRE
Version 0