Authentification par carte

Guide de l'administrateur

Août 2017

www.lexmark.com

Contenus

Historique des modifications

Août 2017

- Ajout d'instructions sur la modification de la méthode de connexion.
- Ajout d'instructions sur la désactivation de l'application Quotas d'appareils.
- Ajout de prise en charge pour les langues suivantes : allemand, chinois simplifié, espagnol, finnois, français, italien et portugais brésilien.

Juillet 2016

- Ajout d'instructions sur la configuration de l'application Envoyer un courrier électronique vers soi.

Janvier 2016

- Version initiale du document pour les produits multifonction avec un écran tactile au format tablette.

Aperçu

Authentification par carte est un ensemble d'applications utilisées pour sécuriser l'accès aux imprimantes et à leurs fonctions. Les applications vous permettent de vous connecter à une imprimante manuellement ou en utilisant une carte, puis d'envoyer des e-mails et d'exécuter des travaux d'impression en toute sécurité. Vous pouvez également configurer d'autres paramètres de sécurité dans une application, comme la signature et le chiffrement des e-mails.

Le pack d'authentification par carte comprend les applications suivantes :

- **Client d'authentification par carte** : vous permet de sécuriser l'accès aux imprimantes en invitant les utilisateurs à se connecter à l'aide d'une carte ou d'un nom d'utilisateur et d'un mot de passe. Vous pouvez sécuriser l'accès à l'écran d'accueil de l'imprimante ou à certaines applications et fonctions spécifiques. L'application propose aussi des options d'authentification Kerberos ainsi qu'un ticket Kerberos utilisable pour sécuriser d'autres applications.
- **Pilote de carte** : permet à l'imprimante de communiquer avec une carte prise en charge.
- **Personnalisation de l'affichage** : vous permet de charger des images sur l'imprimante. Vous pouvez utiliser les images pour créer des diaporamas personnalisés ou pour définir le papier peint et l'économiseur d'écran de l'imprimante. Sécurisez cette application en utilisant le client d'authentification par carte pour inviter les utilisateurs à s'authentifier avant de pouvoir accéder à l'écran d'accueil de l'imprimante.
- **E-mail sécurisé** : vous permet de signer et chiffrer les e-mails envoyés à partir de l'imprimante. Cette application annule la fonction e-mail standard de l'imprimante.
- **Sécuriser les travaux d'impression suspendus** : permet aux utilisateurs authentifiés d'afficher et d'exécuter leurs travaux d'impression suspendus.

Ce document fournit des informations sur la configuration, l'utilisation et le dépannage des applications.

Liste de contrôle préparatoire du déploiement

Vérifiez les points suivants :

- ☐ Les éléments suivants sont installés dans l'imprimante :
  - Au moins 512 Go de RAM
  - Un lecteur de cartes et son pilote
- ☐ L'application Quotas d'appareils est désactivée :
  1. Obtenez l'adresse IP de l'imprimante. Effectuez l'une des opérations suivantes :
     - Recherchez l'adresse IP de l'imprimante sur son écran d'accueil.
     - Sur l'écran d'accueil de l'imprimante, appuyez sur **Paramètres** > **Réseau/Ports** > **Aperçu du réseau**.
  2. Ouvrez un navigateur Web, puis saisissez l'adresse IP de l'imprimante.
  3. Cliquez sur **Applications** > **Quotas d'appareils** > **Arrêter**.

Les éléments suivants sont à votre disposition pour configurer le client d'authentification par carte :

- ☐ Certificat d'autorité de certification (fichier .cer)
- ☐ Comptes Active Directory® et Lightweight Directory Access Protocol (LDAP)

  _____
- ☐ Domaine, nom du domaine et contrôleur de domaine Kerberos

  _____
- ☐ Fichier Kerberos (pour plusieurs domaines)

Configuration des paramètres de l’imprimante

Vous devrez peut-être disposer des droits administrateur pour configurer les paramètres de l'imprimante.

Accès au serveur Web incorporé

1. Obtenez l'adresse IP de l'imprimante. Effectuez l'une des opérations suivantes :
   - Recherchez l'adresse IP de l'imprimante sur son écran d'accueil.
   - Sur l'écran d'accueil de l'imprimante, appuyez sur **Paramètres** > **Réseau/Ports** > **Aperçu du réseau**.
2. Ouvrez un navigateur Web, puis saisissez l'adresse IP de l'imprimante.

Réglage du délai d'affichage

Pour empêcher tout accès non autorisé, vous pouvez limiter la durée de connexion d'un utilisateur à l'imprimante sans activité.

1. Dans Embedded Web Server, cliquez sur **Paramètres** > **Périphérique** > **Préférences**.
2. Dans le champ Délai d'affichage, précisez le temps qui s'écoule avant la mise en veille de l'écran et la déconnexion de l'utilisateur. Nous vous recommandons de définir la valeur sur 30 secondes.
3. Cliquez sur **Enregistrer**.

Installation manuelle de certificats

Remarque : Pour télécharger automatiquement le certificat CA, voir « Installation automatique de certificats » à la page 8.

Avant de configurer les paramètres de Kerberos ou du contrôleur de domaine, installez le certificat CA utilisé pour la validation du contrôleur de domaine. Si vous envisagez de valider le certificat du contrôleur de domaine au moyen de la validation en chaîne, installez la totalité de la chaîne de certificats. Chaque certificat doit se trouver dans un fichier PEM (.cer) distinct.

1. Dans Embedded Web Server, cliquez sur **Paramètres** > **Sécurité** > **Gestion des certificats**.
2. Dans la section Gérer les certificats CA, cliquez sur **Télécharger CA**, puis accédez au format PEM (.cer).

   Exemple de certificat :

   ```
   -----BEGIN CERTIFICATE-----
   MIIE1jCCA76gAwIBAgIQY6sV0KL3tIhBtlr4gHG85zANBgkqhkiG9w0BAQUFADBs
   …
   l3DTbPe0mnIbTq0iWqKEaVne1vvaDt52iSpEQyevwgUcHD16rFy+sOnCaQ==
   -----END CERTIFICATE-----
   ```

3. Cliquez sur **Enregistrer**.

Installation automatique de certificats

1 Dans Embedded Web Server, cliquez sur **Paramètres** > **Sécurité** > **Gestion des certificats** > **Configurer la mise à jour automatique des certificats**.

2 Si vous êtes invité à joindre un domaine Active Directory, cliquez sur **Joindre le domaine**, puis saisissez les informations de domaine.

Remarque : Assurez-vous que le domaine Active Directory correspond à la zone Kerberos ou au domaine utilisé dans les paramètres de la carte à puce. Pour plus d'informations, reportez-vous à la section « Configuration des paramètres de la carte à puce » à la page 14.

3 Sélectionnez **Activer la mise à jour automatique**.

Remarque : Si vous souhaitez installer le certificat CA sans attendre l'heure d'exécution planifiée, sélectionnez **Extraire immédiatement**.

4 Cliquez sur **Enregistrer**.

Configuration des paramètres TCP/IP

1 Dans Embedded Web Server, cliquez sur **Paramètres** > **Réseau/Ports** > **TCP/IP**.

2 Effectuez l'une des opérations suivantes :

- Si vous utilisez une adresse IP statique, saisissez l'adresse du serveur DNS. Si un serveur DNS de secours est disponible, tapez l'adresse du serveur DNS de secours.
- Si l'imprimante se trouve dans un domaine différent, saisissez les autres domaines dans le champ Ordre de recherche de domaine. Si vous choisissez plusieurs domaines, séparez-les par des virgules.

Remarque : Utilisez le nom de domaine attribué aux stations de travail utilisateur.

3 Cliquez sur **Enregistrer**.

Définition de la date et l'heure

Lorsque vous utilisez l'authentification Kerberos, assurez-vous que la différence horaire entre l'imprimante et le contrôleur de domaine ne dépasse pas cinq minutes. Vous pouvez mettre à jour les paramètres de date et d'heure manuellement ou utiliser le protocole NTP (Network Time Protocol) pour synchroniser automatiquement l'heure avec le contrôleur de domaine.

1 Sur Embedded Web Server, cliquez sur **Paramètres** > **Périphérique** > **Préférences** > **Date et heure**.

Configuration manuelle

Remarque : La configuration de la date et de l'heure permet de désactiver manuellement le protocole NTP.

a Dans le champ « Définir heure/date manuellement » de la section Configurer, saisissez la date et l'heure appropriées.

b Sélectionnez le format de date, le format d'heure et le fuseau horaire.

Remarque : Si vous sélectionnez **(GMT+utilisateur) Perso**, spécifiez les valeurs de décalage UTC (GMT) et de l'heure d'été.

Configuration de NTP

a Dans la section Protocole NTP, sélectionnez **Activer NTP**, puis saisissez le nom d'hôte ou l'adresse IP du serveur NTP.

b Si le serveur NTP exige une authentification, dans le menu Activer l'authentification, sélectionnez **Clé MD5**.

c En fonction de votre modèle d'imprimante, saisissez l'ID de clé et le mot de passe ou accédez au fichier contenant les informations d'authentification NTP.

2 Cliquez sur **Enregistrer**.

Configuration des paramètres du compte réseau LDAP

Un compte réseau LDAP est nécessaire pour envoyer des e-mails chiffrés. Les certificats de chiffrement pour les destinataires sont ajoutés et configurés à partir du serveur LDAP. Pour plus d'informations, contactez votre administrateur système.

Remarque : Un compte réseau Kerberos est nécessaire pour créer un compte réseau LDAP + GSSAPI.

1 Dans Embedded Web Server, cliquez sur **Paramètres** > **Sécurité** > **Méthodes de connexion**.

2 Dans la section Comptes réseau, cliquez sur **Ajouter une méthode de connexion** > **LDAP**.

3 Sélectionnez **LDAP** ou **LDAP + GSSAPI**.

4 Dans la section Informations générales, effectuez les configurations suivantes :

- **Configuration de nom** : un nom unique pour le compte réseau LDAP.
- **Adresse du serveur**

  Remarque : Vérifiez que l'adresse est identique à celle du contrôleur de domaine du Client d'authentification par carte à puce ou à l'adresse KDC dans le fichier de configuration Kerberos.
- **Port de serveur** : si vous utilisez SSL, utilisez le port **636**. Sinon, utilisez le port **389**.

5 Dans la section Informations d'identification du périphérique, décochez **Liaison LDAP anonyme**, puis saisissez les informations d'authentification utilisées pour la connexion au serveur LDAP.

6 Si le serveur LDAP nécessite SSL, dans la section Options avancées, définissez Utiliser SSL/TLS sur **SSL/TLS**.

7 Dans la section Configuration du carnet d'adresses, sélectionnez **Utiliser les informations d'identification de l'utilisateur**.

8 Cliquez sur **Enreg. et vérifier**.

Sécurisation de l'accès à l'imprimante

Sécurisation de l'accès à l'écran d'accueil

Les utilisateurs doivent s'authentifier avant de pouvoir accéder à l'écran d'accueil de l'imprimante.

Remarque : Avant de commencer, assurez-vous que l'application Personnalisation de l'affichage est activée dans votre imprimante. Pour plus d'informations, reportez-vous au *Guide de l'administrateur de la personnalisation de l'affichage*.

1. Dans Embedded Web Server, cliquez sur **Paramètres** > **Sécurité** > **Méthodes de connexion**.
2. Dans la section Public, cliquez sur **Gérer autorisations**.
3. Développez **Applications**, décochez **Diaporama**, **Modifier le papier peint** et **Economiseur d'écran**, puis cliquez sur **Enregistrer**.
4. Dans la section Méthodes de connexion supplémentaires, cliquez sur **Gérer autorisations** en regard de Carte à puce.
5. Sélectionnez le groupe dont vous souhaitez gérer les autorisations.

   Remarque : Le groupe Tous les utilisateurs est créé par défaut. Plusieurs noms de groupe s'affichent lorsque vous définissez des groupes Active Directory existants dans le champ Liste des autorisations de groupe. Pour plus d'informations, reportez-vous à la section « Configuration des paramètres avancés » à la page 15.
6. Développez **Applications**, puis sélectionnez **Diaporama**, **Modifier le papier peint** et **Economiseur d'écran**.
7. Cliquez sur **Enregistrer**.

Sécurisation de l'accès à des applications et des fonctions déterminées

Les utilisateurs doivent s'authentifier avant d'accéder à une application ou une fonction intégrée de l'imprimante.

1. Dans Embedded Web Server, cliquez sur **Paramètres** > **Sécurité** > **Méthodes de connexion**.
2. Dans la section Public, cliquez sur **Gérer autorisations**.
3. Limitez l'accès public aux applications ou aux fonctions que vous souhaitez sécuriser. Effectuez l'une des opérations suivantes :
   - Pour E-mail sécurisé, développez **Accès aux fonctions**, décochez **Fonction e-mail**, puis cliquez sur **Enregistrer**.
   - Pour Sécuriser les travaux d'impression suspendus, développez **Applications**, décochez **Sécuriser les travaux d'impression suspendus**, puis cliquez sur **Enregistrer**.
   - Pour d'autres applications ou fonctions, développez une ou plusieurs catégories, décochez l'application ou la fonction, puis cliquez sur **Enregistrer**.
4. Dans la section Méthodes de connexion supplémentaires, cliquez sur **Gérer les autorisations** en regard de Carte.
5. Sélectionnez le groupe dont vous souhaitez gérer les permissions.

   Remarque : Le groupe Tous les utilisateurs est créé par défaut. Plusieurs noms de groupe s'affichent lorsque vous définissez des groupes Active Directory existants dans le champ Liste des autorisations de groupe. Pour plus d'informations, reportez-vous à la section « Configuration des paramètres avancés » à la page 15.

6. Sélectionnez les applications ou fonctions auxquelles vous souhaitez que les utilisateurs authentifiés puissent accéder. Effectuez l'une des opérations suivantes :
   - Pour E-mail sécurisé, développez **Accès aux fonctions**, puis sélectionnez **Fonction e-mail**.
   - Pour Sécuriser les travaux d'impression suspendus, développez **Applications**, puis sélectionnez **Sécuriser les travaux d'impression suspendus**.
   - Pour d'autres applications ou fonctions, développez une ou plusieurs catégories, puis sélectionnez l'application ou la fonction.
7. Cliquez sur **Enregistrer**.

Affichage des applications ou fonctions sécurisées sur l'écran d'accueil

Par défaut, les applications ou fonctions sécurisées sont masquées dans l'écran d'accueil de l'imprimante.

1. Dans Embedded Web Server, cliquez sur **Paramètres** > **Sécurité** > **Divers**.
2. Dans le menu Fonctions protégées, sélectionnez **Afficher**.
3. Cliquez sur **Enregistrer**.

Configuration des paramètres e-mail de l’imprimante

Cette application annule la fonction e-mail de l'imprimante.

Configuration des paramètres de code SMTP

1. Dans Embedded Web Server, cliquez sur **Paramètres** > **E-mail** > **Configuration de la messagerie**.
2. Configurez les éléments suivants :
   - **Passerelle SMTP primaire** : l'adresse IP ou le nom d'hôte du serveur utilisé pour l'envoi d'e-mails.

     Remarque : Pour l'authentification Kerberos, utilisez le nom d'hôte.
   - **Port de la passerelle SMTP primaire**
   - **Passerelle SMTP secondaire** : l'adresse IP ou le nom d'hôte du serveur SMTP secondaire ou de sauvegarde.
   - **Port du serveur SMTP secondaire**
   - **Délai SMTP**
   - **Utiliser SSL/TLS**
   - **Adresse de réponse**
   - **Authentification du serveur SMTP**

     Remarques :

     - Si **Kerberos 5** est sélectionné, saisissez le domaine Kerberos.
     - Si **NTLM** est sélectionné, saisissez le domaine NTLM.
     - Si le serveur SMTP requiert une authentification, mais ne prend pas en charge Kerberos, dans le champ Adresse de réponse, saisissez l'adresse IP ou le nom d'hôte.

- **E-mail du périphérique** : les informations d'identification du périphérique sont requises pour les e-mails du périphérique.

  Remarque : Si **Utilisation des informations d'identification SMTP du périphérique** est sélectionné, saisissez les informations d'authentification.
- **E-mail de l'utilisateur** : les informations d'identification de l'utilisateur sont requises pour les e-mails de l'utilisateur.

  Remarque : Si vous utilisez l'authentification Kerberos, sélectionnez **Utiliser l'ID utilisateur et le mot de passe de la session**.

3 Cliquez sur **Enregistrer**.

Configuration des paramètres d'e-mail et de numérisation par défaut

1 Dans Embedded Web Server, cliquez sur **Paramètres** > **E-mail** > **Paramètres d'e-mail par défaut**.

2 Configurez les paramètres.

3 Si nécessaire, réglez les paramètres de numérisation et de contrôle administratif avancés.

4 Cliquez sur **Enregistrer**.

Configuration de Envoyer un courrier électronique vers soi

Envoyer un courrier électronique vers soi permet aux utilisateurs d'envoyer une copie de l'e-mail à leur adresse. Pour plus d'informations, reportez-vous au *Guide de l'administrateur d'Envoyer un courrier électronique vers soi*.

Selon votre modèle d'imprimante, effectuez l'une des opérations suivantes :

Pour la version intégrée de l'application

1 Dans Embedded Web Server, cliquez sur **Paramètres** > **E-mail** > **Paramètres d'e-mail par défaut** > **Contrôles admin**.

2 Sélectionnez **Limiter les destinataires d'e-mail**.

3 Cliquez sur **Enregistrer**.

Pour l'application Embedded Solutions Framework (eSF)

1 Accédez à la page de configuration de l'application à partir d'Embedded Web Server :

Applications > **Envoyer un courrier électronique vers soi** > **Configurer**

2 Sélectionnez **Activer**.

3 Cliquez sur **Appliquer**.

Configuration des applications

Configuration du client d'authentification par carte

Vous devrez peut-être disposer des droits administrateur pour configurer l'application.

Configuration des paramètres de l'écran de connexion

Utilisez les paramètres de l'écran de connexion pour définir la méthode de connexion des utilisateurs à l'imprimante.

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server :

   Applications > **Client d'authentification par carte à puce** > **Configurer**

2. Dans la section Ecran de connexion, sélectionnez le type de connexion.
3. Dans le menu Mode de validation de l'utilisateur, sélectionnez la méthode de validation des certificats utilisateur.
   - **Active Directory** : le certificat utilisateur de la carte à puce est validé à l'aide de l'authentification Kerberos. Ce paramètre peut nécessiter des recherches LDAP.
   - **Active Directory avec accès invité** : les utilisateurs possédant des cartes à puce, mais qui ne sont pas dans l'annuaire Active Directory, peuvent accéder à certaines fonctions de l'imprimante. Un serveur Online Certificate Status Protocol (OCSP) correctement configuré est requis. En cas d'échec de l'authentification Active Directory, l'application interroge le serveur OCSP.
   - **Code Pin uniquement** : les utilisateurs peuvent accéder uniquement aux applications ou fonctions qui ne nécessitent pas d'authentification Kerberos.
4. Dans le menu Valider la carte à puce, sélectionnez la méthode d'authentification des utilisateurs après avoir appuyé sur une carte à puce.
5. Si nécessaire, autorisez les utilisateurs à modifier la méthode de connexion.
6. Cliquez sur **Appliquer**.

Configuration des paramètres de connexion manuelle

Pour la connexion manuelle, l'imprimante utilise le domaine par défaut spécifié dans le fichier de configuration Kerberos. Si vous utilisez un domaine différent, spécifiez le nom de domaine dans les paramètres de connexion manuelle.

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server :

   Applications > **Client d'authentification par carte à puce** > **Configurer**

2. Dans le champ Domaines de connexion manuelle de la section Configuration de la connexion manuelle, saisissez un ou plusieurs domaines.
3. Cliquez sur **Appliquer**.

Configuration des paramètres de la carte à puce

Remarque : Assurez-vous que la connexion réseau entre l'imprimante et le serveur d'authentification est correctement configurée. Pour plus d'informations, contactez votre administrateur système.

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server :

   Applications > **Client d'authentification par carte à puce** > **Configurer**

2. Dans le menu Informations Kerberos de la section Configuration de la carte à puce, sélectionnez l'un des éléments suivants :
   - **Utiliser le fichier de configuration Kerberos du périphérique** : un fichier de configuration Kerberos doit être installé manuellement sur l'imprimante. Procédez comme suit :
     a. Dans Embedded Web Server, cliquez sur **Paramètres** > **Sécurité** > **Méthodes de connexion**.
     b. Dans la section Comptes réseau, cliquez sur **Ajouter une méthode de connexion** > **Kerberos**.
     c. Dans la section Importer le fichier Kerberos, accédez au fichier krb5.conf approprié.
     d. Si votre réseau n'utilise pas la recherche DNS inversée, dans la section Autres paramètres, sélectionnez **Désactiver les recherches IP inversées**.
     e. Cliquez sur **Enreg. et vérifier**.
   - **Utiliser la configuration Kerberos simple** : un fichier Kerberos est créé automatiquement sur l'imprimante. Indiquez les éléments suivants :
     - **Zone** : la zone doit être saisie en majuscules.
     - **Contrôleur de domaine** : utilisez des virgules pour séparer plusieurs valeurs. Les contrôleurs de domaine sont validés dans l'ordre de la liste.
     - **Domaine** : spécifiez le domaine qui doit être mappé à la zone Kerberos spécifiée dans le champ Zone. Si vous choisissez plusieurs domaines, séparez-les par des virgules.

       Remarque : Le domaine est sensible à la casse.
     - **Délai** : saisissez une valeur comprise entre 3 et 30 secondes.

3. Dans le menu Validation du contrôleur de domaine, sélectionnez la méthode de validation du certificat du contrôleur de domaine.

   Remarque : Avant de configurer ce paramètre, assurez-vous que les certificats appropriés sont installés sur l'imprimante. Pour plus d'informations, reportez-vous à la section « Installation manuelle de certificats » à la page 7.
   - **Utiliser la validation par certificat de périphérique** : le certificat CA installé sur l'imprimante est utilisé.
   - **Utilisation de la validation en chaîne du périphérique** : l'intégralité de la chaîne de certificats installée sur l'imprimante est utilisée.
   - **Utiliser la validation OCSP** : le serveur OCSP est utilisé. L'ensemble de la chaîne de certificats doit être installé sur l'imprimante. Dans la section Online Certificate Status Protocol (OCSP), configurez ce qui suit :
     - **URL du répondeur** : spécifiez l'adresse IP ou le nom d'hôte du répondeur/répéteur OCSP, ainsi que le numéro de port utilisé. Si vous choisissez plusieurs valeurs, séparez-les par des virgules.
       Par exemple, **`http://x:y`**, où ***x*** est l'adresse IP ou le nom d'hôte et ***y*** est le numéro de port.
     - **Certificat de répondeur** : le certificat de répondeur X.509 est utilisé.
     - **Délai du répondeur** : saisissez une valeur comprise entre 5 et 30 secondes.
     - **Autoriser état inconnu**: les utilisateurs peuvent se connecter même si l'état d'un ou plusieurs certificats est inconnu.

4. Cliquez sur **Appliquer**.

Configuration des paramètres avancés

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server :

   Applications > **Client d'authentification par carte à puce** > **Configurer**

2. Dans la section Paramètres avancés, sélectionnez un ID utilisateur de session.

   Remarque : Certaines applications, telles que Sécuriser les travaux d'impression suspendus et E-mail sécurisé, requièrent une valeur pour l'ID utilisateur de la session.

3. Dans le menu Adresse à partir de l'e-mail, sélectionnez l'emplacement où l'imprimante récupère les adresses e-mail de l'utilisateur.

4. Si nécessaire, sélectionnez **Attendre les informations de l'utilisateur** pour récupérer toutes les informations utilisateur avant d' autoriser l'utilisateur à accéder à l'écran d'accueil ou à l'application sécurisée.

   Si les paramètres suivants sont définis sur Recherche LDAP, sélectionnez cette option.

   - ID utilisateur de la session
   - Origine de l'adresse e-mail

   Si les paramètres suivants ne sont pas vides, sélectionnez cette option.

   - Autres attributs utilisateur
   - Liste des autorisations de groupe

   Remarque : Si vous utilisez la connexion manuelle pour E-mail sécurisé, sélectionnez cette option pour stocker l'adresse e-mail de l'utilisateur dans la session de connexion. Pour permettre aux utilisateurs de la connexion manuelle d'envoyer un e-mail à eux-mêmes, activez « M'envoyer une copie » dans les paramètres de courrier électronique de l'imprimante.

5. Si nécessaire, sélectionnez **Utiliser SSL pour les informations utilisateur** pour récupérer les informations utilisateur à partir du contrôleur de domaine à l'aide d'une connexion SSL.

6. Si nécessaire, dans le champ Autres attributs utilisateur, saisissez les autres attributs LDAP qui doivent être ajoutés à la session. Si vous choisissez plusieurs valeurs, séparez-les par des virgules.

7. Dans la liste des autorisations de groupe, saisissez les groupes Active Directory qui peuvent accéder aux applications ou fonctions. Si vous choisissez plusieurs valeurs, séparez-les par des virgules.

   Remarque : Les groupes doivent être sur le serveur LDAP.

8. Si DNS n'est pas activé sur votre réseau, téléchargez un fichier d'hôtes.

   Saisissez les mappages dans le fichier texte dans le format ***xy***, où ***x*** est l'adresse IP et ***y*** le nom d'hôte. Vous pouvez attribuer plusieurs noms d'hôte à une adresse IP. Par exemple, **`255.255.255.255 Nom d'hôte1 Nom d'hôte2 Nom d'hôte3`**.

   Vous ne pouvez pas attribuer plusieurs adresses IP à un nom d'hôte. Pour attribuer des adresses IP à des groupes de noms d'hôtes, saisissez chaque adresse IP et ses noms d'hôte associés sur une ligne distincte du fichier texte.

   Par exemple :

   ```
   123.123.123.123 Nom d'hôte1 Nom d'hôte2
   456.456.456.456 Nom d'hôte3
   ```

9. Cliquez sur **Appliquer**.

Configuration de Sécuriser l'email

Vous devrez peut-être disposer des droits administrateur pour configurer l'application.

Configuration des paramètres d'e-mail sécurisé

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server :

   Applications > **E-mail sécurisé** > **Configurer**

2. Configurez les paramètres.

   Remarques :

   - Pour signer numériquement un e-mail, vous devez posséder un certificat de signature numérique valide et vous connecter à l'aide d'une carte à puce. Les certificats de signature sont disponibles uniquement à partir de la carte à puce. Pour plus d'informations, contactez votre administrateur système.
   - Pour recevoir un e-mail chiffré, le destinataire doit apparaître dans le carnet d'adresses du serveur LDAP et disposer d'un certificat de chiffrement valide. Pour plus d'informations, reportez-vous à la section « Configuration des paramètres du compte réseau LDAP » à la page 9.
   - Pour appliquer une marque de sécurité à un e-mail, activez ce paramètre, puis saisissez le texte que vous souhaitez utiliser.
   - Pour plus d'informations sur chaque paramètre, reportez-vous à l'aide contextuelle.

3. Cliquez sur **Appliquer**.

Configuration de Sécuriser les travaux d'impression suspendus

Restreindre l'affichage des travaux suspendus pour les utilisateurs non authentifiés

L'application intégrée de travaux suspendus peut être utilisée pour afficher tous les travaux suspendus dans l'imprimante. Après avoir configuré l'option Sécuriser les travaux d'impression suspendus, supprimez l'icône Travaux suspendus de l'écran d'accueil de l'imprimante.

1. Dans Embedded Web Server, cliquez sur **Paramètres** > **Périphérique** > **Icônes visibles de l'écran d'accueil**.
2. Décochez **Travaux suspendus**.
3. Cliquez sur **Enregistrer**.

Configuration des paramètres Sécuriser les travaux d'impression suspendus

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server :

   Applications > **Sécuriser les travaux d'impression suspendus** > **Configurer**

2. Dans la section Options de diffusion, configurez les paramètres.
   - **Méthode de diffusion** : indique comment les utilisateurs impriment leurs travaux suspendus.
   - **Afficher les travaux d'impression triés par** : indique comment les travaux d'impression sont répertoriés sur l'écran.
3. Cliquez sur **Appliquer**.

Conversion des travaux d'impression pour sécuriser les travaux d'impression suspendus

1. Dans Embedded Web Server, cliquez sur **Paramètres** > **Sécurité** > **Configuration des impressions confidentielles**.
2. Sélectionnez **Conserver tous les travaux suspendus**.
3. Cliquez sur **Enregistrer**.

Importation ou exportation d'un fichier de configuration

Remarque : L'importation de fichiers de configuration écrase les configurations d'applications existantes.

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server. Effectuez l'une des opérations suivantes :
   - Cliquez sur **Applications** > **Client d'authentification par carte** > **Configurer**
   - Cliquez sur **Applications** > **E-mail sécurisé** > **Configurer**
   - Cliquez sur **Applications** > **Sécuriser les travaux d'impression suspendus** > **Configurer**
2. Cliquez sur **Importer** ou sur **Exporter**.

Utilisation des applications

Sécuriser l'email

Envoi d'un e-mail chiffré à signature numérique

Remarques :

- Lorsque vous utilisez la connexion manuelle, configurez les paramètres d'authentification du Client d'authentification par carte à puce pour récupérer toutes les informations utilisateur. Pour obtenir plus d'informations, reportez-vous au *Guide de l'administrateur de l'authentification par carte à puce*.
- Pour envoyer un e-mail, assurez-vous que vous disposez d'une adresse e-mail valide attribuée à votre compte.

1. Connectez-vous à l'imprimante
2. Sur l'écran d'accueil de l'imprimante, appuyez sur l'icône de l'application.
3. Chargez un document dans le tiroir du DAA ou placez-le sur la vitre du scanner.
4. Saisissez l'adresse électronique du destinataire. S'il y a plusieurs adresses e-mail, séparez-les par des virgules.
5. Si nécessaire, configurez d'autres paramètres d'e-mail et de numérisation.
6. Appuyez sur **Envoyer**.
7. Signez numériquement ou chiffrez l'e-mail

   Remarque : Pour signer numériquement un e-mail, vous devez posséder un certificat de signature numérique valide et vous connecter à l'aide d'une carte à puce. Les certificats de signature sont disponibles uniquement à partir de la carte à puce. Pour plus d'informations, contactez votre administrateur système.
8. Si nécessaire, sélectionnez une option de sécurité.
9. Appuyez sur **Envoyer**.
10. Si une erreur de chiffrement se produit, procédez comme suit :
    - Pour envoyer un e-mail chiffré uniquement aux destinataires possédant des certificat de chiffrement, sélectionnez **Envoyer des e-mails chiffrés**.
    - Pour envoyer un e-mail non chiffré à tous les destinataires, sélectionnez **Envoyer un e-mail non chiffré**.
11. Appuyez sur **Envoyer**.

Sécuriser les travaux d'impression suspendus

Impression des tâches suspendues

Remarques :

- Assurez-vous de convertir les travaux d'impression standard pour sécuriser les travaux d'impression suspendus. Pour plus d'informations, reportez-vous à la section « Conversion des travaux d'impression pour sécuriser les travaux d'impression suspendus » à la page 17.
- Assurez-vous que la fonction Imprimer et suspendre est prise en charge par le pilote d'impression avant de l'utiliser. Pour plus d'informations, reportez-vous à l'*Aide du pilote d'impression*. Vous pouvez télécharger le pilote d'impression universel Lexmark pour Windows et le pilote d'impression pour Macintosh à l'adresse **www.lexmark.com**.

1. Lorsqu'un document est ouvert, cliquez sur **Fichier** > **Imprimer**.
2. Sélectionner une imprimante.

   Remarque : Si nécessaire, configurez les paramètres d'impression.
3. Si nécessaire, utilisez la fonction Imprimer et suspendre.
   a. Sélectionnez la fonction Imprimer et suspendre.
      - Pour les utilisateurs Windows, cliquez sur **Propriétés**, **Préférences**, **Options** ou **Configuration**, puis sur **Imprimer et suspendre**.
      - Pour les utilisateurs Macintosh, sélectionnez **Imprimer et suspendre** dans le menu des options.

   b. Sélectionnez le type de tâche d'impression.
      - **Différer** : envoie et stocke les travaux d'impression dans la mémoire de l'imprimante pour les imprimer ultérieurement.
      - **Vérifier** : imprime la première copie d'un travail d'impression comprenant plusieurs copies pour vérification. Les copies restantes sont mises en suspens jusqu'à ce qu'elles soient imprimées ou annulées.
      - **Répéter** : imprime immédiatement le travail d'impression et stocke une copie dans la mémoire de l'imprimante pour permettre l'impression ultérieure d'autres copies.

      Remarque : L'application Sécuriser les travaux d'impression suspendus ne prend pas en charge les travaux d'impression confidentiels.

   c. Saisissez le nom d'utilisateur du répertoire LDAP associé à la tâche d'impression.
4. Cliquez sur **OK** ou **Imprimer**.
5. Sur l'écran d'accueil de l'imprimante, connectez-vous à votre compte, puis appuyez sur l'icône de l'application.

   Remarques :

   - Assurez-vous d'utiliser le même compte pour la connexion à l'imprimante et pour l'envoi de travaux d'impression.
   - Selon la manière dont l'application est configurée, toutes les tâches de votre file d'attente d'impression peuvent s'imprimer automatiquement quand vous touchez l'icône de l'application. Pour plus d'informations, reportez-vous à la section « Configuration des paramètres Sécuriser les travaux d'impression suspendus » à la page 17.

6 Si vous y êtes invité, entrez vos informations d'authentification.

7 Sélectionnez le ou les travaux que vous souhaitez imprimer, puis précisez le nombre d’exemplaires à imprimer.

8 Appuyez sur **Imprimer**.

Dépannage

Erreur d'application

Essayez les solutions suivantes :

Vérifiez le journal de diagnostic

1. Ouvrez un navigateur Web, puis saisissez ***IP*/se**, où ***IP*** est l'adresse IP de l'imprimante.
2. Cliquez sur **Solutions intégrées**, puis procédez comme suit :
   a. Effacez le fichier journal.
   b. Définissez le niveau de journalisation sur **Oui**.
   c. Générez le fichier journal.
3. Analysez le journal, puis résolvez le problème.

   Remarque : Une fois le problème résolu, définissez le niveau de journalisation sur **Non**.

Contactez votre représentant Lexmark

Problèmes de connexion

Impossible de détecter le lecteur de carte ou la carte à puce

Essayez les solutions suivantes :

Vérifiez que le lecteur de carte est correctement connecté à l'imprimante

Assurez-vous que le lecteur de cartes et la carte à puce sont compatibles

Vérifiez que le lecteur de carte est bien pris en charge

Pour obtenir la liste des lecteurs de cartes pris en charge, consultez le fichier *Readme*.

Assurez-vous que le pilote de lecteur de carte approprié est installé sur l'imprimante

Contactez votre représentant Lexmark

L'utilisateur est bloqué

Essayez les solutions suivantes :

Augmentez le nombre d'échecs de connexion autorisé et le délai de verrouillage.

Remarque : Cette solution n'est applicable que sur certains modèles d'imprimante.

1. Dans Embedded Web Server, cliquez sur **Paramètres** > **Sécurité** > **Restrictions de connexion**.
2. Augmentez le nombre d'échecs de connexion autorisé et le délai de verrouillage.
3. Cliquez sur **Enregistrer**.

   Remarque : Les nouveaux paramètres prendront effet à l'expiration du délai de verrouillage.

Réinitialiser ou remplacer la carte à puce

Impossible de valider le code PIN

Essayez les solutions suivantes :

Vérifiez que le code PIN saisi est correct.

Contactez l'administrateur du système.

Impossible de se connecter manuellement.

Essayez les solutions suivantes :

Vérifiez que le domaine spécifié dans la configuration Kerberos est correct

Spécifiez les domaines dans les paramètres de connexion manuelle

Pour plus d'informations, reportez-vous à la section « Configuration des paramètres de connexion manuelle » à la page 13.

Contactez l'administrateur du système.

L'écran d'accueil de l'imprimante ne se verrouille pas

Essayez les solutions suivantes :

Vérifiez que la Personnalisation de l'affichage est activée.

Pour plus d'informations, reportez-vous au *Guide de l'administrateur de la personnalisation de l'affichage*.

Sécuriser de l'accès à l'écran d'accueil

Pour plus d'informations, reportez-vous à la section « Sécurisation de l'accès à l'écran d'accueil » à la page 9.

Problèmes d'authentification

Echec de l'authentification Kerberos

Essayez les solutions suivantes :

Vérifiez le journal de diagnostic

1. Ouvrez un navigateur Web, puis saisissez ***IP*/se**, où ***IP*** est l'adresse IP de l'imprimante.
2. Cliquez sur **Solutions intégrées**, puis procédez comme suit :
   a. Effacez le fichier journal.
   b. Définissez le niveau de journalisation sur **Oui**.
   c. Générez le fichier journal.
3. Analysez le journal, puis résolvez le problème.

   Remarque : Après avoir analysé le journal, définissez le niveau de journalisation sur **Non**.

Assurez-vous que le fichier de configuration approprié est installé sur l'imprimante

- Si vous utilisez la configuration Kerberos simple pour créer le fichier de configuration Kerberos, procédez comme suit :
  1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server : **Applications** > **Client d'authentification par carte à puce** > **Configurer**
  2. Dans la section de configuration de Kerberos simple, vérifiez que le domaine, le contrôleur de domaine, le domaine et les valeurs de délai sont corrects.
- Si vous utilisez le fichier de configuration Kerberos du périphérique, procédez comme suit :
  1. Dans Embedded Web Server, cliquez sur **Paramètres** > **Sécurité** > **Méthodes de connexion**.
  2. Dans la section Comptes réseau, cliquez sur **Kerberos** > **Afficher le fichier**.
  3. Si le fichier de configuration Kerberos n'est pas installé, dans la section Importer le fichier Kerberos, accédez au fichier krb5.conf approprié.
  4. Cliquez sur **Enreg. et vérifier**.

Assurez-vous que le contenu et le format du fichier de configuration sont corrects

- Si vous utilisez la configuration Kerberos simple, modifiez ses paramètres.
- Si vous utilisez le fichier de configuration Kerberos du périphérique, modifiez-le et réinstallez-le.

Vérifier que la zone Kerberos est en majuscules

- Si vous utilisez la configuration Kerberos simple, procédez comme suit :
  1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server : **Applications** > **Client d'authentification par carte à puce** > **Configurer**
  2. Dans la section Configuration Kerberos simple, vérifiez que la zone est correcte et qu'elle a été saisie en majuscules.
  3. Cliquez sur **Appliquer**.

- Si vous utilisez le fichier de configuration Kerberos du périphérique, procédez comme suit :
  1. Dans Embedded Web Server, cliquez sur **Paramètres** > **Sécurité** > **Méthodes de connexion**.
  2. Dans la section Comptes réseau, cliquez sur **Kerberos** > **Afficher le fichier**.
  3. Vérifiez que les zones du fichier de configuration sont en majuscules.

Spécifiez le domaine du système d'exploitation Microsoft® Windows®

- Si vous utilisez la configuration Kerberos simple, procédez comme suit :
  1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server : **Applications** > **Client d'authentification par carte à puce** > **Configurer**
  2. Dans le champ Domaine de la section Configuration Kerberos simple, ajoutez le domaine Windows. Par exemple, si la valeur du champ Domaine est **`NomDomaine,.NomDomaine`** et le domaine Windows est **`x.y.z`**, remplacez la valeur du le champ Domaine par **`NomDomaine,.NomDomaine,x.y.z`**.

     Remarque : Le domaine est sensible à la casse.
  3. Cliquez sur **Appliquer**.
- Si vous utilisez le fichier de configuration Kerberos, ajoutez une entrée à la section **`domaine_zone`** du fichier. Saisissez la zone du domaine Windows en majuscules, puis réinstallez le fichier sur l'imprimante.

Contactez votre représentant Lexmark

Impossible de générer ou de lire les informations de certificat depuis la carte à puce

Essayez les solutions suivantes :

Assurez-vous que les informations du certificat sur la carte à puce sont correctes.

Contactez votre représentant Lexmark

Impossible de valider le contrôleur de domaine

Essayez les solutions suivantes :

Assurez-vous que la zone, le contrôleur de domaine et le domaine dans le fichier de configuration Kerberos sont corrects

- Si vous utilisez la configuration Kerberos simple, procédez comme suit :
  1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server : **Applications** > **Client d'authentification par carte à puce** > **Configurer**
  2. Dans la section de configuration de Kerberos simple, vérifiez que la zone, le contrôleur de domaine et le domaine sont corrects.

- Si vous utilisez le fichier de configuration Kerberos du périphérique, procédez comme suit :
  1. Dans Embedded Web Server, cliquez sur **Paramètres** > **Sécurité** > **Méthodes de connexion**.
  2. Dans la section Comptes réseau, cliquez sur **Kerberos** > **Afficher le fichier**.
  3. Assurez-vous que la zone, le contrôleur de domaine et le domaine sont corrects.

Augmentez la valeur du délai d'attente du contrôleur de domaine.

- Si vous utilisez la configuration Kerberos simple, procédez comme suit :
  1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server :
     Applications > **Client d'authentification par carte à puce** > **Configurer**
  2. Dans la section Configuration Kerberos simple, dans le champ Délai, saisissez une valeur comprise entre 3 et 30 secondes.
  3. Cliquez sur **Appliquer**.
- Si vous utilisez le fichier de configuration Kerberos du périphérique, saisissez une valeur comprise entre 3 et 30 secondes. Quand vous avez terminé, réinstallez le fichier sur l'imprimante. Pour plus d'informations sur la configuration des paramètres de carte à puce, reportez-vous à la section « Configuration des paramètres de la carte à puce » à la page 14.

Vérifiez que le contrôleur de domaine est disponible

Si vous choisissez plusieurs valeurs, séparez-les par des virgules. Les contrôleurs de domaine sont validés dans l'ordre de la liste.

Vérifiez que le port 88 n'est pas bloqué entre l'imprimante et le contrôleur de domaine

Impossible de valider le certificat du contrôleur de domaine

Essayez les solutions suivantes :

Assurez-vous que les certificats installés sur l'imprimante sont corrects

Pour plus d'informations, reportez-vous à la section « Installation manuelle de certificats » à la page 7.

Vérifiez que la méthode de validation du contrôleur de domaine est correctement configurée

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server :
   Applications > **Client d'authentification par carte à puce** > **Configurer**
2. Dans le menu Validation du contrôleur de domaine de la section Configuration de carte à puce, sélectionnez la méthode de validation appropriée.
3. Cliquez sur **Appliquer**.

Impossible de trouver la zone dans le fichier de configuration Kerberos

Ajouter ou modifier la zone

- Si vous utilisez la configuration Kerberos simple, procédez comme suit :
  1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server : **Applications** > **Client d'authentification par carte à puce** > **Configurer**
  2. Dans le champ Zone de la section Configuration Kerberos simple, ajoutez ou modifiez le domaine. La zone doit être saisie en majuscules.

     Remarque : La configuration Kerberos simple ne prend pas en charge plusieurs entrées de zone Kerberos. Si plusieurs zones sont requises, installez un fichier de configuration Kerberos contenant les éléments dont vous avez besoin.
  3. Cliquez sur **Appliquer**.
- Si vous utilisez le fichier de configuration Kerberos du périphérique, ajoutez ou modifiez la zone dans le fichier. La zone doit être saisie en majuscules. Quand vous avez terminé, réinstallez le fichier sur l'imprimante.

Les horloges du contrôleur de domaine et du périphérique sont désynchronisées

Assurez-vous que la différence de temps entre l'imprimante et le contrôleur de domaine ne dépasse pas cinq minutes

Pour plus d'informations, reportez-vous à la section « Définition de la date et l'heure » à la page 8.

Impossible de valider la chaîne de certificats du contrôleur de domaine

Essayez les solutions suivantes :

Assurez-vous que tous les certificats requis pour la validation de la chaîne sont installés sur l'imprimante et que les informations sont correctes

Pour plus d'informations, reportez-vous à la section « Installation manuelle de certificats » à la page 7.

Assurez-vous que la chaîne de certificats mène du contrôleur de domaine à l'autorité de certification racine

Assurez-vous que tous les certificats n'ont pas expiré

1. Dans Embedded Web Server, cliquez sur **Paramètres** > **Sécurité** > **Gestion des certificats**.
2. Assurez-vous que les dates de début et de fin de validité n'ont pas expiré.

Autorisez les utilisateurs à se connecter à l'imprimante, même si l'état d'un ou plusieurs certificats n'est pas connu.

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server :

   Applications > **Client d'authentification par carte à puce** > **Configurer**
2. Sous la section OCSP (Online Certificate Status Protocol), sélectionnez **Autoriser état inconnu**.
3. Cliquez sur **Appliquer**.

Contactez votre représentant Lexmark

Impossible de se connecter au répondeur OCSP

Essayez les solutions suivantes :

Vérifiez que l'URL du répondeur OCSP est correcte.

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server :

   Applications > **Client d'authentification par carte à puce** > **Configurer**
2. Dans la section OCSP (Online Certificate Status Protocol), assurez-vous que l'URL du répondeur est correcte.
3. Cliquez sur **Appliquer**.

Augmentez la valeur du délai du répondeur

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server :

   Applications > **Client d'authentification par carte à puce** > **Configurer**
2. Dans le champ Délai du répondeur de la section OCSP (Online Certificate Status Protocol), saisissez une valeur comprise entre 5 et 30.
3. Cliquez sur **Appliquer**.

Impossible de valider le certificat du contrôleur de domaine auprès du répondeur OCSP

Essayez les solutions suivantes :

Vérifiez que l'URL et le certificat du répondeur OCSP sont correctement configurés

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server :

   Applications > **Client d'authentification par carte à puce** > **Configurer**
2. Dans la section Online Certificate Status Protocol (OCSP), dans le champ URL du répondeur, spécifiez les éléments suivants :
   - Adresse IP ou nom d'hôte du répondeur ou du relais OCSP
   - Numéro de port utilisé

   Par exemple, **`http://x:y`**, où ***x*** est l'adresse IP et ***y*** est le numéro de port.

3 Dans le champ Certificat de répondeur, accédez au certificat approprié.

4 Cliquez sur **Appliquer**.

Vérifiez que le contrôleur de domaine renvoie le certificat correct

Assurez-vous que le répondeur OCSP valide le certificat du contrôleur de domaine correct

Impossible d'accéder aux applications et aux fonctions individuelles de l'imprimante

Essayez les solutions suivantes :

Mettez en œuvre un accès sécurisé aux applications ou aux fonctions

Pour plus d'informations, reportez-vous à la section « Sécurisation de l'accès à des applications et des fonctions déterminées » à la page 10.

Si l'utilisateur appartient à un groupe Active Directory, vérifiez que ce groupe est autorisé à accéder aux applications et aux fonctions

Problèmes de Sécuriser l'email

Impossible d'envoyer un e-mail à l'aide de l'application

Assurez-vous que l'application Device Quotas est désactivée

Depuis Embedded Web Server, cliquez sur **Applications** > **Device Quotas** > **Arrêter**.

Impossible de récupérer l'adresse e-mail de l'utilisateur

Essayez les solutions suivantes :

Vérifiez que la fonction d'e-mail de l'imprimante est sécurisée

Pour plus d'informations, reportez-vous à la section « Sécurisation de l'accès à l'imprimante » à la page 9.

Vérifiez que l'adresse e-mail de l'utilisateur est correctement récupérée

1 Accédez à la page de configuration du client d'authentification par carte à puce à partir d'Embedded Web Server.

Applications > **Client d'authentification par carte à puce** > **Configurer**

2 Dans le menu Adresse à partir de l'e-mail de la section Paramètres avancés, sélectionnez l'emplacement où l'imprimante récupère les adresses e-mail de l'utilisateur.

3 Sélectionnez **Attendre les informations de l'utilisateur**.

4 Cliquez sur **Appliquer**.

Contactez votre représentant Lexmark

Impossible de récupérer le certificat de signature de l'utilisateur

Essayez les solutions suivantes :

Assurez-vous qu'un certificat de signature est disponible pour l'utilisateur

Installez le certificat de signature approprié sur la carte à puce de l'utilisateur.

Vérifiez que les certificats sont correctement récupérés.

1. Accédez à la page de configuration du client d'authentification par carte à puce à partir d'Embedded Web Server.

   Applications > **Client d'authentification par carte à puce** > **Configurer**
2. Sous la section Paramètres avancés, sélectionnez **Attendre les informations de l'utilisateur**.
3. Cliquez sur **Appliquer**.

Contactez votre représentant Lexmark

Certificat de signature non disponible pour l'utilisateur

Effectuez l'une des opérations suivantes :

Envoyez l'e-mail sans signature numérique

Assurez-vous qu'un certificat de signature est disponible pour l'utilisateur

Installez le certificat de signature approprié sur la carte à puce de l'utilisateur.

Contactez l'administrateur du système.

Impossible de récupérer des certificats auprès du serveur LDAP

Essayez les solutions suivantes :

Vérifiez que les câbles réseau sont correctement branchés et que les paramètres réseau de l'imprimante sont correctement configurés

Pour plus d'informations, reportez-vous au *Guide de l'utilisateur* de l'imprimante.

Assurez-vous que les paramètres du serveur et du pare-feu sont configurés pour permettre à l'imprimante et au serveur LDAP de communiquer sur le port 389 ou 636.

Si vous utilisez SSL, utilisez le port **636**. Sinon, utilisez le port **389**.

Vérifiez que l'adresse du serveur LDAP contient le nom d'hôte et non pas l'adresse IP.

Pour plus d'informations, reportez-vous à la section « Configuration des paramètres du compte réseau LDAP » à la page 9.

Si le serveur LDAP exige SSL, assurez-vous que les paramètres SSL sont corrects

Pour plus d'informations, reportez-vous à la section « Configuration des paramètres du compte réseau LDAP » à la page 9.

Limitez le plus possible la base de recherche LDAP, mais en incluant tous les utilisateurs requis.

Vérifiez que tous les attributs LDAP sont corrects

Contactez l'administrateur du système.

Impossible de chiffrer l'e-mail pour un ou plusieurs destinataires

Essayez les solutions suivantes :

Envoyez un e-mail chiffré à des destinataires sans certificat de chiffrement et un autre avec certificat de chiffrement

Sélectionnez **Envoyer à tous**. Pour plus d'informations, reportez-vous à la section « Envoi d'un e-mail chiffré à signature numérique » à la page 18.

Envoyez un e-mail chiffré uniquement aux destinataires disposant d'un certificat de chiffrement

Sélectionnez **Envoyer un e-mail chiffré** Pour plus d'informations, reportez-vous à la section « Envoi d'un e-mail chiffré à signature numérique » à la page 18.

Envoyez un e-mail non chiffré à tous les destinataires

Sélectionnez **Envoyer un e-mail non chiffré**. Pour plus d'informations, reportez-vous à la section « Envoi d'un e-mail chiffré à signature numérique » à la page 18.

Contactez votre représentant Lexmark

Impossible de se connecter au serveur de messagerie

Essayez les solutions suivantes :

Vérifiez que l'imprimante est connectée à un domaine.

Pour plus d'informations, reportez-vous à la section « Configuration des paramètres TCP/IP » à la page 8.

Vérifiez que le paramètre Authentification du serveur SMTP est correct

1. Dans Embedded Web Server, cliquez sur **Paramètres** > **E-mail** > **Configuration de la messagerie**.
2. Dans le menu Authentification du serveur SMTP, effectuez l'une des opérations suivantes :
   - Si le serveur SMTP requiert les informations d'authentification utilisateur, sélectionnez **Kerberos 5**.
   - Si Kerberos n'est pas pris en charge, sélectionnez **Aucune authentification requise**.
   - Si le serveur SMTP requiert une authentification, mais ne prend pas en charge Kerberos, dans le champ Adresse de réponse, saisissez l'adresse IP ou le nom d'hôte.
3. Cliquez sur **Enregistrer**.

Remarque : Pour plus d'informations, reportez-vous à la section « Configuration des paramètres de code SMTP » à la page 11.

Si le serveur SMTP utilise Kerberos, vérifiez que les noms d'hôte de la passerelle SMTP primaire et secondaire sont corrects

1. Dans Embedded Web Server, cliquez sur **Paramètres** > **E-mail** > **Configuration de la messagerie**.
2. Dans les champs Passerelle SMTP primaire et Passerelle SMTP secondaire, saisissez le nom d'hôte de la passerelle au lieu de l'adresse IP.
3. Cliquez sur **Enregistrer**.

Assurez-vous que les paramètres du serveur et du pare-feu sont configurés pour permettre à l'imprimante et au serveur SMTP de communiquer sur le port 25.

Vérifiez que les câbles réseau sont correctement branchés et que les paramètres réseau de l'imprimante sont correctement configurés

Pour plus d'informations, reportez-vous au *Guide de l'utilisateur* de l'imprimante.

Contactez l'administrateur du système.

Impossible d'envoyer une copie à soi-même

Essayez les solutions suivantes :

Vérifiez que toutes les informations utilisateur sont saisies dans la session de connexion

Assurez-vous que l'imprimante est configurée pour récupérer toutes les informations utilisateur

1. Accédez à la page de configuration du client d'authentification par carte à puce à partir d'Embedded Web Server.

   Applications > **Client d'authentification par carte à puce** > **Configurer**
2. Sous la section Paramètres avancés, sélectionnez **Attendre les informations de l'utilisateur**.
3. Cliquez sur **Appliquer**.

Vérifiez qu'Envoyer un e-mail à soi-même est correctement configuré

Pour plus d'informations, reportez-vous à la section « Configuration de Envoyer un courrier électronique vers soi » à la page 12.

Contactez votre représentant Lexmark

Problèmes de Sécuriser les travaux d'impression suspendus

Impossible de déterminer l'ID utilisateur

Cette erreur indique que la méthode de connexion (compte local, compte réseau ou module d'authentification) ne définit pas l'ID utilisateur pour la session. Essayez les solutions suivantes :

Vérifiez que l'application est sécurisée

Pour plus d'informations, reportez-vous à la section « Configuration des paramètres Sécuriser les travaux d'impression suspendus » à la page 17.

Vérifiez que l'ID utilisateur de la session est correctement défini

Dans Embedded Web Server, effectuez l'une des opérations suivantes :

Utilisation d'une méthode de connexion avec compte local

1. Cliquez sur **Paramètres** > **Sécurité** > **Méthodes de connexion**.
2. Dans la section Comptes locaux, cliquez sur le type de compte local, puis assurez-vous que le compte possède un nom d'utilisateur.
3. Cliquez sur **Enregistrer**.

Utilisation d'une méthode de connexion avec compte réseau

1. Cliquez sur **Paramètres** > **Sécurité** > **Méthodes de connexion**.
2. Dans la section Comptes réseau, cliquez sur le compte réseau, puis assurez-vous que le compte dispose de l'ID utilisateur correct. Pour plus d'informations, contactez votre administrateur système.
3. Cliquez sur **Enregistrer**.

Utilisation d'un module d'authentification

1. Cliquez sur **Applications**.
2. Sélectionnez le module d'authentification, puis cliquez sur **Configurer**.
3. Spécifiez le paramètre approprié pour l'ID utilisateur de la session.
4. Cliquez sur **Enregistrer** ou sur **Appliquer**.

Contactez votre fournisseur de solutions

Si vous ne parvenez toujours pas à résoudre le problème, contactez votre fournisseur de solution.

Aucun travail d'impression n'est disponible pour l'utilisateur

Essayez les solutions suivantes :

Vérifiez que les travaux sont envoyés à l'imprimante correcte et qu'ils n'ont pas expiré

Il est possible que l'utilisateur ait envoyé les travaux à une autre imprimante ou que les travaux aient été supprimés automatiquement parce qu'ils n'avaient pas été imprimés dans le temps imparti.

Vérifiez que l'ID utilisateur de la session est correctement défini

Dans Embedded Web Server, effectuez l'une des opérations suivantes :

Utilisation d'une méthode de connexion avec compte local

1. Cliquez sur **Paramètres** > **Sécurité** > **Méthodes de connexion**.
2. Dans la section Comptes locaux, cliquez sur le type de compte local, puis assurez-vous que le compte possède un nom d'utilisateur.
3. Cliquez sur **Enregistrer**.

Utilisation d'une méthode de connexion avec compte réseau

1. Cliquez sur **Paramètres** > **Sécurité** > **Méthodes de connexion**.
2. Dans la section Comptes réseau, cliquez sur le compte réseau, puis assurez-vous que le compte dispose de l'ID utilisateur correct. Pour plus d'informations, contactez votre administrateur système.
3. Cliquez sur **Enregistrer**.

Utilisation d'un module d'authentification

1. Cliquez sur **Applications**.
2. Sélectionnez le module d'authentification, puis cliquez sur **Configurer**.
3. Spécifiez le paramètre approprié pour l'ID utilisateur de la session.
4. Cliquez sur **Enregistrer** ou sur **Appliquer**.

Contactez votre fournisseur de solutions

Si vous ne parvenez toujours pas à résoudre le problème, contactez votre fournisseur de solution.

Problèmes avec LDAP

échec des recherches LDAP

Essayez les solutions suivantes :

Assurez-vous que les paramètres du serveur et du pare-feu sont configurés pour permettre à l'imprimante et au serveur LDAP de communiquer sur les ports 389 et 636.

Si votre réseau n'utilise pas la recherche inversée DNS, désactivez-la dans les paramètres Kerberos

1. Depuis le serveur Web incorporé, cliquez sur **Paramètres** > **Sécurité**.
2. Dans la section Comptes réseau, cliquez sur **Kerberos**.
3. Dans la section Autres paramètres, sélectionnez **Désactiver les recherches IP inversées**.
4. Cliquez sur **Enreg. et vérifier**.

Si le serveur LDAP exige SSL, activez SSL pour les recherches LDAP.

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server : **Applications** > **Client d'authentification par carte à puce** > **Configurer**
2. Dans la section Paramètres avancés, sélectionnez **Utiliser SSL pour les informations utilisateur**.
3. Cliquez sur **Appliquer**.

Limitez le plus possible la base de recherche LDAP, mais en incluant tous les utilisateurs requis.

Vérifiez que tous les attributs LDAP sont corrects

Erreur de licence

Contactez votre représentant Lexmark

Avis

Note d'édition

Août 2017

Le paragraphe suivant ne s'applique pas aux pays dans lesquels lesdites clauses ne sont pas conformes à la législation en vigueur : LEXMARK INTERNATIONAL, INC. FOURNIT CETTE PUBLICATION "TELLE QUELLE", SANS GARANTIE D'AUCUNE SORTE, EXPLICITE OU IMPLICITE, Y COMPRIS, MAIS SANS SE LIMITER AUX GARANTIES IMPLICITES DE COMMERCIABILITE OU DE CONFORMITE A UN USAGE SPECIFIQUE. Certains Etats n'admettent pas la renonciation aux garanties explicites ou implicites pour certaines transactions ; c'est pourquoi il se peut que cette déclaration ne vous concerne pas.

Cette publication peut contenir des imprécisions techniques ou des erreurs typographiques. Des modifications sont périodiquement apportées aux informations contenues dans ce document ; ces modifications seront intégrées dans les éditions ultérieures. Des améliorations ou modifications des produits ou programmes décrits dans cette publication peuvent intervenir à tout moment.

Dans la présente publication, les références à des produits, programmes ou services n'impliquent nullement la volonté du fabricant de les rendre disponibles dans tous les pays où celui-ci exerce une activité. Toute référence à un produit, programme ou service n'affirme ou n'implique nullement que seul ce produit, programme ou service puisse être utilisé. Tout produit, programme ou service équivalent par ses fonctions, n'enfreignant pas les droits de propriété intellectuelle, peut être utilisé à la place. L'évaluation et la vérification du fonctionnement en association avec d'autres produits, programmes ou services, à l'exception de ceux expressément désignés par le fabricant, se font aux seuls risques de l'utilisateur.

Pour contacter l'assistance technique de Lexmark, consultez la page **http://support.lexmark.com**.

Pour obtenir des informations sur les consommables et les téléchargements, visitez le site **www.lexmark.com**.

Marques commerciales

Lexmark et le logo Lexmark sont des marques commerciales ou des marques déposées de Lexmark International, Inc. aux Etats-Unis et dans d'autres pays.

Microsoft, Windows et Active Directory sont des marques déposées ou des marques commerciales du groupe Microsoft aux Etats-Unis et dans d'autres pays.

Les autres marques commerciales sont la propriété de leurs détenteurs respectifs.

Index

E

F

H

I