Client d'authentification par carte

Version 2.1

Guide de l'administrateur

Août 2017

www.lexmark.com

Contenus

Historique des modifications

Août 2017

- Ajout d'instructions de modification de la méthode de connexion.
- Ajout de la prise en charge des langues suivantes : portugais brésilien, finnois, français, allemand, italien, chinois simplifié et espagnol.

Janvier 2016

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

Aperçu

Cette application vous permet de sécuriser l'accès aux imprimantes en exigeant des utilisateurs qu'ils se connectent à l'aide d'une carte à puce 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 ou fonctions.

L'application propose aussi des options d'authentification Kerberos ainsi qu'un ticket Kerberos utilisable pour sécuriser d'autres applications.

Ce document fournit des instructions sur la configuration et le dépannage de l'application.

Liste de contrôle préparatoire du déploiement

Vérifiez les points suivants :

- ☐ L'imprimante possède au moins 512 Mo de RAM.
- ☐ Un lecteur de cartes à puce et son pilote sont installés sur l'imprimante.

Vous disposez des informations suivantes pour configurer l'application :

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

  _____

- ☐ Zone, 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 7.

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 11.

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**.

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 12.

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 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 Développez une ou plusieurs catégories, puis décochez les applications ou les fonctions que vous souhaitez sécuriser, 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 12.

6 Développez une ou plusieurs catégories, puis sélectionnez les applications ou les fonctions que vous souhaitez rendre accessibles aux utilisateurs authentifiés.

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 de l'application

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 6.
   - **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**.

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 :

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

2 Cliquez sur **Importer** ou sur **Exporter**.

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 10.

Contactez l'administrateur du système.

L'utilisateur est déconnecté immédiatement après s'être connecté

Augmentez la valeur du délai d'affichage

Pour plus d'informations, reportez-vous à la section « Réglage du délai d'affichage » à la page 6.

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 8.

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 11.

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 6.

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 7.

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 6.

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 8.

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

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.

Licence publique générale secondaire GNU

Consultez la Licence publique générale secondaire GNU en ligne à l'adresse **http://www.gnu.org/licenses/lgpl.html**.

Additional copyrights

This product includes software developed by:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.

2. Redistribution in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution:

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Index