Authentification par carte

Version 5.8

Guide de l'administrateur

Décembre 2020 **www.lexmark.com**

Contenus

Historique des modifications

Décembre 2020

- Ajout d'informations sur un avertissement lié à l'absence d'un lecteur de carte.

Juin 2020

- Ajout d'informations sur les nouveaux paramètres de vérification des certificats.
- Suppression des informations de licence requise.

Juillet 2019

- Ajout d'instructions sur la configuration de l'authentification par code PIN uniquement.

Décembre 2018

- Ajout d'instructions sur la configuration de l'authentification administrateur.

Août 2017

- Ajout d'informations sur les éléments suivants :
  - Paramètres de l'écran de verrouillage
  - Profil personnalisé
- Suppression des informations sur l'utilisation de l'application Personnalisation de l'affichage pour gérer l'écran de connexion.

Août 2016

- Ajout d'informations sur les éléments suivants :
  - Prise en charge de l'authentification par code PIN
  - Boutons d'accès rapide pour la connexion manuelle et la connexion par code PIN

Juillet 2016

- Ajout d'informations sur les éléments suivants :
  - Connexion manuelle
  - Prise en charge de plusieurs domaines
  - Utilisation de comptes de service pour l'authentification auprès du fournisseur de service d'identification
  - Domaines Kerberos multiples pour l'enregistrement de carte et la connexion manuelle
  - Personnalisation de la couleur du texte de connexion
  - Autorisations de groupe

Janvier 2016

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

Aperçu

Utilisez l'application pour sécuriser l'accès à une imprimante à l'aide d'un lecteur de carte. Lorsque les utilisateurs s'identifient avec leur badge, leurs informations d'authentification de l'utilisateur sont utilisées d'une des manières suivantes :

- Via une imprimante maître. Si l'imprimante maître est hors ligne, une imprimante de sauvegarde endosse le rôle d'imprimante maître jusqu'à ce que l'imprimante maître soit de nouveau en ligne.

  Remarque : Lorsque vous configurez les imprimantes, vérifiez qu'elles sont connectées au même réseau.
- Serveurs Lightweight Directory Access Protocol (LDAP), Lexmark™ Document Distributor (LDD) ou Fournisseurs de service d'identité, selon l'authentification définie par l'entreprise.

Vous pouvez également configurer l'application pour permettre aux utilisateurs de se connecter en utilisant un compte de service, un nom d'utilisateur et un mot de passe, un nom d'utilisateur ou encore un code PIN.

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

Liste de contrôle préparatoire du déploiement

Avant de commencer, vérifiez les points suivants :

- ☐ Au moins un compte local ou réseau est configuré sur votre imprimante. Pour plus d'informations, contactez votre administrateur système.
- ☐ Un lecteur de cartes et son pilote sont installés sur l'imprimante.
- ☐ Vous disposez de l'adresse du serveur Web pour configurer l’authentification par code PIN.

Vous disposez des informations suivantes pour configurer la validation de carte à partir de l'imprimante :

- ☐ Nom d'hôte ou adresse IP de l'imprimante maître

  _____

- ☐ Nom d'hôte ou adresse IP de l'imprimante de sauvegarde

  _____

Vous disposez des informations suivantes pour configurer la validation de carte par le service Web :

- ☐ URL du serveur

  _____

- ☐ Enregistrement et consultation de la version de l'interface

Vous disposez des informations suivantes pour configurer la validation de carte LDAP :

Remarque : Vous pouvez également utiliser un compte réseau LDAP existant configuré dans votre imprimante.

- ☐ Adresse du serveur

  _____

- ☐ Numéro de port du serveur

  _____

- ☐ Base de recherche

  _____

- ☐ Nom d'utilisateur

  _____

- ☐ Mot de passe de connexion

_____

☐ Attributs LDAP
- ID utilisateur

  _____
- ID Badge

  _____
- Informations utilisateur (facultatif)

  _____

Vous disposez des informations suivantes pour configurer la validation de carte du service d'identité :

☐ Adresse du fournisseur de service d'identité

_____

☐ Adresse du fournisseur de services liés aux badges

_____

Configuration de l'application

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.

Configuration de l'application en tant que méthode de connexion par défaut

1. Dans Embedded Web Server, cliquez sur **Paramètres** > **Sécurité** > **Méthodes de connexion**.
2. Cliquez sur **Modifier** en regard de Méthode de connexion du panneau de commandes par défaut.
3. Dans le menu du panneau de commandes, sélectionnez **Authentification par carte**.
4. Cliquez sur **Enregistrer**.

Configuration de la validation de carte basée sur l'imprimante

Utilisez la validation basée sur l'imprimante lors de la validation des utilisateurs via une imprimante maître.

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

   Applications > **Authentification par carte** > **Configurer**
2. Dans la section Authentification de l'utilisateur, définissez l'option Validation de carte sur **Basée sur l'imprimante**.

   Remarque : Le paramètre Vérifier le certificat s'applique uniquement à la validation du service d'identification et du service Web.
3. Dans la section Paramètres basés sur l'imprimante, procédez comme suit :
   a. Définissez le rôle de cette imprimante.
      - **Maître** : cette imprimante gère la liste des utilisateurs enregistrés.
      - **Sauvegarde** : si l'imprimante maître est hors ligne, l'imprimante de sauvegarde endosse le rôle de maître jusqu'à ce que l'imprimante maître soit de nouveau en ligne.
      - **Cliente** : cette imprimante ne stocke aucune information sur les utilisateurs. Une imprimante maître ou de sauvegarde est nécessaire pour valider les informations d'identification de l'utilisateur.

      Remarques :

      - Si vous n'utilisez qu'une imprimante, attribuez-lui le rôle de maître.
      - Si vous en utilisez deux, configurez l'une d'elles comme imprimante maître et l'autre comme imprimante de sauvegarde.

- Si vous en utilisez trois ou plus, configurez l'une d'elles comme imprimante maître, la deuxième comme imprimante de sauvegarde et les autres comme imprimantes clientes.

b Saisissez le nom d'hôte ou l'adresse IP de l'imprimante maître et de l'imprimante de sauvegarde.

Remarques :

- Lorsque vous configurez une imprimante de sauvegarde, vous devez saisir le nom d'hôte ou l'adresse IP de l'imprimante maître.
- Lorsque vous configurez des imprimantes clientes, vous devez saisir les noms d'hôte ou les adresses IP de l'imprimante maître et de l'imprimante de sauvegarde.
- Avant d'attribuer une imprimante cliente à une nouvelle imprimante maître, supprimez l'imprimante cliente de l'ancienne imprimante maître.

4 Cliquez sur **Enregistrer**.

Configuration de la validation de carte de service Web

Utilisez la validation basée sur le service Web lors de la validation des utilisateurs via un serveur LDD.

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

Applications > **Authentification par carte** > **Configurer**

2 Dans la section Authentification de l'utilisateur, définissez l'option Validation de carte sur **Service Web**.

3 Sélectionnez **Vérifier le certificat** pour valider toutes les connexions au serveur. Si l'option Vérifier le certificat n'est pas sélectionnée, l'autorité de certification ne sera pas validée.

4 Dans le menu Mode Vérification, sélectionnez **chaîne** ou **pair**.

Remarque : La valeur par défaut est chaîne.

5 Chargez le certificat SSL du serveur pour vous connecter au serveur de manière sécurisée.

6 Dans le champ Vérification Noms d'hôte, saisissez les noms d'hôte supplémentaires (autres que l'URL du serveur par défaut) pour vérifier les entrées du certificat. Utilisez des virgules pour séparer plusieurs noms d'hôte.

Remarque : Par défaut, cette liste blanche contient uniquement l'URL du serveur. Saisissez des noms d'hôte supplémentaires dans le champ Vérification Noms d'hôte pour les inclure dans la liste blanche.

7 Dans la section Paramètres du service Web, saisissez l'URL du serveur LDD.

8 Si nécessaire, réglez le délai de connexion du serveur.

9 Définissez l'interface d'enregistrement. Sélectionnez un des profils suivants :

- **Version 1** : seuls l'ID de badge et l'ID utilisateur sont affichés dans la boîte de dialogue Informations du badge.
- **Version 2** : les éléments suivants sont affichés dans la boîte de dialogue Informations du badge :
  - ID de badge
  - ID utilisateur
  - Adresse IP
  - Nom de l'hôte

10 Définissez l'interface de consultation. Pour enregistrer la date et le lieu où le badge a été utilisé pour la dernière fois, sélectionnez la **version 2**.

11 Cliquez sur **Enregistrer**.

Configuration de la validation de carte LDAP

Utilisez le protocole LDAP lors de la validation des utilisateurs via un serveur LDAP.

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

Applications > **Authentification par carte** > **Configurer**

2 Dans la section Authentification de l'utilisateur, définissez l'option Validation de carte sur **LDAP**.

Remarque : Le paramètre Vérifier le certificat s'applique uniquement à la validation du service d'identification et du service Web.

3 Dans la section Configuration du serveur LDAP, configurez les paramètres.

Remarque : Si l'option **Utiliser le carnet d'adresses** est sélectionnée, l'application utilise alors les paramètres LDAP déjà configurés dans les comptes réseau de l'imprimante. Si plusieurs comptes LDAP sont configurés dans l'imprimante, l'application sélectionne le nom de configuration selon l'ordre alphabétique. Les noms de configuration commençant par une majuscule sont sélectionnés avant les noms commençant par une minuscule.

- **Adresse du serveur** : saisissez l'adresse du serveur LDAP.
- **Port du serveur** : saisissez le numéro de port LDAP.
- **Utiliser SSL** : sélectionnez cette option pour activer une connexion sécurisée.
- **Base de recherche** : saisissez le nœud au niveau duquel se trouvent les comptes utilisateur sur le serveur LDAP. Vous pouvez saisir plusieurs bases de recherche, séparées par des virgules.
- **Nom d'utilisateur de connexion** : saisissez le nom d'utilisateur du compte LDAP. Dans certaines configurations du serveur LDAP, les informations d'identification de l'utilisateur sont requises.
- **Mot de passe de connexion** : saisissez le mot de passe du compte LDAP. Dans certaines configurations du serveur LDAP, les informations d'identification de l'utilisateur sont requises.

4 Dans la section Attributs LDAP, configurez les paramètres.

- **ID utilisateur** : saisissez l'attribut LDAP que l'application recherche lors de l'authentification des informations d'identification de l'utilisateur. Par exemple, **`nomcomptesam`**, **`uid`**, **`cn`** ou un attribut défini par l'utilisateur.
- **ID de badge** : saisissez l'attribut LDAP pour authentifier les utilisateurs avec leurs numéros de badge affectés. Par exemple, **`numéroEmployé`**.
- **Informations utilisateur** : saisissez les autres informations utilisateur que l'application peut récupérer sur le serveur LDAP.
- **Attribut Appartenance au groupe** : saisissez l'attribut LDAP requis pour la recherche de groupe.
- **Liste de groupes** : saisissez le groupe LDAP auquel les comptes utilisateur appartiennent. Les groupes définis sont ajoutés à la liste des autorisations de groupe de l'application, dans laquelle vous pouvez définir les contrôles d'accès spécifiques pour chaque groupe. Vous pouvez saisir plusieurs noms de groupe, séparés par des virgules.

5 Cliquez sur **Enregistrer**.

Configuration de la validation de carte du service d'identification

Utilisez la validation de carte du service d'identification lors de la validation des utilisateurs via un fournisseur de service d'identification.

1. Depuis Embedded Web Server, accédez à la page de configuration de l'application :

   Applications > **Authentification par carte** > **Configurer**

2. Dans la section Authentification de l'utilisateur, définissez l'option Validation de carte sur **Service d'identification**.
3. Sélectionnez **Vérifier le certificat** pour valider toutes les connexions au serveur. Si l'option Vérifier le certificat n'est pas sélectionnée, l'autorité de certification ne sera pas validée.
4. Dans le menu Mode Vérification, sélectionnez **chaîne** ou **pair**.

   Remarque : La valeur par défaut est chaîne.

5. Chargez le Certificat SSL du serveur pour vous connecter au serveur de manière sécurisée.
6. Dans le champ Vérification Noms d'hôte, saisissez les noms d'hôte supplémentaires (autres que l'URL du serveur par défaut) pour vérifier les entrées du certificat. Utilisez des virgules pour séparer plusieurs noms d'hôte.

   Remarque : Par défaut, cette liste blanche contient uniquement l'URL du serveur. Saisissez des noms d'hôte supplémentaires dans le champ Vérification Noms d'hôte pour les inclure dans la liste blanche.

7. Dans la section Paramètres de service d'identification, saisissez le nom d'hôte ou l'adresse IP du fournisseur de service d'identification.
8. Saisissez le nom d'hôte ou l'adresse IP du fournisseur de services liés aux badges.
9. Définissez la stratégie d'accès à l'application.
   - **Continuer** : continuez à utiliser l'imprimante même si la connexion au serveur du service d'identification échoue.
   - **Echec** : revenez à l'écran de connexion si la connexion au serveur du service d'identification échoue.
10. Si vous disposez d'un ID client et d'un secret client auprès de votre fournisseur de service d'identification, saisissez les informations dans les champs correspondants.
11. Réglez le délai d'attente du socket et du réseau.
12. Téléchargez le certificat SSL du serveur pour vous connecter au serveur de manière sécurisée.
13. Pour permettre aux utilisateurs de se connecter à l'imprimante avec un compte de service distinct, sélectionnez **Utiliser le compte de service**, puis saisissez les informations d'identification du compte de service.
14. Définissez Enregistrement de la carte sur **Service d'identification**.
15. Cliquez sur **Enregistrer**.

Configuration de l'authentification par code PIN

Avant de commencer, assurez-vous que vos informations d'identification sont configurées dans les paramètres de compte local ou réseau de l'imprimante.

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

   Applications > **Authentification par carte** > **Configurer**

2. Dans la section Authentification de l'utilisateur, sous Connexion par code PIN, sélectionnez **Activer la connexion par code PIN**.
3. Sélectionnez **Afficher sur l'écran de veille** pour afficher le bouton Connexion par code PIN sur l'écran de veille.
4. Dans la section Paramètres de code PIN, sous Authentif. requise, sélectionnez une méthode de connexion.
   - **ID util. + PIN** : nom d'utilisateur et code PIN nécessaires pour l'authentification.
   - **Code PIN uniquement** : code PIN nécessaire pour l'authentification.

   Remarque : Si la méthode Code PIN uniquement est sélectionnée, vous ne pouvez pas enregistrer un nouveau code PIN ni mettre à jour un code PIN existant.
5. Saisissez l'adresse du serveur Web à l'endroit où les codes PIN sont enregistrés.
6. Si nécessaire, saisissez le texte de connexion par code PIN, puis définissez la longueur minimum du code PIN.

   Remarque : Si le champ de texte du code PIN reste vide, le texte de connexion par code PIN s'affiche. Le texte de connexion par code PIN par défaut est **`Saisissez vos informations d'identification utilisateur pour vous connecter.`**
7. Si nécessaire, saisissez les messages d'erreur signalant un code PIN non valide.

   Remarque : Si les champs de texte restent vides, les messages d'erreur par défaut seront affichés. Les messages d'erreur par défaut sont **`Longueur du code PIN non valide.`** et **`Code PIN non valide.`**
8. Si nécessaire, réglez le délai d'attente du socket et du réseau.

   Remarque : La valeur par défaut pour le délai d'attente du socket et du réseau est de 15 secondes.
9. Cliquez sur **Enregistrer**.

Attribution d'une méthode de connexion pour l'enregistrement de carte

Avant de commencer, assurez-vous que vos informations d'identification sont configurées dans les paramètres de compte local ou réseau de l'imprimante.

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

   Applications > **Authentification par carte** > **Configurer**

2. Dans la section Authentification de l'utilisateur, sous Enregistrement de la carte, sélectionnez une méthode de connexion.

   Remarque : Si vous souhaitez utiliser Kerberos, Active Directory ou LDAP+GSSAPI, sélectionnez un domaine. Si la méthode de connexion sélectionnée comporte plusieurs domaines, le domaine sélectionné est le domaine affiché par défaut lors de l'enregistrement de carte.

3. Cliquez sur **Enregistrer**.

Attribution d'une méthode de connexion pour la connexion manuelle

Avant de commencer, assurez-vous que vos informations d'identification sont configurées dans les paramètres de compte local ou réseau de l'imprimante.

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

   Applications > **Authentification par carte** > **Configurer**

2. Dans la section Authentification de l'utilisateur, dans la section Paramètres de connexion manuelle, définissez **Connexion manuelle** comme méthode de connexion préférée.

   Remarques :

   - Si la connexion manuelle est définie sur Service d'identité et que l'option Utiliser le compte de service est activée, les utilisateurs ne sont pas invités à saisir leurs informations d'identification manuellement. L'application utilise le compte de service pour la connexion.
   - Si vous souhaitez utiliser Kerberos, Active Directory ou LDAP+GSSAPI, sélectionnez un domaine. Si la méthode de connexion sélectionnée comporte plusieurs domaines, le domaine sélectionné est le domaine affiché par défaut lors de la connexion manuelle.

3. Sélectionnez **Afficher sur l'économiseur d'écran** pour afficher le bouton Connexion manuelle sur l'économiseur d'écran.

4. Cliquez sur **Enregistrer**.

Configuration de l'authentification administrateur

1. Depuis Embedded Web Server, accédez à la page de configuration de l'application :

   Applications > **Authentification par carte** > **Configurer**

2. Dans la section Authentification de l'utilisateur, sous Paramètres de connexion administrateur, choisissez une méthode de connexion pour **Connexion administrateur**.

   Remarque : Assurez-vous d'avoir configuré un compte d'administrateur local pour l'imprimante et d'avoir configuré les autorisations pour le Groupe d'administrateurs du périphérique. Par défaut, les fonctions et les menus ne sont pas autorisés dans ce groupe.

3. Sélectionnez un groupe autorisé pouvant utiliser la fonction de connexion administrateur.

   Remarque : Ce paramètre est uniquement applicable aux comptes nom d'utilisateur et aux comptes nom d'utilisateur et mot de passe.

4. Sélectionnez **Afficher sur l'économiseur d'écran** pour afficher le bouton Connexion administrateur sur l'écran de veille.

5. Cliquez sur **Enregistrer**.

Affichage des domaines pour les comptes utilisateur

La fonction Utiliser le domaine sélectionné ne s'applique que si la méthode de connexion pour l'enregistrement de carte et la connexion manuelle est Kerberos, Active Directory ou LDAP+GSSAPI. En outre, cette fonction s'applique uniquement si la validation de carte est définie sur Service Web ou Basée sur l'imprimante.

Pour l'enregistrement de carte, si cette fonction est activée, l'ID de badge enregistrée est au format nomdutilisateur@domaine.

Pour la connexion manuelle, si cette fonction est activée, le nom d'utilisateur indiqué sur le panneau de commandes de l'imprimante est au format nomdutilisateur@domaine.

Ces paramètres ne s'appliquent pas à la connexion par code PIN ni à l'enregistrement de code PIN.

Pour activer cette fonction, procédez comme suit :

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

   Applications > **Authentification par carte** > **Configurer**

2. Dans la section Paramètres avancés, sélectionnez **Utiliser le domaine sélectionné**.

3. Cliquez sur **Enregistrer**.

Configuration de l'écran de connexion

Remarque : Vérifiez que le paramètre de l'écran de veille de l'application Personnalisation de l'affichage est désactivé. Pour plus d'informations, reportez-vous au *Guide de l'administrateur de la personnalisation de l'affichage*.

1. Depuis Embedded Web Server, accédez à la page de configuration de l'application :

   Applications > **Authentification par carte** > **Configurer**

2. Dans la section Paramètres de l'écran de connexion, procédez comme suit :
   - Pour personnaliser le message de connexion, sélectionnez **Utiliser un texte de connexion personnalisé**, puis saisissez le message.
   - Définissez la couleur personnalisée du texte de connexion sur noir ou blanc.
   - Pour modifier l'arrière-plan de l'écran de connexion, sélectionnez **Utiliser une image personnalisée pour l'écran de connexion**, puis téléchargez le fichier image.
   - Pour personnaliser le message de connexion manuelle, saisissez un message dans le champ Texte de connexion manuelle.
   - Pour personnaliser le message de connexion administrateur, saisissez un message dans le champ Texte de connexion administrateur.
   - Activez la copie et la télécopie sans connexion.
   - Désactivez l'avertissement informant l'utilisateur qu'aucun lecteur de cartes n'est connecté.
3. Dans la section Paramètres de l'écran de verrouillage, sélectionnez l'emplacement du texte de connexion, puis saisissez le nom du profil ou l'ID de l'application. Le profil se lance automatiquement après la connexion.
4. Dans la section Profil personnalisé, saisissez le nom du profil, l'ID de l'application ou la fonction d'imprimante, puis saisissez le nom personnalisé de l'icône. Si nécessaire, sélectionnez **Utiliser une icône personnalisée**, puis téléchargez le fichier image.
5. Cliquez sur **Enregistrer**.

   Remarque : L'écran de connexion peut être désactivé uniquement dans les environnements qui utilisent le service d'identification.

Activez l'accès public pour les fonctions de copie et de télécopie

1. Dans Embedded Web Server, cliquez sur **Paramètres** > **Sécurité** > **Méthodes de connexion**.
2. Dans la section Public, cliquez sur **Gérer les autorisations**.
3. Développez **Accès aux fonctions**, puis sélectionnez **Fonction Copie** et **Fonction Télécopie**.
4. Cliquez sur **Enregistrer**.

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

Pour obliger les utilisateurs à s'authentifier avant d'accéder à une application ou à une fonction de l'imprimante, procédez comme suit :

Restreindre l'accès public aux applications ou fonctions

1. Dans Embedded Web Server, cliquez sur **Paramètres** > **Sécurité** > **Méthodes de connexion**.
2. Dans la section Public, cliquez sur **Gestion des autorisations**.

3 Développez une ou plusieurs catégories, puis décochez l'application ou la fonction que vous souhaitez sécuriser.

4 Cliquez sur **Enregistrer**.

Gérer les autorisations de groupe

Remarque : Si la fonction Connexion administrateur est activée, configurez les autorisations Groupe d'administrateurs du périphérique.

1 Dans la section Méthodes de connexion supplémentaires, cliquez sur **Gestion des autorisations** en regard de Authentification par carte.

2 Sélectionnez le groupe dont vous souhaitez gérer les autorisations.

Remarque : La liste indique les groupes ajoutés à la Liste de groupes LDAP dans la page de configuration de l'application.

3 Développez une ou plusieurs catégories, puis sélectionnez l'application ou la fonction que vous souhaitez rendre accessible.

4 Cliquez sur **Enregistrer**.

Remarques :

- Lors de la connexion, l'application applique les autorisations du groupe auquel l'utilisateur appartient. Si l'utilisateur appartient à plusieurs groupes, l'application fusionne toutes les autorisations. Par exemple : seule la copie est autorisée pour le groupe A et seule la télécopie est autorisée pour le groupe B. Si l'utilisateur appartient aux deux groupes, l'application permet à l'utilisateur de copier et d'envoyer des télécopies.
- Les autorisations de groupe de la méthode de connexion attribuée pour l'enregistrement de carte et la connexion manuelle doivent être identiques aux autorisations de groupe configurées dans l'application.

Configuration du délai de déconnexion du badge

Définissez la durée après laquelle l'imprimante interprète un deuxième passage du badge comme une déconnexion. Si vous passez votre carte dans le temps imparti, vous resterez connecté. Si vous passez votre carte après expiration du délai, vous serez déconnecté.

Si vous êtes connecté et qu'un autre utilisateur se connecte avec une carte, vous serez immédiatement déconnecté et l'autre utilisateur sera connecté. Ce comportement prend effet même si le délai de déconnexion du badge n'a pas expiré.

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

Applications > **Authentification par carte** > **Configurer**

2 Dans la section Paramètres avancés, définissez le délai de déconnexion du badge.

3 Cliquez sur **Enregistrer**.

Importation ou exportation d'un fichier de configuration

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 > **Authentification par carte** > **Configurer**

2. Cliquez sur **Importer/exporter la configuration**.
3. Effectuez l'une des opérations suivantes :
   - Localisez le fichier de configuration, puis cliquez sur **Importer**.
   - Cliquez sur **Exporter**.

Gestion de l'application

Pour la validation de carte basée sur l'imprimante, vous pouvez gérer les imprimantes clientes et les comptes utilisateur dans la page d'état de l'application.

Remarques :

- La page d'état de l'application est disponible uniquement lorsque vous utilisez l'authentification basée sur l'imprimante.
- Si aucun rôle n'est attribué à une imprimante, celle-ci apparaît comme non configurée dans la page d'état de l'application. Assurez-vous de définir le rôle de l'imprimante. Pour plus d'informations, reportez-vous à la section « Configuration de la validation de carte basée sur l'imprimante » à la page 8.

Accès à la page d'état de l'application

La fenêtre d'état vous permet de suivre l'activité de l'imprimante.

1. Depuis Embedded Web Server, cliquez sur **Applications** > **Lancement d'applications** > **Authentification par carte**.
2. Notez les informations suivantes :
   - **Etat** : présente l'état d'activité de l'imprimante.
     - **Non configurée** : aucune imprimante n’a été configurée.
     - **Hors ligne** : aucune activité ou communication de l'imprimante n'est en cours.
     - **En ligne** : l'imprimante est active.
   - **Fonctionnement** : durée de fonctionnement de l'application.
   - **(cette imprimante)** : imprimante actuelle.
   - **Dernière activité** : dernière activité effectuée sur l'imprimante maître.
   - **Nombre d'utilisateurs** : nombre total d'utilisateurs enregistrés.
   - **Etat de l'enregistrement** : indique si l'imprimante est en ligne ou hors ligne.
   - **Dernière synchronisation avec l'imprimante maître** : date de la dernière mise à jour de l'imprimante de sauvegarde avec l'imprimante maître.
   - **Dernier contact avec l'imprimante maître** : date de la dernière communication de l'imprimante de sauvegarde avec l'imprimante maître.
   - **Dernière synchronisation en tant qu'imprimante maître** : date de la dernière fois où l'imprimante de sauvegarde a assumé le rôle d'imprimante maître.
   - **Dernière activité en tant qu'imprimante maître** : dernière activité de l'imprimante de sauvegarde en tant qu'imprimante maître.
   - **Durée d'utilisation en tant qu'imprimante maître** : durée du fonctionnement de l'imprimante de sauvegarde en tant qu'imprimante maître.
   - **Service en cours par** : imprimante cliente récemment entrée en contact avec l'imprimante maître ou l'imprimante de sauvegarde.
   - **Dernière activité avec l'imprimante de sauvegarde** : date du dernier contact de l'imprimante cliente avec l'imprimante de sauvegarde.

Gestion des imprimantes clientes et des comptes utilisateur

Remarque : Cette fonction s'affiche uniquement lorsque l'imprimante est la machine maître.

1. Depuis Embedded Web Server, cliquez sur **Applications** > **Lancement d'applications** > **Authentification par carte**.
2. Dans la section Clientes, effectuez une des procédures suivantes :

Ajouter des imprimantes clientes

a. Cliquez sur **Ajouter des clientes**.

b. Saisissez l'adresse IP de l'imprimante cliente et cliquez sur **Ajouter clientes**.

Remarques :

- Si vous utilisez plusieurs adresses IP, séparez-les par des virgules.
- Utilisez l'astérisque comme dernier octet pour rechercher plusieurs adresses IP. Par exemple, saisissez **`10.194.1.*`**.

Supprimer des imprimantes clientes

a. Sélectionnez une ou plusieurs imprimantes clientes dans la liste Clientes.

b. Cliquez sur **Supprimer des clientes**.

Remarque : Vous ne pouvez pas supprimer d'imprimantes clientes lorsque l'application est hors ligne ou si elle a été désinstallée.

Suppression de comptes utilisateur

1. Depuis Embedded Web Server, cliquez sur **Applications** > **Lancement d'applications** > **Authentification par carte**.
2. Dans la section Maître, cliquez sur **Supprimer des utilisateurs**.
3. Saisissez l'ID utilisateur.

   Remarque : Si vous recherchez plusieurs ID utilisateur, séparez-les par des virgules.
4. Cliquez sur **Supprimer**.

Réattribution des rôles d'imprimante

Configuration d'une nouvelle imprimante maître

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

   Applications > **Authentification par carte** > **Configurer**
2. Cliquez sur **Authentification de l'utilisateur**, puis dans la section Paramètres basés sur l'imprimante, définissez le rôle sur **Maître**.

3 Saisissez le nom d'hôte ou l'adresse IP de l'imprimante de sauvegarde.

4 Cliquez sur **Enregistrer**.

Attribution de l'imprimante de sauvegarde à la nouvelle imprimante maître

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

Applications > **Authentification par carte** > **Configurer**

2 Cliquez sur **Authentification de l'utilisateur**, puis dans la section Paramètres basés sur l'imprimante, définissez le rôle sur **Sauvegarde**.

3 Entrez le nom d'hôte ou l'adresse IP de la nouvelle imprimante maître.

4 Cliquez sur **Enregistrer**.

Réattribution d'une imprimante cliente

1 Dans l'Embedded Web Server de l'imprimante maître actuelle, cliquez sur **Applications** > **Lancement d'applications** > **Authentification par carte**.

2 Dans la section Clientes, supprimez l'imprimante cliente.

3 Effectuez l'une des opérations suivantes :

Ajouter l'imprimante cliente via la page de configuration de l'application

a Accédez à la page de configuration de l'application à partir d'Embedded Web Server sur l'imprimante cliente :

Applications > **Authentification par carte** > **Configurer**

b Cliquez sur **Authentification de l'utilisateur**, puis dans la section Paramètres basés sur l'imprimante, définissez le rôle sur **Cliente**.

c Saisissez les noms d'hôte ou les adresses IP de la nouvelle imprimante maître et de la nouvelle imprimante de sauvegarde.

d Cliquez sur **Enregistrer**.

Ajouter l'imprimante cliente via la page d'état de l'imprimante maître

a Dans Embedded Web Server de la nouvelle imprimante maître, cliquez sur **Applications** > **Lancement d'applications** > **Authentification par carte**.

b Dans la section Clientes, cliquez sur **Ajouter clientes**.

c Saisissez l'adresse IP de l'imprimante cliente.

d Cliquez sur **Ajouter des clientes**.

Utilisation de l'application

Enregistrement des utilisateurs

1. Passez votre carte sur le lecteur de carte.
2. Saisissez vos informations d'identification sur le panneau de commandes de l'imprimante.

   Remarque : Si vous utilisez Kerberos, Active Directory ou LDAP+GSSAPI pour l'enregistrement de carte, sélectionnez un domaine.
3. Appuyez sur **Enregistrer**.

   Remarque : Une fois l'enregistrement terminé, vous êtes automatiquement connecté. Si vous passez votre carte au cours de la période définie pour le délai de déconnexion, vous resterez connecté. Pour vous déconnecter, appuyez sur le bouton d'accueil ou sur le nom d'utilisateur dans le coin supérieur droit du panneau de commandes de l'imprimante, puis confirmez la déconnexion. Pour plus d'informations, reportez-vous à la section « Configuration du délai de déconnexion du badge » à la page 16.

Enregistrement d'un code PIN

1. Dans le panneau de commandes de l'imprimante, appuyez sur **Connexion par code PIN**.
2. Appuyez sur ⋮ > **Enregistrer le code PIN**.

   Remarque : Pour modifier un code PIN, appuyez sur **Modifier le code PIN**.
3. Suivez les instructions qui s'affichent à l'écran.

Connexion manuelle à l'imprimante

1. Sur le panneau de commandes de l'imprimante, appuyez sur l'une des options suivantes :
   - **Connexion par code PIN**
   - **Connexion manuelle**
   - **Connexion administrateur**

   Remarque : Si vous sélectionnez **Connexion administrateur**, il est impossible de récupérer les informations d'autres utilisateurs à partir du serveur LDAP.
2. Saisissez vos identifiants de connexion.

   Remarque : Si vous utilisez Kerberos, Active Directory ou LDAP+GSSAPI pour la connexion manuelle, sélectionnez un domaine.
3. Suivez les instructions qui s'affichent à l'écran.

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

Erreur d'authentification

Essayez les solutions suivantes :

Augmentez le délai de mise en veille de l'imprimante

Si vous utilisez Service d'identité en tant que méthode de validation de carte, l'imprimante aura peut-être besoin de plus de temps pour communiquer avec le fournisseur de service d'identité.

1. Dans Embedded Web Server, cliquez sur **Paramètres** > **Périphérique**.
2. Procédez comme suit :

   #### Réglez le délai d'affichage

   a. Cliquez sur **Préférences**.
   b. Augmentez la valeur du délai d'affichage.
   c. Cliquez sur **Enregistrer**.

   #### Réglez le délai de passage en mode Veille

   a. Cliquez sur **Gestion de l'alimentation**.
   b. Augmentez la valeur du mode Veille.
   c. Cliquez sur **Enregistrer**.

Vérifiez que l'imprimante est connectée au réseau.

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

Vérifiez que le serveur de sécurité est en ligne et qu'il n'est pas occupé.

Pour plus d'informations, contactez votre administrateur système.

L'utilisateur est bloqué

Mettez à jour le délai de verrouillage et le nombre de tentatives de connexion autorisé

Il est possible que l'utilisateur ait atteint le nombre d'échecs de connexion autorisé.

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. Mettez à jour le délai de verrouillage et le nombre de tentatives de connexion autorisé.
3. Cliquez sur **Enregistrer**.

   Remarque : Attendez que le délai de verrouillage soit écoulé pour que les nouveaux paramètres prennent effet.

Impossible d'enregistrer une imprimante cliente

Essayez les solutions suivantes :

Vérifiez que l'imprimante maître ou l'imprimante de sauvegarde est en ligne.

Pour plus d'informations, reportez-vous à la section « Accès à la page d'état de l'application » à la page 18.

Vérifiez que l'imprimante maître et l'imprimante de sauvegarde sont correctement configurées.

Pour plus d'informations, reportez-vous à la section « Configuration de la validation de carte basée sur l'imprimante » à la page 8.

Contactez votre fournisseur de solutions.

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

Impossible de se connecter au serveur LDAP

Essayez les solutions suivantes :

Vérifiez que les paramètres LDAP sont correctement configurés.

Pour plus d'informations, reportez-vous à la section « Configuration de la validation de carte LDAP » à la page 10.

Contactez votre fournisseur de solutions.

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

Certains paramètres n'apparaissent pas dans la page de configuration

Essayez l'une ou plusieurs des solutions suivantes :

Assurez-vous d'utiliser le navigateur Web recommandé

Pour plus d'informations, reportez-vous au fichier *Readme*.

Lorsque vous utilisez Internet Explorer, assurez-vous que les sites Intranet ne s'affichent pas en mode Affichage de compatibilité.

Pour plus d'informations, reportez-vous à l'aide du navigateur.

Contactez votre représentant Lexmark

L'utilisateur n'a aucun droit d'accès

Essayez les solutions suivantes :

Activez les autorisations de la méthode de connexion attribuée à l'enregistrement de carte et à la connexion manuelle

1. Dans Embedded Web Server, cliquez sur **Paramètres** > **Sécurité** > **Méthodes de connexion**.
2. Cliquez sur **Gérer groupes/autorisations** en regard de la méthode de connexion attribuée à l'enregistrement de carte et à la connexion manuelle.
3. Activez les autorisations identiques aux autorisations d'authentification par carte.
4. Cliquez sur **Enregistrer**.

Contactez votre représentant Lexmark

Impossible de trouver les informations sur le domaine

L'option Utiliser le domaine sélectionné est activée dans l'application, mais la méthode de connexion attribuée pour la connexion manuelle ou l'enregistrement de carte ne nécessite pas de sélection de domaine. Par exemple, des comptes locaux ou LDAP. Les méthodes de connexion qui nécessitent une sélection de domaine sont Kerberos, Active Directory et LDAP+GSSAPI.

Essayez les solutions suivantes :

Désactivez la sélection de domaine

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

   Applications > **Authentification par carte** > **Configurer**
2. Dans la section Paramètres avancés, décochez **Utiliser le domaine sélectionné**.
3. Cliquez sur **Enregistrer**.

Modifiez la méthode de connexion

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

   Applications > **Authentification par carte** > **Configurer**
2. Dans la section Authentification de l'utilisateur, définissez la méthode de connexion pour l'enregistrement de carte et la connexion manuelle sur Kerberos, Active Directory ou LDAP+GSSAPI.
3. Cliquez sur **Enregistrer**.

Contactez votre représentant Lexmark

Foire Aux Questions (FAQ)

Pourquoi ne puis-je pas ajouter ou supprimer une imprimante cliente lorsque l'imprimante de sauvegarde endosse le rôle de maître ?

Pour que vous puissiez supprimer ou ajouter une imprimante cliente, l'imprimante maître doit être en ligne.

Puis-je supprimer une imprimante cliente même si l'imprimante maître est hors ligne, puis la réattribuer à la nouvelle imprimante maître ?

Oui. Procédez comme suit :

1. Réinstallez l'application à partir de l'imprimante cliente.
2. Attribuez-lui le rôle d'imprimante cliente et associez-la avec l'imprimante maître et l'imprimante de sauvegarde. Pour plus d'informations, reportez-vous à la section « Configuration de la validation de carte basée sur l'imprimante » à la page 8.

Pourquoi ne puis-je pas voir un bouton Copie ou Télécopie sur l'écran de verrouillage alors que j'ai activé la copie ou la télécopie sans connexion ?

Si aucun contrôle d'accès n'est pas défini pour la fonction de copie ou de télécopie, le bouton Copie ou Télécopie n'apparaît pas. Pour plus d'informations, reportez-vous à la section « Configuration de l'écran de connexion » à la page 14.

Comment puis-je restreindre l'accès public à la page de configuration pour toutes les applications ?

1. Dans Embedded Web Server, cliquez sur **Paramètres** > **Sécurité** > **Méthodes de connexion**.
2. Dans la section Public, cliquez sur **Gérer autorisations**.
3. Développez **Gestion des périphériques**, puis décochez **Configuration des applications**.
4. Cliquez sur **Enregistrer**.
5. Dans Embedded Web Server, cliquez sur **Paramètres** > **Sécurité** > **Méthodes de connexion**.
6. Cliquez sur **Gérer autorisations** ou **Gérer groupes/autorisations** en regard de la méthode de connexion que vous souhaitez configurer.

7 Cliquez sur le groupe auquel vous souhaitez donner l'accès à la page de configuration pour toutes les applications.

8 Développez **Gestion des périphériques**, puis assurez-vous que l'option **Configuration des applications** est sélectionnée.

9 Cliquez sur Enregistrer.

Avis

Note d'édition

Décembre 2020

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 bénéficier de l'assistance technique de Lexmark, rendez-vous sur le site **http://support.lexmark.com**.

Pour obtenir des informations sur la politique de confidentialité de Lexmark régissant l'utilisation de ce produit, consultez la page **www.lexmark.com/privacy**.

Pour obtenir des informations sur les fournitures et les téléchargements, rendez-vous sur 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.

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

Index

P

Q

R

S

U

V