Authentification par carte

Guide de l'administrateur

Décembre 2020

www.lexmark.com

Contenus

Aperçu

Utilisez l'application pour sécuriser l'accès à une imprimante à l'aide d'un lecteur de carte. Lorsque les utilisateurs s'identifient, leurs informations de connexion sont authentifiées à l’aide de l'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) ou Lexmark™ Document Distributor (LDD), ou Fournisseurs de service d'identité, selon l'authentification définie par l'organisation.

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

Configuration des éléments requis

Vous devrez peut-être disposer des droits administrateur pour configurer 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.
   - Dans la section TCP/IP du menu Réseau/Ports, affichez l'adresse IP.
2. Ouvrez un navigateur Web, puis saisissez l'adresse IP de l'imprimante.

Ajout d'un compte d'utilisateur interne

Un compte d'utilisateur interne est nécessaire en cas d'utilisation de l'authentification basée sur l'imprimante.

1. Dans Embedded Web Server, cliquez sur **Paramètres** ou **Configuration**.
2. Selon votre modèle d'imprimante, effectuez l'une des opérations suivantes :
   - Cliquez sur **Sécurité** > **Configuration de sécurité** > **Comptes internes** > **Ajouter un compte interne**.
   - Cliquez sur **Sécurité** > **Modifier les configurations de sécurité** > **Comptes internes** > **Ajouter un compte interne**.
3. Entrez les informations de compte, puis cliquez sur **Envoyer**.
4. Si nécessaire, dans la section Gérer les comptes internes, saisissez un nom de bloc fonctionnel personnalisé, puis indiquez les informations d'identification requises.
5. Cliquez sur **Envoyer**.

Configuration de groupes pour comptes d'utilisateur interne

1. Dans Embedded Web Server, cliquez sur **Paramètres** ou **Configuration**.
2. Selon votre modèle d'imprimante, effectuez l'une des opérations suivantes :
   - Cliquez sur **Sécurité** > **Configuration de la sécurité** > **Comptes internes** > **Groupes pour utilisation des comptes internes**.
   - Cliquez sur **Sécurité** > **Modifier les configurations de sécurité** > **Comptes internes** > **Groupes pour utilisation des comptes internes**.
3. Entrez un nom de groupe et cliquez sur **Ajouter**.
4. Ajoutez des comptes internes au groupe.
5. Cliquez sur **Envoyer**.

Création d'un modèle de sécurité

Un modèle de sécurité est composé de blocs fonctionnels de sécurité, tels que des comptes internes, Kerberos, LDAP, LDAP+GSSAPI ou encore Active Directory. Ces modèles sont appliqués au contrôle d'accès pour sécuriser les applications et les fonctions de l'imprimante.

1. Dans Embedded Web Server, cliquez sur **Paramètres** ou **Configuration**.
2. Selon votre modèle d'imprimante, effectuez l'une des opérations suivantes :
   - Cliquez sur **Sécurité** > **Configuration de la sécurité** > **Modèle de sécurité** > **Ajouter un modèle de sécurité**.
   - Cliquez sur **Sécurité** > **Modifier les configurations de sécurité** > **Modèles de sécurité** > **Ajouter un modèle de sécurité**.
3. Saisissez un nom de modèle de sécurité, puis sélectionnez l'une des configurations d'authentification suivantes :
   - Pour l'authentification basée sur l'imprimante dans une configuration autonome, sélectionnez un bloc fonctionnel de compte interne.
   - Pour l'authentification basée sur l'imprimante avec l'impression à la demande sans serveur LPM (solution d'infogérance d'impression Lexmark) dans une configuration Active Directory, sélectionnez un bloc fonctionnel LDAP+GSSAPI.
   - Pour l'authentification LDAP, sélectionnez un bloc fonctionnel LDAP.
4. Cliquez sur **Enregistrer modèle**.

Remarque : Pour modifier un modèle de sécurité existant, cliquez sur le modèle de sécurité, puis ajoutez ou modifiez une autorisation pour le modèle.

Configuration des contrôles d'accès

Remarque : Lorsque vous utilisez la fonction **Connexion administrateur** , assurez-vous d'avoir configuré le modèle de sécurité pour les comptes internes. Pour plus d'informations, reportez-vous à la section « Création d'un modèle de sécurité » à la page 6.

1. Dans Embedded Web Server, cliquez sur **Paramètres** ou **Configuration**.
2. Selon votre modèle d'imprimante, effectuez l'une des opérations suivantes :
   - Cliquez sur **Securité** > **Configuration de la sécurité** > **Contrôles d'accès**.
   - Cliquez sur **Sécurité** > **Modifier les configurations de sécurité** > **Contrôles d'accès**.
3. Cliquez sur **Applications de périphérique** ou **Solutions de périphérique**, puis procédez comme suit :
   - Appliquez App 1 ou Solution 1 à un modèle de sécurité de compte interne, LDAP+GSSAPI ou Active Directory.
   - Appliquez App 2 ou Solution 2 au modèle de sécurité de l'application.

     Remarque : Le modèle de sécurité de l'application est le modèle pour lequel la configuration d'authentification est CardAuth. Pour plus d'informations, reportez-vous à la section « Création d'un modèle de sécurité » à la page 6.
   - Appliquez App 3 ou Solution 3 à un modèle de sécurité LDAP.

Remarques :

- Si l'impression à la demande LPM est installée, appliquez le contrôle d'accès d'impression à la demande au modèle de sécurité de l'application.
- Les imprimantes avec structure Embedded Solutions (eSF) version 2.x requièrent l'application eSF Security Manager pour configurer le contrôle d'accès. Pour voir une liste de ces imprimantes, consultez le fichier *Readme*.

4 Cliquez sur **Envoyer**.

Configuration de l'application

Avant de commencer, effectuez les opérations suivantes :

- Désactivez l'arrière-plan et l'écran de veille ainsi que toute application d'authentification existante.
- Installez les éléments suivants :
  - Programme d'installation de l'authentification par carte
  - Pilote du lecteur de cartes
  - Lecteur de cartes
  - Gestionnaire de sécurité eSF

    Remarque : Les imprimantes eSF version 2.x requièrent l'application eSF Security Manager pour configurer le contrôle d'accès. Pour voir une liste de ces imprimantes, consultez le fichier *Readme*.

Accès à la page de configuration de l'application

1. Dans Embedded Web Server, cliquez sur **Paramètres** ou **Configuration**.
2. Selon votre modèle d'imprimante, effectuez l'une des opérations suivantes :
   - Cliquez sur **Applications** > **Gestion des applications**.
   - Cliquez sur **Solutions pour l'appareil** > **Solutions (eSF)**.
   - Cliquez sur **Embedded Solutions**.
3. Cliquez sur **Authentification par carte** > **Configurer**.

Configuration de l'authentification administrateur

Remarque : Lorsque vous utilisez la fonction **Connexion administrateur** , assurez-vous d'avoir configuré le modèle de sécurité pour les comptes internes, le code PIN et le mot de passe. Pour plus d'informations, reportez-vous à la section « Création d'un modèle de sécurité » à la page 6.

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server.
2. Dans la section Authentification d'utilisateur, choisissez une méthode de connexion pour **Contrôle d'accès de connexion administrateur**.

   Remarques :

   - Vérifiez que le contrôle d'accès sélectionné est configuré avec un modèle de sécurité. Pour plus d'informations, reportez-vous à la section « Création d'un modèle de sécurité » à la page 6.
   - Si vous sélectionnez **Désactivé**, l'option **Connexion administrateur** ne s'affichera pas sur le panneau de commandes de l'imprimante.
3. Cliquez sur **Appliquer**.

Configuration de l'écran de connexion

L'écran de connexion peut être configuré pour effectuer les opérations suivantes :

- Utiliser les fonctions de copie et de télécopie sans connexion.
- Choisir la méthode de connexion à utiliser.
- Ajouter un arrière-plan d'écran de connexion et personnaliser le message de connexion.
- Désactiver l'avertissement informant l'utilisateur qu'aucun lecteur de cartes n'est connecté.

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server.
2. Dans la section Ecran de connexion, configurez les paramètres.

   Remarque : Pour plus d'informations sur chaque paramètre, reportez-vous à l'aide contextuelle.
3. Cliquez sur **Appliquer**.

Activation de la copie ou de la télécopie sans connexion

Si les options « Autoriser copie sans connexion » ou « Autoriser télécopie sans connexion » sont activées, procédez comme suit :

1. Dans Embedded Web Server, cliquez sur **Paramètres** ou **Configuration**.
2. Selon votre modèle d'imprimante, effectuez l'une des opérations suivantes :
   - Cliquez sur **Sécurité** > **Configuration de sécurité** > **Contrôles d'accès** > **Accès aux fonctions**.
   - Cliquez sur **Sécurité** > **Modifier les configurations de sécurité** > **Contrôles d'accès**.
3. Définissez la fonction de copie ou de télécopie sur **Pas de sécurité**.
4. Cliquez sur **Envoyer**.

Authentification basée sur l'imprimante

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

Configuration de l'authentification d'utilisateur basée sur l'imprimante

Avant de commencer, vérifiez les points suivants :

- Le contrôle d'accès App 1 ou Solution 1 s'applique à un modèle de sécurité de compte interne, LDAP+GSSAPI ou Active Directory.
- Le contrôle d'accès App 2 ou Solution 2 s'applique au modèle de sécurité de l'application.

  Remarque : Pour plus d'informations, reportez-vous à la section « Configuration des contrôles d'accès » à la page 6.

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server.
2. Depuis la section Ecran de connexion, définissez la méthode de connexion sur **Carte ou Connexion manuelle**.
3. Dans la section Authentification de l'utilisateur, procédez comme suit :
   - Définissez la validation de carte sur **Basée sur l'imprimante**.
   - Définissez le contrôle d'accès d'enregistrement de carte sur **App 1** ou **Solution 1**.

- Définissez le contrôle d'accès de connexion manuelle sur **App 1** ou **Solution 1**.
- Définissez le contrôle d'accès de session sur **App 2** ou **Solution 2**.

Remarques :

- Si le contrôle d'accès d'enregistrement de carte est défini sur **Aucun**, vous ne pouvez pas enregistrer votre carte sur l'imprimante.
- Si le contrôle d'accès de connexion manuelle est défini sur **Aucun**, la connexion nécessite uniquement une carte, même si la méthode de connexion est définie sur **Carte ou Connexion manuelle**.
- Pour plus d'informations sur chaque paramètre, reportez-vous à l'aide contextuelle.

4 Cliquez sur **Appliquer**.

Configuration du rôle de l'imprimante

Remarque : Une imprimante maître et une imprimante de sauvegarde sont nécessaires pour configurer une imprimante cliente.

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

2 Dans la section Validation de carte basée sur l'imprimante, choisissez le rôle de l'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.

3 Saisissez les noms d'hôte ou les adresses 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 **Appliquer**.

Authentification par service Web

Utilisez l'authentification par service Web lors de la validation des utilisateurs via un serveur LDD.

Configuration de l'authentification d'utilisateur par service Web

Avant de commencer, assurez-vous que le contrôle d'accès App 2 ou Solution 2 s'applique au modèle de sécurité de l'application. Pour plus d'informations, reportez-vous à la section « Configuration des contrôles d'accès » à la page 6.

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server.
2. Depuis la section Ecran de connexion, définissez Méthode de connexion sur **Carte ou Connexion manuelle**.
3. Dans la section Authentification de l'utilisateur, procédez comme suit :
   - Définissez Validation de carte sur **Service Web**.
   - Définissez Contrôle d'accès d'enregistrement de carte et Contrôle d'accès de connexion manuelle sur votre option de contrôle d'accès préférée.
   - Définissez Contrôle d'accès de session sur **App 2** ou **Solution 2**.

   Remarques :

   - Si Contrôle d'accès d'enregistrement de carte est défini sur **Aucun**, vous ne pouvez pas enregistrer votre carte sur l'imprimante.
   - Si Contrôle d'accès de connexion manuelle est défini sur **Aucun**, la connexion nécessite uniquement une carte, même si Méthode de connexion est défini sur **Carte ou Connexion manuelle**.
   - Pour plus d'informations sur chaque paramètre, reportez-vous à l'aide contextuelle.
4. 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.

   Remarque : Le paramètre Vérifier le certificat s'applique uniquement à la validation du service d'identification et du service Web.
5. Dans le menu Mode Vérification, sélectionnez **chaîne** ou **pair**.

   Remarque : La valeur par défaut est chaîne.
6. Chargez le Certificat SSL du serveur pour vous connecter au serveur de manière sécurisée.
7. 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.
8. Cliquez sur **Appliquer**.

Configuration des paramètres de service Web

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server.
2. Dans la section Paramètres de service Web, configurez les paramètres.

   Remarque : Pour plus d'informations sur chaque paramètre, reportez-vous à l'aide contextuelle.

3 Cliquez sur **Appliquer**.

Authentification par service d'identité

Utilisez l'authentification par service d'identité lors de la validation des utilisateurs via un serveur de service d'identité, tel que le serveur logiciel en tant que service (SaaS) LPM.

Configuration de l'authentification d'utilisateur par service d'identification

Avant de commencer, assurez-vous que le contrôle d'accès App 2 ou Solution 2 s'applique au modèle de sécurité de l'application. Pour plus d'informations, reportez-vous à la section « Configuration des contrôles d'accès » à la page 6.

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

2 Depuis la section Ecran de connexion, définissez Méthode de connexion sur **Carte ou Connexion manuelle**.

3 Dans la section Authentification de l'utilisateur, procédez comme suit :
   - Définissez Validation de carte sur **Service d'identification**.
   - Définissez Contrôle d'accès d'enregistrement de carte sur **Service d'identification**.
   - Définissez Contrôle d'accès de connexion manuelle sur **Service d'identification**.
   - Définissez Contrôle d'accès de session sur **App 2** ou **Solution 2**.

   Remarques :

   - Si Contrôle d'accès d'enregistrement de carte est défini sur **Aucun**, vous ne pouvez pas enregistrer votre carte sur l'imprimante.
   - Si Contrôle d'accès de connexion manuelle est défini sur **Aucun**, la connexion nécessite uniquement une carte, même si Méthode de connexion est défini sur **Carte ou Connexion manuelle**.
   - Pour plus d'informations sur chaque paramètre, reportez-vous à l'aide contextuelle.

4 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.

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

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

   Remarque : La valeur par défaut est chaîne.

6 Chargez le Certificat SSL du serveur pour vous connecter au serveur de manière sécurisée.

7 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.

8 Cliquez sur **Appliquer**.

Configuration des paramètres de service d'identité

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server.
2. Si nécessaire, dans la section Paramètres de service d'identité, sélectionnez **Activer l'écran de veille**.

   Remarque : Les imprimantes eSF version 2.x requièrent l'application eSF Security Manager lorsque l'option **Activer l'écran de veille** est désactivée. Pour voir une liste de ces imprimantes, consultez le fichier *Readme*.
3. Saisissez le nom d'hôte ou l'adresse IP du fournisseur de service d'identité.
4. Si nécessaire, saisissez le nom d'hôte ou l'adresse IP du fournisseur de services liés aux badges.
5. Téléchargez le certificat SSL du serveur pour vous connecter au serveur de manière sécurisée.
6. Si vous disposez d'un ID client et d'un secret client auprès de votre fournisseur de service d'identité, saisissez les informations dans les champs correspondants.
7. Définissez la stratégie d'accès à l'application.
   - **Continuer** : continuez à utiliser l'imprimante même si la connexion au serveur du service d'identité échoue.
   - **Echec** : revenez à l'écran de connexion si la connexion au serveur du service d'identité échoue.
8. 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.
9. Cliquez sur **Appliquer**.

authentification par code PIN

Configuration de l'authentification d'utilisateur par code PIN

Avant de commencer, assurez-vous que le contrôle d'accès App 2 ou Solution 2 s'applique au modèle de sécurité de l'application. Pour plus d'informations, reportez-vous à la section « Configuration des contrôles d'accès » à la page 6.

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server.
2. Depuis la section Ecran de connexion, définissez la méthode de connexion sur une option prenant en charge l'authentification par code PIN.
3. Dans la section Authentification de l'utilisateur, procédez comme suit :
   - Définissez la validation de carte sur votre méthode d'authentification préférée.
   - Définissez le contrôle d'accès d'enregistrement de carte sur votre option de contrôle d'accès préférée.
   - Définissez le contrôle d'accès par code PIN sur **App 1** ou **Solution 1**.
   - Définissez le contrôle d'accès de connexion manuelle sur votre option de contrôle d'accès préférée.
   - Définissez le contrôle d'accès de session sur **App 2** ou **Solution 2**.

   Remarques :

   - Si le contrôle d'accès par code PIN est défini sur **Aucun**, vous ne pouvez pas enregistrer votre code PIN sur l'imprimante.

- Pour plus d'informations sur chaque paramètre, reportez-vous à l'aide contextuelle.

4 Cliquez sur **Appliquer**.

Configuration des paramètres de code PIN

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

2 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.

3 Saisissez l'adresse du serveur Web, puis sélectionnez la longueur minimale du code PIN.

4 Saisissez les messages d'erreur signalant un code PIN non valide.

5 Cliquez sur **Appliquer**.

authentification LDAP

Utilisez l'authentification LDAP lors de la validation des utilisateurs via un serveur LDAP.

Configuration de l'authentification d'utilisateur LDAP

Avant de commencer, vérifiez les points suivants :

- Le contrôle d'accès App 2 ou Solution 2 s'applique au modèle de sécurité de l'application.
- Le contrôle d'accès App 3 ou Solution 3 s'applique à un modèle de sécurité LDAP.

  Remarque : Pour plus d'informations, reportez-vous à la section « Configuration des contrôles d'accès » à la page 6.

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

2 Depuis la section Ecran de connexion, définissez la méthode de connexion sur **Carte ou Connexion manuelle**.

3 Dans la section Authentification de l'utilisateur, procédez comme suit :
- Définissez la validation de carte sur **LDAP**.
- Définissez le contrôle d'accès d'enregistrement de carte sur **App 3** ou **Solution 3**.
- Définissez le contrôle d'accès de connexion manuelle sur **App 3** ou **Solution 3**.
- Définissez le contrôle d'accès de session sur **App 2** ou **Solution 2**.

  Remarques :

  - Si le contrôle d'accès d'enregistrement de carte est défini sur **Aucun**, vous ne pouvez pas enregistrer votre carte sur l'imprimante.
  - Si le contrôle d'accès de connexion manuelle est défini sur **Aucun**, la connexion nécessite uniquement une carte, même si la méthode de connexion est définie sur **Carte ou Connexion manuelle**.
  - Pour plus d'informations sur chaque paramètre, reportez-vous à l'aide contextuelle.

4 Cliquez sur **Appliquer**.

Configuration des paramètres LDAP

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server.
2. Dans la section Paramètres LDAP, configurez les paramètres.

   Remarques :

   - 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.
   - Pour plus d'informations sur chaque paramètre, reportez-vous à l'aide contextuelle.
3. Cliquez sur **Appliquer**.

Configuration des préférences de l'application

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server.
2. Essayez une ou plusieurs des solutions suivantes :
   - Pour personnaliser l'écran d'accueil de l'imprimante, configurez les paramètres de l'écran d'accueil.
   - Pour afficher les messages d'enregistrement, dans la section Paramètres avancés, sélectionnez **Afficher le message de début d'enregistrement**, puis **Afficher le message d'enregistrement terminé**.
   - Pour entendre un *bip* en cas de connexion réussie, dans la section Paramètres avancés, sélectionnez **Activer le bip de connexion réussie**, puis réglez sa fréquence.
   - Pour utiliser un profil en cas de connexion réussie, dans la section Paramètres avancés, tapez un nom de profil dans le champ Profil de connexion.

   Remarque : Pour plus d'informations sur chaque paramètre, reportez-vous à l'aide contextuelle.
3. Cliquez sur **Appliquer**.

Affichage des profils disponibles

1. Dans Embedded Web Server, cliquez sur **Paramètres** ou **Configuration**.
2. Cliquez sur **Gérer les raccourcis** > **Gérer les raccourcis profil**.

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.
2. Dans la section Paramètres avancés, sélectionnez **Utiliser le domaine sélectionné**.
3. Cliquez sur **Appliquer**.

Exportation ou importation d'un fichier de configuration

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server.
2. Exportez ou importez le fichier de configuration.

Remarques :

- Si l'erreur **JVM saturée** se produit, répétez la procédure d'exportation jusqu'à ce que le fichier de configuration soit enregistré.
- Si le délai expire et un écran vide apparaît, réactualisez le navigateur Web, puis cliquez sur **Appliquer**.

Gestion de l'application

Remarque : La page d'état de l'application est disponible uniquement lorsque vous utilisez l'authentification basée sur l'imprimante.

Accès à la page d'état de l'application

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

1. A partir d'Embedded Web Server, cliquez sur **Applications** > **Authentification par carte**.
2. Notez les informations suivantes :
   - **Etat** : présente l'état d'activité de l'imprimante.
     - **Non configurée** : l'imprimante n'a pas été configurée.
     - **Hors ligne** : aucune activité ou communication de l'imprimante n'est en cours.
     - **En ligne** : l'imprimante est active.
   - **Fonctionnement** : indique la 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** : indique la 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 comptes utilisateur et des imprimantes clientes

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

1. Accédez à la page d'état de l'application à partir d'Embedded Web Server.
2. Effectuez l'une des opérations suivantes :

Supprimer des comptes utilisateur

a Dans la section Maître, cliquez sur **Supprimer des utilisateurs**.

b Saisissez un ou plusieurs ID utilisateur, puis supprimez-les.

Ajouter des imprimantes clientes

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

b Saisissez une ou plusieurs adresses IP d'imprimante, puis ajoutez-les.

Supprimer des imprimantes clientes

Remarque : Vous ne pouvez pas supprimer des imprimantes clientes lorsque l'imprimante maître est hors ligne ou lorsque l'application est désinstallée.

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

b Cliquez sur **Supprimer des clientes**.

Réattribution des rôles d'imprimante

1 Configurez une nouvelle imprimante maître.

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

b Dans la section Validation de carte basée sur l'imprimante, définissez le rôle sur **Maître**.

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

d Cliquez sur **Appliquer**.

2 Attribuez l'imprimante de sauvegarde à la nouvelle imprimante maître.

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

b Dans la section Validation de carte basée sur l'imprimante, entrez le nom d'hôte ou l'adresse IP de la nouvelle imprimante maître.

c Cliquez sur **Appliquer**.

3 Supprimez l'imprimante cliente sur l'imprimante maître actuelle.

a Accédez à la page d'état de l'application à partir d'Embedded Web Server sur l'imprimante maître actuelle.

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

4 Réattribuez l'imprimante cliente à la nouvelle imprimante maître. Effectuez l'une des opérations suivantes :

Depuis 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.

b Dans la section Validation de carte basée sur l'imprimante, définissez le rôle sur **Cliente**.

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

Remarque : Vérifiez le nom d'hôte ou l'adresse IP de l'imprimante de sauvegarde.

d Cliquez sur **Appliquer**.

Depuis la page d'état de l'imprimante maître

a Accédez à la page d'état de l'application à partir d'Embedded Web Server sur la nouvelle imprimante maître.

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

c Saisissez l'adresse IP de l'imprimante cliente et ajoutez celle-ci.

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. Suivez les instructions qui s'affichent à l'écran.

Enregistrement d'un code PIN

Avant de commencer, assurez-vous que la méthode de connexion choisie prend en charge l'authentification par code PIN.

1. Dans le panneau de commandes de l'imprimante, appuyez sur **Connexion par code PIN**.
2. 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 : Lorsque 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 système

1. Dans Embedded Web Server, cliquez sur **Paramètres** ou **Configuration**.
2. Selon votre modèle d'imprimante, effectuez l'une des opérations suivantes :
   - Cliquez sur **Applications** > **Gestion des applications**.
   - Cliquez sur **Solutions pour l'appareil** > **Solutions (eSF)**.
   - Cliquez sur **Embedded Solutions**.
3. Cliquez sur **Système** > **Journal**.
4. Sélectionnez et soumettez les filtres appropriés.
5. Analysez le journal, puis résolvez le problème.

Contactez votre représentant Lexmark

L'application ne fonctionne pas avec la version mise à jour d'impression à la demande SaaS

Essayez les solutions suivantes :

Vérifiez que l'impression à la demande est correctement configurée

Si vous avez mis à niveau votre application Print Management SaaS vers l'impression à la demande version 2.0 ou ultérieure, assurez-vous de désactiver l'option Arrière-plan et écran de veille. Attribuez le contrôle d'accès d'authentification de carte à l'impression à la demande, puis vérifiez que l'impression à la demande est correctement configurée. Pour obtenir plus d'informations, reportez-vous au *Guide de l'administrateur de l'impression à la demande*.

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** ou **Configuration**.
2. Cliquez sur **Paramètres** > **Paramètres généraux**Délais.
3. Augmentez le délai d'affichage et de mode Veille.
4. Cliquez sur **Envoyer**.

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

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

Augmenter le délai de verrouillage et le nombre de tentatives de connexion autorisé

1. Selon votre modèle d'imprimante, depuis Embedded Web Server, effectuez l'une des opérations suivantes :
   - Cliquez sur **Paramètres** > **Sécurité** > **Divers paramètres de sécurité** > **Restrictions de connexion**.
   - Cliquez sur **Configuration** > **Sécurité**.
2. Augmentez le délai de verrouillage et le nombre de tentatives de connexion autorisé, ou le délai de déconnexion automatique.
3. Cliquez sur **Envoyer**.

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 17.

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

Pour plus d'informations, reportez-vous à la section « Configuration de l'authentification d'utilisateur basée sur l'imprimante » à la page 9.

Assurez-vous de ne pas enregistrer plus de 23 imprimantes clientes

Pour plus d'informations, reportez-vous à la section « Gestion des comptes utilisateur et des imprimantes clientes » à la page 17.

Contactez votre représentant Lexmark

Impossible de valider la carte

Essayez les solutions suivantes :

Définissez le mode de connexion sur Carte ou Connexion manuelle

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server.
2. Depuis la section Ecran de connexion, définissez la méthode de connexion sur **Carte ou Connexion manuelle**.
3. Cliquez sur **Appliquer**.

Contactez votre représentant Lexmark

Impossible de trouver les informations sur le domaine

Essayez les solutions suivantes :

Certaines méthodes de connexion pour la connexion manuelle ou l'enregistrement de carte, telles que par comptes locaux ou LDAP, ne nécessitent pas une sélection de domaine. Les méthodes de connexion qui nécessitent une sélection de domaine sont Kerberos, Active Directory et LDAP+GSSAPI.

Désactivez la sélection de domaine

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server.
2. Dans la section Paramètres avancés, décochez **Utiliser le domaine sélectionné**.
3. Cliquez sur **Appliquer**.

Modifiez la méthode de connexion

1. Accédez à la page de configuration de l'application à partir d'Embedded Web Server.
2. Dans la section Authentification de l'utilisateur, définissez le contrôle d'accès d'enregistrement de carte et le contrôle d'accès de connexion manuelle sur **App 1** ou **Solution 1**.

3 Cliquez sur **Appliquer**.

Contactez votre représentant Lexmark

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 des paramètres LDAP » à la page 15.

Contactez votre représentant Lexmark

Foire Aux Questions (FAQ)

Pourquoi ne puis-je pas ajouter ou supprimer une imprimante cliente lorsqu'une 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 et l'attribuer à sa nouvelle imprimante maître même si l'imprimante maître actuelle est hors ligne ?

Oui, pour cela, procédez comme suit :

1. Depuis Embedded Web Server, installez l'application sur l'imprimante cliente.
2. Attribuez-lui le rôle d'imprimante cliente, puis associez-la à l'imprimante maître et l'imprimante de sauvegarde. Pour plus d'informations, reportez-vous à la section « Configuration du rôle de l'imprimante » à la page 10.

Que faut-il faire si l'application a été désinstallée par erreur à partir de l'imprimante ?

1. Depuis Embedded Web Server, installez l'application.
2. Définissez un rôle pour l'imprimante. Pour plus d'informations, reportez-vous à la section « Configuration du rôle de l'imprimante » à la page 10.

   Remarque : Veillez à configurer consécutivement l'imprimante maître, l'imprimante de sauvegarde, puis les imprimantes clientes.
3. Configurez l'imprimante en fonction de son rôle.

   Remarques :

   - Si l'application est réinstallée sur une imprimante maître, attribuez celle-ci à son imprimante de sauvegarde.
   - Si l'application est réinstallée sur une imprimante de sauvegarde, attribuez celle-ci à son imprimante maître.
   - Si l'application est réinstallée sur une imprimante cliente, attribuez celle-ci à son imprimante maître et à son imprimante de sauvegarde.
   - Pour plus d'informations, reportez-vous à la section « Réattribution des rôles d'imprimante » à la page 18.

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

Définissez le contrôle d'accès aux fonctions de copie et de télécopie sur **Pas de sécurité**. Pour plus d'informations, reportez-vous à la section « Configuration de l'écran de connexion » à la page 9.

Que se passe-t-il si le contrôle d'accès de connexion manuelle et le contrôle d'accès de session ont les mêmes contrôles d'accès ?

Pour accéder aux fonctions de l'imprimante depuis l'écran d'accueil, vous devez entrer vos informations d'authentification lorsque vous vous connectez manuellement.

Puis-je définir des contrôles d'accès différents pour le contrôle d'accès de connexion manuelle et la validation de carte ?

Oui, sauf lorsque vous utilisez l'authentification par Service d'identité et définissez Contrôle d'accès de connexion manuelle et Validation de carte sur **Service d'identité**.

Pourquoi la fonction Connexion administrateur ne fonctionne-t-elle pas avec les comptes réseaux ?

La fonction **Connexion administrateur** est applicable uniquement pour les modèles de sécurité Comptes internes, Code PIN et Mot de passe.

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**.

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

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