



Lexmark™

Kartenauthentifizierung

Administratorhandbuch

Dezember 2020

www.lexmark.com

Inhalt

- Übersicht..... 4**
- Installieren erforderlicher Komponenten..... 5**
 - Zugriff auf den Embedded Web Server..... 5
 - Hinzufügen eines internen Benutzerkontos..... 5
 - Einrichten von Gruppen für interne Benutzerkonten..... 5
 - Erstellen einer Sicherheitsvorlage..... 6
 - Konfigurieren von Zugriffssteuerungen..... 6
- Konfigurieren der Anwendung..... 8**
 - Zugriff auf die Konfigurationsseite für die Anwendung..... 8
 - Konfigurieren der Administratorauthentifizierung..... 8
 - Konfigurieren des Anmeldebildschirms..... 9
 - Druckerbasierte Authentifizierung..... 9
 - Webdienst-Authentifizierung..... 11
 - Identitätsdienst-Authentifizierung..... 12
 - PIN-Authentifizierung..... 13
 - LDAP-Authentifizierung..... 14
 - Einrichten der Anwendungseinstellungen..... 15
 - Anzeigen von Bereichen für Benutzerkonten..... 15
 - Exportieren oder Importieren einer Konfigurationsdatei..... 16
- Verwalten der Anwendung..... 17**
 - Zugriff auf die Statusseite für die Anwendung..... 17
 - Verwalten von Benutzerkonten und Client-Druckern..... 17
 - Neuzuweisen der Druckerrollen..... 18
- Verwenden der Anwendung..... 20**
 - Registrieren von Benutzern..... 20
 - Registrieren einer PIN..... 20
 - Manuelle Anmeldung am Drucker..... 20
- Fehlerbehebung..... 21**

| | |
|-------------------------------------|-----------|
| Häufig gestellte Fragen..... | 25 |
| Hinweise..... | 27 |
| Index..... | 29 |

Übersicht

Verwenden Sie diese Anwendung, um Zugriff auf einen Drucker mit einem Kartenlesegerät sicherzustellen. Wenn Benutzer sich anmelden, werden ihre Anmeldeinformationen auf eine der folgenden Arten authentifiziert:

- Mit einem Masterdrucker. Wenn der Masterdrucker offline ist, übernimmt ein Backup-Drucker die Funktion eines Masterdruckers, bis dieser Drucker wieder online ist.

Hinweis: Stellen Sie beim Einrichten der Drucker sicher, dass diese auf dem gleichen Netzwerk liegen.

- Entweder mit dem Lightweight Directory Access Protocol (LDAP), den Lexmark™ Document Distributor (LDD) Servern oder den Identitätsserviceanbietern, je nach von der Organisation festgelegten Authentifizierung.

Dieses Dokument bietet Anleitungen zu Konfiguration und Verwendung der Anwendung sowie zur Fehlerbehebung dafür.

Installieren erforderlicher Komponenten

Zur Konfiguration der Anwendung benötigen Sie möglicherweise Administratorrechte.

Zugriff auf den Embedded Web Server

- 1 Suchen Sie die IP-Adresse des Druckers. Führen Sie einen der folgenden Schritte aus:
 - Suchen Sie die IP-Adresse des Druckers auf dem Startbildschirm des Druckers.
 - Zeigen Sie die IP-Adresse im Abschnitt "TCP/IP" des Menüs "Netzwerk/Anschlüsse" an.
- 2 Öffnen Sie einen Webbrowser, und geben Sie die IP-Adresse des Druckers ein.

Hinzufügen eines internen Benutzerkontos

Bei Verwendung einer druckerbasierten Authentifizierung ist ein internes Benutzerkonto erforderlich.

- 1 Klicken Sie im Embedded Web Server auf **Einstellungen** oder **Konfiguration**.
- 2 Führen Sie je nach Druckermodell einen der folgenden Schritte aus:
 - Klicken Sie auf **Sicherheit > Sicherheitseinstellung > Interne Konten > Hinzufügen eines internen Kontos**.
 - Klicken Sie auf **Sicherheit > Sicherheitseinstellungen bearbeiten > Interne Konten > Hinzufügen eines internen Kontos**.
- 3 Geben Sie die Kontoinformationen ein, und klicken Sie dann auf **Senden**.
- 4 Geben Sie bei Bedarf im Bereich "Verwalten der internen Konten" einen benutzerdefinierten Bausteinnamen ein, und geben Sie dann die erforderlichen Benutzeranmeldeinformationen ein.
- 5 Klicken Sie auf **Übernehmen**.

Einrichten von Gruppen für interne Benutzerkonten

- 1 Klicken Sie im Embedded Web Server auf **Einstellungen** oder **Konfiguration**.
- 2 Führen Sie je nach Druckermodell einen der folgenden Schritte aus:
 - Klicken Sie auf **Sicherheit > Sicherheitseinrichtung > Interne Konten > Einrichten von Gruppen für interne Benutzerkonten**.
 - Klicken Sie auf **Sicherheit > Sicherheitseinrichtungen bearbeiten > Interne Konten > Einrichten von Gruppen für interne Benutzerkonten**.
- 3 Geben Sie einen Gruppennamen ein und klicken Sie anschließend auf **Hinzufügen**.
- 4 Fügen Sie der Gruppe interne Konten hinzu.
- 5 Klicken Sie auf **Übernehmen**.

Erstellen einer Sicherheitsvorlage

Eine Sicherheitsvorlage besteht aus Sicherheitsbausteinen, z. B. interne Konten, Kerberos, LDAP, LDAP+GSSAPI und Active Directory. Diese Vorlagen werden für die Zugriffssteuerung auf Sicherheitsdruckerfunktionen und -anwendungen angewendet.

- 1 Klicken Sie im Embedded Web Server auf **Einstellungen** oder **Konfiguration**.
- 2 Führen Sie je nach Druckermodell einen der folgenden Schritte aus:
 - Klicken Sie auf **Sicherheit > Sicherheitseinstellung > Sicherheitsvorlage > Hinzufügen einer Sicherheitsvorlage**.
 - Klicken Sie auf **Sicherheit > Sicherheitseinstellungen bearbeiten > Sicherheitsvorlagen > Hinzufügen einer Sicherheitsvorlage**.
- 3 Geben Sie einen Name für die Sicherheitsvorlage ein, und wählen Sie anschließend eine der folgenden Authentifizierungs-Installationen:
 - Für eine druckerbasierte Authentifizierung bei einer eigenständigen Installation wählen Sie einen Baustein "Internes Konto".
 - Für eine druckerbasierte Authentifizierung mit Lexmark Print Management (LPM) Serverloser Print Release in einer Active Directory-Installation wählen Sie einen LDAP+GSSAPI-Baustein.
 - Für eine LDAP-Authentifizierung wählen Sie einen LDAP-Baustein.
- 4 Klicken Sie auf **Vorlage speichern**.

Hinweis: Um eine vorhandene Sicherheitsvorlage zu ändern, klicken Sie auf die Sicherheitsvorlage und fügen Sie dann eine Berechtigung für die Vorlage hinzu oder ändern Sie diese.

Konfigurieren von Zugriffssteuerungen

Hinweis: Wenn Sie die Funktion **Administratoranmeldung** verwenden, stellen Sie sicher, dass Sie die Sicherheitsvorlage für interne Accounts konfiguriert haben. Weitere Informationen finden Sie unter ["Erstellen einer Sicherheitsvorlage" auf Seite 6](#).

- 1 Klicken Sie im Embedded Web Server auf **Einstellungen** oder **Konfiguration**.
- 2 Führen Sie je nach Druckermodell einen der folgenden Schritte aus:
 - Klicken Sie auf **Sicherheit > Sicherheitseinstellung > Zugriffssteuerungen**.
 - Klicken Sie auf **Sicherheit > Sicherheitseinstellungen bearbeiten > Zugriffssteuerungen**.
- 3 Klicken Sie auf **Geräte-Apps** oder **Gerätelösungen**, und gehen Sie wie folgt vor:
 - Legen Sie für App 1 oder Lösung 1 ein internes Konto oder LDAP+GSSAPI- oder Active Directory-Sicherheitsvorlage fest.
 - Legen Sie für App 2 oder Lösung 2 die Sicherheitsvorlage der Anwendung fest.

Hinweis: Die Sicherheitsvorlage der Anwendung ist die Vorlage mit CardAuth als Authentifizierungskonfiguration. Weitere Informationen finden Sie unter ["Erstellen einer Sicherheitsvorlage" auf Seite 6](#).
 - Legen Sie für App 3 oder Lösung 3 die LDAP-Sicherheitsvorlage fest.

Hinweise:

- Wenn LPM Print Release installiert ist, dann legen Sie für die Zugriffssteuerung von Print Release die Sicherheitsvorlage der Anwendung fest.

- Drucker mit Embedded Solutions Framework (eSF) Version 2.x benötigen den eSF-Sicherheitsmanager, um die Zugriffssteuerung zu konfigurieren. Eine Liste dieser Drucker finden Sie in der *Readme*-Datei.

4 Klicken Sie auf **Übernehmen**.

Konfigurieren der Anwendung

Führen Sie vor Beginn Folgendes aus:

- Deaktivieren Sie "Hintergrund und inaktiver Bildschirm" und jede bestehende Authentifizierungsanwendung.
- Installieren Sie Folgendes:
 - Installationsprogramm für Kartenauthentifizierung
 - Kartenlesertreiber
 - Kartenleser
 - eSF Sicherheits-Manager

Hinweis: Drucker mit eSF-Version 2.x benötigen den eSF-Sicherheitsmanager, um die Zugriffssteuerung zu konfigurieren. Eine Liste dieser Drucker finden Sie in der *Readme*-Datei.

Zugriff auf die Konfigurationsseite für die Anwendung

- 1 Klicken Sie im Embedded Web Server auf **Einstellungen** oder **Konfiguration**.
- 2 Führen Sie je nach Druckermodell einen der folgenden Schritte aus:
 - Klicken Sie auf **Apps > Apps-Management**.
 - Klicken Sie auf **Gerätelösungen > Lösungen (eSF)**.
 - Klicken Sie auf **Embedded Solutions**.
- 3 Klicken Sie auf **Kartenauthentifizierung > Konfigurieren**.

Konfigurieren der Administratorauthentifizierung

Hinweis: Wenn Sie die Funktion **Administratoranmeldung** verwenden, stellen Sie sicher, dass Sie die Sicherheitsvorlage für interne Accounts, PIN und Kennwort konfiguriert haben. Weitere Informationen finden Sie unter ["Erstellen einer Sicherheitsvorlage" auf Seite 6](#).

- 1 Greifen Sie über Embedded Web Server auf die Konfigurationsseite der Anwendung zu.
- 2 Legen Sie die **Zugangskontrolle für Administratoranmeldung** im Abschnitt Benutzerauthentifizierung als Ihre bevorzugte Anmeldemethode fest.

Hinweise:

- Stellen Sie sicher, dass die ausgewählte Zugangskontrolle mit einer Sicherheitsvorlage konfiguriert ist. Weitere Informationen finden Sie unter ["Erstellen einer Sicherheitsvorlage" auf Seite 6](#).
- Wenn Sie **Deaktiviert** wählen, wird die Option **Administratoranmeldung** im Bedienfeld ausgeblendet.

- 3 Klicken Sie auf **Übernehmen**.

Konfigurieren des Anmeldebildschirms

Zum Konfigurieren des Anmeldebildschirms gehen Sie wie folgt vor:

- Benutzern erlauben die Kopie- und Faxfunktionen ohne Anmeldung zu verwenden.
- Benutzern erlauben die zu verwendende Anmeldungsmethode auszuwählen.
- Fügen Sie einen Anmeldehintergrund hinzu, und passen Sie die Anmeldemeldung an.
- Deaktivieren Sie die Warnung, wenn kein Kartenleser angeschlossen ist.

1 Greifen Sie über Embedded Web Server auf die Konfigurationsseite der Anwendung zu.

2 Konfigurieren Sie im Abschnitt Anmeldebildschirm die Einstellungen.

Hinweis: Weitere Informationen zu den einzelnen Einstellungen finden Sie in der jeweiligen QuickInfo.

3 Klicken Sie auf **Übernehmen**.

Aktivieren von Kopieren und Faxen ohne Anmeldung

Wenn Kopieren ohne Anmeldung erlauben oder Faxen ohne Anmeldung erlauben aktiviert ist, gehen Sie wie folgt vor:

1 Klicken Sie im Embedded Web Server auf **Einstellungen** oder **Konfiguration**.

2 Führen Sie je nach Druckermodell einen der folgenden Schritte aus:

- Klicken Sie auf **Sicherheit** > **Sicherheitsinstallation** > **Zugriffsteuerungen** > **Funktionszugriff**.
- Klicken Sie auf **Sicherheit** > **Sicherheitseinstellungen bearbeiten** > **Zugriffssteuerungen**.

3 Legen Sie für die Kopier- oder Faxfunktion **Keine Sicherheit** fest.

4 Klicken Sie auf **Übernehmen**.

Druckerbasierte Authentifizierung

Verwenden Sie eine druckerbasierte Authentifizierung, wenn Sie Benutzer über einen Masterdrucker prüfen.

Konfigurieren der druckerbasierten Benutzerauthentifizierung

Stellen Sie zu Beginn Folgendes sicher:

- Für die Zugriffssteuerung für App 1 oder Lösung 1 ist ein internes Konto oder eine LDAP+GSSAPI- oder Active Directory-Sicherheitsvorlage festgelegt.
- Die Zugriffssteuerung für App 2 oder Lösung 2 ist auf die Sicherheitsvorlage der Anwendung festgelegt.

Hinweis: Weitere Informationen finden Sie unter ["Konfigurieren von Zugriffssteuerungen"](#) auf Seite 6.

1 Greifen Sie über Embedded Web Server auf die Konfigurationsseite der Anwendung zu.

2 Legen Sie im Bereich "Anmeldebildschirm" die Anmeldemethode als **Karte oder Manuelle Anmeldung** fest.

3 Gehen Sie im Abschnitt "Benutzerauthentifizierung" wie folgt vor:

- Legen Sie für die Kartvalidierung **Druckerbasiert** fest.
- Legen Sie die Zugriffssteuerung für die Kartenregistrierung auf **App 1** oder **Lösung 1** fest.

- Legen Sie die Zugriffssteuerung für die Manuelle Anmeldung auf **App 1** oder **Lösung 1** fest.
- Legen Sie die Zugriffssteuerung für die Sitzung auf **App 2** oder **Lösung 2** fest.

Hinweise:

- Wenn die Zugriffssteuerung der Kartenregistrierung auf **Keine** eingestellt ist, dann können Sie Ihre Karte nicht am Drucker registrieren.
- Die Einstellung der Zugriffssteuerung für Manuelle Anmeldung auf **Keine** erfordert lediglich eine Karte für die Anmeldung, selbst wenn die Anmeldemethode auf **Karte oder Manuelle Anmeldung** festgelegt ist.
- Weitere Informationen zu den einzelnen Einstellungen finden Sie in der jeweiligen QuickInfo.

4 Klicken Sie auf **Übernehmen**.

Einrichten der Rolle für den Drucker

Hinweis: Ein Client-Drucker erfordert einen Masterdrucker und einen Backup-Drucker.

- 1** Greifen Sie über Embedded Web Server auf die Konfigurationsseite der Anwendung zu.
- 2** Wählen Sie im Abschnitt "Druckerbasierte Kartenüberprüfung" eine Rolle für den Drucker aus.
 - **Master** – Dieser Drucker verwaltet die Liste der registrierten Benutzer.
 - **Backup** – Wenn der Masterdrucker offline ist, übernimmt der Backup-Drucker die Rolle des Masterdruckers, bis dieser wieder online ist.
 - **Client** – Dieser Drucker speichert keine Benutzerinformationen. Ein Master- oder Backup-Drucker ist zur Überprüfung von Benutzeranmeldeinformationen erforderlich.

Hinweise:

- Wenn Sie nur einen Drucker haben, legen Sie diesen als Masterdrucker fest.
- Wenn Sie zwei Drucker haben, legen Sie einen als Masterdrucker und den anderen als Backup-Drucker fest.
- Wenn Sie drei oder mehr Drucker haben, können Sie einen als Masterdrucker, einen als Backup-Drucker und die übrigen als Client-Drucker festlegen.

3 Geben Sie die Host-Namen oder die IP-Adressen des Masterdruckers und des Backup-Druckers ein.

Hinweise:

- Beim Einrichten eines Backup-Druckers sind der Host-Name oder die IP-Adresse des Masterdruckers erforderlich.
- Beim Einrichten von Client-Druckern sind die Host-Namen oder die IP-Adressen des Masterdruckers und des Backup-Druckers erforderlich.
- Bevor Sie einen Client-Drucker einem neuen Masterdrucker zuweisen, löschen Sie den Client-Drucker vom alten Masterdrucker.

4 Klicken Sie auf **Übernehmen**.

Webdienst-Authentifizierung

Verwenden Sie die Authentifizierung per Webdienst, wenn Sie Benutzer über einen LDD-Server überprüfen.

Konfigurieren der Benutzerauthentifizierung für den Webdienst

Stellen Sie zunächst sicher, dass die Zugriffssteuerung für App 2 oder Lösung 2 auf die Sicherheitsvorlage der Anwendung festgelegt ist. Weitere Informationen finden Sie unter "[Konfigurieren von Zugriffssteuerungen](#)" auf [Seite 6](#).

- 1 Greifen Sie über Embedded Web Server auf die Konfigurationsseite der Anwendung zu.
- 2 Legen Sie im Bereich Anmeldebildschirm die Anmeldemethode als **Karte oder manuelle Anmeldung** fest.
- 3 Gehen Sie im Abschnitt Benutzerauthentifizierung wie folgt vor:
 - Legen Sie für die Kartenüberprüfung **Webdienst** fest.
 - Legen Sie für die Zugriffssteuerung für die Kartenregistrierung und Zugriffssteuerung für die manuelle Anmeldung Ihre bevorzugte Zugriffssteuerung fest.
 - Legen Sie die Zugriffssteuerung für die Sitzung auf **App 2** oder **Lösung 2** fest.

Hinweise:

- Wenn die Zugriffssteuerung für die Kartenregistrierung auf **Keine** eingestellt ist, dann können Sie Ihre Karte nicht am Drucker registrieren.
 - Die Einstellung der Zugriffssteuerung für die manuelle Anmeldung auf **Keine** erfordert lediglich eine Karte für die Anmeldung, selbst wenn die Anmeldemethode auf **Karte oder Manuelle Anmeldung** festgelegt ist.
 - Weitere Informationen zu den einzelnen Einstellungen finden Sie in der jeweiligen QuickInfo.
- 4 Wählen Sie **Zertifikat überprüfen**, um alle Verbindungen zum Server zu validieren. Wenn Zertifikat überprüfen nicht ausgewählt ist, wird CA nicht validiert.

Hinweis: Die Einstellung Zertifikat überprüfen gilt nur für die Validierung des Identitäts-Service und des Webdienstes.

- 5 Wählen Sie im Menü Verifizierungsmodus entweder **Kette** oder **Peer**.

Hinweis: Der Standardwert lautet Kette.

- 6 Laden Sie das SSL-Zertifikat des Servers hoch, um sich sicher mit dem Server zu verbinden.
- 7 Geben Sie im Feld Hosts prüfen die zusätzlichen Hostnamen ein (andere als die Standard-Server-URL), um die Einträge im Zertifikat zu überprüfen. Verwenden Sie Kommas, um mehrere Hostnamen zu trennen.

Hinweis: Standardmäßig enthält diese weiße Liste nur die Server-URL. Geben Sie zusätzliche Hostnamen in das Feld Hosts prüfen ein, um sie in die weiße Liste aufzunehmen.

- 8 Klicken Sie auf **Übernehmen**.

Konfigurieren der Einstellungen für Webdienst

- 1 Greifen Sie über Embedded Web Server auf die Konfigurationsseite der Anwendung zu.
- 2 Konfigurieren Sie im Abschnitt "Webdienst-Einstellungen" die Einstellungen.

Hinweis: Weitere Informationen zu jeder Einstellung erhalten Sie in der jeweiligen QuickInfo.

3 Klicken Sie auf **Übernehmen**.

Identitätsdienst-Authentifizierung

Verwenden Sie die Identitätsdienst-Authentifizierung, wenn Sie Benutzer über einen Identitätsdienstserver, z. B. LPM-Software, als einen Dienste- (SaaS) Server überprüfen.

Konfigurieren der Benutzerauthentifizierung für Identitätsdienst

Stellen Sie zunächst sicher, dass die Zugriffssteuerung für App 2 oder Lösung 2 auf die Sicherheitsvorlage der Anwendung festgelegt ist. Weitere Informationen finden Sie unter ["Konfigurieren von Zugriffssteuerungen"](#) auf [Seite 6](#).

- 1** Greifen Sie über Embedded Web Server auf die Konfigurationsseite der Anwendung zu.
- 2** Legen Sie im Bereich Anmeldebildschirm die Anmeldemethode als **Karte oder manuelle Anmeldung** fest.
- 3** Gehen Sie im Abschnitt Benutzerauthentifizierung wie folgt vor:
 - Legen Sie für die Kartenüberprüfung **Identitätsdienst** fest.
 - Legen Sie die Zugriffssteuerung für die Kartenregistrierung auf **Identitätsdienst** fest.
 - Legen Sie die Zugriffsteuerung für die manuelle Anmeldung auf **Identitätsdienst** fest.
 - Legen Sie die Zugriffssteuerung für die Sitzung auf **App 2** oder **Lösung 2** fest.

Hinweise:

- Wenn die Zugriffssteuerung für die Kartenregistrierung auf **Keine** eingestellt ist, dann können Sie Ihre Karte nicht am Drucker registrieren.
 - Die Einstellung der Zugriffssteuerung für die manuelle Anmeldung auf **Keine** erfordert lediglich eine Karte für die Anmeldung, selbst wenn die Anmeldemethode auf **Karte oder Manuelle Anmeldung** festgelegt ist.
 - Weitere Informationen zu den einzelnen Einstellungen finden Sie in der jeweiligen QuickInfo.
- 4** Wählen Sie **Zertifikat überprüfen**, um alle Verbindungen zum Server zu validieren. Wenn Zertifikat überprüfen nicht ausgewählt ist, wird CA nicht validiert.

Hinweis: Die Einstellung Zertifikat überprüfen gilt nur für die Validierung des Identitäts-Service und des Webdienstes.

- 5** Wählen Sie im Menü Verifizierungsmodus entweder **Kette** oder **Peer**.

Hinweis: Der Standardwert lautet Kette.

- 6** Laden Sie das SSL-Zertifikat des Servers hoch, um sich sicher mit dem Server zu verbinden.

- 7** Geben Sie im Feld Hosts prüfen die zusätzlichen Hostnamen ein (andere als die Standard-Server-URL), um die Einträge im Zertifikat zu überprüfen. Verwenden Sie Kommas, um mehrere Hostnamen zu trennen.

Hinweis: Standardmäßig enthält diese weiße Liste nur die Server-URL. Geben Sie zusätzliche Hostnamen in das Feld Hosts prüfen ein, um sie in die weiße Liste aufzunehmen.

- 8** Klicken Sie auf **Übernehmen**.

Konfigurieren der Einstellungen des Identitätsdienstes

- 1 Greifen Sie über Embedded Web Server auf die Konfigurationsseite der Anwendung zu.
- 2 Wählen Sie bei Bedarf im Bereich der Identitätsdiensteinstellungen **Inaktiven Bildschirm aktivieren**.
Hinweis: Drucker mit eSF-Version 2.x benötigen einen eSF-Sicherheits-Manager, wenn **Inaktiven Bildschirm aktivieren** deaktiviert ist. Eine Liste dieser Drucker finden Sie in der *Readme*-Datei.
- 3 Geben Sie den Hostnamen oder die IP-Adresse des Identitätsdiensteanbieters ein.
- 4 Geben Sie bei Bedarf den Hostnamen oder die IP-Adresse des Kennkartendiensteanbieters ein.
- 5 Laden Sie das SSL-Zertifikat des Servers hoch, um sich sicher mit dem Server zu verbinden.
- 6 Wenn Sie eine Client-ID und ein Client-Secret vom Identitätsdiensteanbieter haben, dann geben Sie die Informationen in die entsprechenden Felder ein.
- 7 Legen Sie die Richtlinie für den Anwendungszugriff fest.
 - **Fortfahren** – Der Drucker kann weiterhin verwendet werden, auch wenn die Verbindung zum Server des Identitätsdienstes nicht hergestellt werden konnte.
 - **Fehlgeschlagen** – Zum Anmeldebildschirm zurückkehren, auch wenn die Verbindung zum Server des Identitätsdienstes nicht hergestellt werden konnte.
- 8 Um Benutzern das Anmelden am Drucker mit einem separaten Service-Konto zu ermöglichen, wählen Sie **Service-Konto verwenden** und geben Sie dann die Benutzerinformationen für das Service-Konto ein.
- 9 Klicken Sie auf **Übernehmen**.

PIN-Authentifizierung

Konfigurieren der PIN-Benutzerauthentifizierung

Stellen Sie zunächst sicher, dass die Zugriffssteuerung für App 2 oder Lösung 2 auf die Sicherheitsvorlage der Anwendung festgelegt ist. Weitere Informationen finden Sie unter ["Konfigurieren von Zugriffssteuerungen" auf Seite 6](#).

- 1 Greifen Sie über Embedded Web Server auf die Konfigurationsseite der Anwendung zu.
- 2 Legen Sie im Anmeldebildschirm für die Anmeldemethode eine Option fest, die PIN Authentifizierung unterstützt.
- 3 Gehen Sie im Abschnitt "Benutzerauthentifizierung" wie folgt vor:
 - Legen Sie für die Kartenüberprüfung Ihre bevorzugte Authentifizierungsmethode fest.
 - Legen Sie für die Kartenregistrierung Ihre bevorzugte Zugriffssteuerung fest.
 - Legen Sie für die PIN-Zugriffssteuerung **App 1** oder **Lösung 1** fest.
 - Legen Sie für die Manuelle Anmeldung Ihre bevorzugte Zugriffssteuerung fest.
 - Legen Sie die Zugriffssteuerung für die Sitzung auf **App 2** oder **Lösung 2** fest.

Hinweise:

- Wenn die PIN-Zugriffssteuerung auf **Keine** eingestellt ist, dann können Sie Ihre PIN nicht am Drucker registrieren.

- Weitere Informationen zu den einzelnen Einstellungen finden Sie in der jeweiligen QuickInfo.

4 Klicken Sie auf **Übernehmen**.

Konfigurieren der PIN-Einstellungen

- 1** Greifen Sie über den Embedded Web Server auf die Konfigurationsseite der Anwendung zu.
- 2** Wählen Sie im Abschnitt PIN-Einstellungen im Menü Erforderliche Anmeldeinformationen eine Anmeldeinformation aus.
 - Benutzer-ID und PIN – erfordert einen Benutzernamen und eine PIN für die Authentifizierung.
 - Nur PIN: erfordert eine PIN für die Authentifizierung.
- 3** Geben Sie die Web-Serveradresse ein, und wählen Sie dann die minimale PIN-Länge.
- 4** Geben Sie die Fehlermeldungen für eine ungültige PIN ein.
- 5** Klicken Sie auf **Übernehmen**.

LDAP-Authentifizierung

Verwenden Sie die LDAP-Authentifizierung, wenn Sie Benutzer über einen LDAP-Server überprüfen.

Konfigurieren der LDAP-Benutzerauthentifizierung

Stellen Sie zu Beginn Folgendes sicher:

- Die Zugriffssteuerung für App 2 oder Lösung 2 ist auf die Sicherheitsvorlage der Anwendung festgelegt.
- Die Zugriffssteuerung für App 3 oder Lösung 3 ist auf die LDAP-Sicherheitsvorlage festgelegt.

Hinweis: Weitere Informationen finden Sie unter "[Konfigurieren von Zugriffssteuerungen](#)" auf Seite 6.

- 1** Greifen Sie über Embedded Web Server auf die Konfigurationsseite der Anwendung zu.
- 2** Legen Sie im Bereich "Anmeldebildschirm" die Anmeldeinformation als **Karte oder Manuelle Anmeldung** fest.
- 3** Gehen Sie im Abschnitt "Benutzerauthentifizierung" wie folgt vor:
 - Legen Sie für die Kartenvalidierung **LDAP** fest.
 - Legen Sie die Zugriffssteuerung für die Kartenregistrierung auf **App 3** oder **Lösung 3** fest.
 - Legen Sie die Zugriffssteuerung für die Manuelle Anmeldung auf **App 3** oder **Lösung 3** fest.
 - Legen Sie die Zugriffssteuerung für die Sitzung auf **App 2** oder **Lösung 2** fest.

Hinweise:

- Wenn die Zugriffssteuerung der Kartenregistrierung auf **Keine** eingestellt ist, dann können Sie Ihre Karte nicht am Drucker registrieren.
- Die Einstellung der Zugriffssteuerung für Manuelle Anmeldung auf **Keine** erfordert lediglich eine Karte für die Anmeldung, selbst wenn die Anmeldeinformation auf **Karte oder Manuelle Anmeldung** festgelegt ist.
- Weitere Informationen zu den einzelnen Einstellungen finden Sie in der jeweiligen QuickInfo.

4 Klicken Sie auf **Übernehmen**.

Konfigurieren der LDAP-Einstellungen

- 1 Greifen Sie über Embedded Web Server auf die Konfigurationsseite der Anwendung zu.
- 2 Konfigurieren Sie im Abschnitt "LDAP-Einstellungen" die Einstellungen.

Hinweise:

- Wenn **Adressbuch verwenden** ausgewählt ist, verwendet die Anwendung die in den Drucker-Netzwerkkonten konfigurierten LDAP-Einstellungen.
- Weitere Informationen zu den einzelnen Einstellungen finden Sie in der jeweiligen QuickInfo.

- 3 Klicken Sie auf **Übernehmen**.

Einrichten der Anwendungseinstellungen

- 1 Greifen Sie über Embedded Web Server auf die Konfigurationsseite der Anwendung zu.
- 2 Führen Sie eine oder mehrere der folgenden Methoden aus:
 - Zum Anpassen des Drucker-Startbildschirms konfigurieren Sie die Einstellungen des Startbildschirms.
 - Zum Anzeigen von Registrierungsmeldungen aus den "Erweiterten Einstellungen" wählen Sie **Meldung der Registrierungseinführung anzeigen** und **Meldung des Registrierungsabschlusses anzeigen**.
 - Für ein *akustisches Signal* nach einem erfolgreichen Login wählen Sie im Bereich "Erweiterte Einstellungen" **Signalton für erfolgreiche Anmeldung aktivieren**, und passen Sie dann die Signaltonfrequenz an.
 - Für die Verwendung eines Profils nach einer erfolgreichen Anmeldung geben Sie im Abschnitt "Erweiterte Einstellungen" in das Feld "Anmeldeprofil" einen Profilnamen ein.

Hinweis: Weitere Informationen zu den einzelnen Einstellungen finden Sie in der jeweiligen QuickInfo.

- 3 Klicken Sie auf **Übernehmen**.

Anzeigen verfügbarer Profile

- 1 Klicken Sie im Embedded Web Server auf **Einstellungen** oder **Konfiguration**.
- 2 Klicken Sie auf **Kurzwahlen verwalten** > **Profil-Kurzwahlnummern verwalten**.

Anzeigen von Bereichen für Benutzerkonten

Die Funktion "Ausgewählte Bereich verwenden" ist nur anwendbar, wenn für die Kartenregistrierung und die manuelle Anmeldung Kerberos, Active Directory oder LDAP+GSSAPI als Anmeldemethoden verwendet werden. Diese Funktion ist ebenfalls nur anwendbar, wenn Kartenvalidierung auf "Web-Service" oder "Druckerbasiert" festgelegt ist.

Wenn diese Funktion aktiv ist, ist bei der Kartenregistrierung die registrierte Kennkartenkennung im Format "benutzername@bereich".

Wenn diese Funktion aktiv ist, ist bei der manuellen Anmeldung der im Druckerbedienfeld angezeigte Name im Format "benutzername@bereich".

Diese Einstellungen gelten nicht für "PIN-Anmeldung" und "PIN-Registrierung".

Um diese Funktion zu aktivieren, gehen Sie wie folgt vor:

- 1 Greifen Sie über Embedded Web Server auf die Konfigurationsseite der Anwendung zu.
- 2 Wählen Sie im Bereich "Erweiterte Einstellungen" die Option **Ausgewählten Bereich verwenden**.
- 3 Klicken Sie auf **Übernehmen**.

Exportieren oder Importieren einer Konfigurationsdatei

- 1 Greifen Sie über Embedded Web Server auf die Konfigurationsseite der Anwendung zu.
- 2 Exportieren oder importieren Sie die Konfigurationsdatei.

Hinweise:

- Wenn ein **JVM-Fehler aufgrund von zu wenig Arbeitsspeicher** aufgetreten ist, müssen Sie den Exportprozess wiederholen, bis die Konfigurationsdatei gespeichert wurde.
- Wenn eine Zeitüberschreitung auftritt oder ein leerer Bildschirm angezeigt wird, müssen Sie den Webbrowser aktualisieren und anschließend auf **Anwenden** klicken.

Verwalten der Anwendung

Hinweis: Die Statusseite für die Anwendung ist nur verfügbar, wenn die druckerbasierte Authentifizierung verwendet wird.

Zugriff auf die Statusseite für die Anwendung

Verwenden Sie die Statusseite zur Überwachung der Druckeraktivität.

- 1 Klicken Sie im Embedded Web Server auf **Anwendungen > Kartenauthentifizierung**.
- 2 Beachten Sie folgende Informationen:
 - **Status** – Zeigt den Aktivitätsstatus des Druckers an.
 - **Nicht konfiguriert** – Der Drucker wurde nicht konfiguriert.
 - **Offline** – Es wird keine Druckeraktivität oder Kommunikation ausgeführt.
 - **Online** – Der Drucker ist aktiv.
 - **Betriebszeit** – Zeigt an, wie lange die Anwendung bereits ausgeführt wird.
 - **(dieser Drucker)** – Der aktuelle Drucker.
 - **Letzte Aktivität** – Die letzte Aktivität des Masterdruckers.
 - **Benutzeranzahl** – Die Gesamtanzahl der registrierten Benutzer.
 - **Registrierungsstatus** – Gibt an, ob der Drucker offline oder online ist.
 - **Letzte Synchronisierung mit Master** – Das letzte Mal, dass der Backup-Drucker über den Master aktualisiert wurde.
 - **Letzter Kontakt mit Master** – Das letzte Mal, dass der Backup-Drucker mit dem Master kommuniziert hat.
 - **Letzte Synchronisierung als Master** – Das letzte Mal, dass der Backup-Drucker als Master fungiert hat.
 - **Letzte Aktivität als Master** – Die letzte Aktivität des Backup-Druckers als Master.
 - **Dauer als Master** – Zeigt an, wie lange der Backup-Drucker als Master fungiert hat.
 - **Momentan bedient durch** – Der Client-Drucker, der kürzlich Kontakt mit dem Master- oder Backup-Drucker hatte.
 - **Letzte Aktivität mit Backup** – Das letzte Mal, dass der Client-Drucker mit dem Backup-Drucker Kontakt hatte.

Verwalten von Benutzerkonten und Client-Druckern

Hinweis: Diese Funktion wird nur angezeigt, wenn ein Drucker als Masterdrucker fungiert.

- 1 Greifen Sie über Embedded Web Server auf die Statusseite der Anwendung zu.
- 2 Gehen Sie wie folgt vor:

Löschen von Benutzerkonten

- a Klicken Sie im Abschnitt "Master" auf **Benutzer löschen**.
- b Geben Sie eine oder mehrere Benutzer-IDs ein, und löschen Sie diese anschließend.

Client-Drucker hinzufügen

- a Klicken Sie im Abschnitt "Clients" auf **Clients hinzufügen**.
- b Geben Sie eine oder mehrere Drucker-IP-Adressen ein, und fügen Sie diese anschließend hinzu.

Client-Drucker löschen

Hinweis: Sie können Client-Drucker nicht löschen, wenn der Master-Drucker offline ist oder wenn die Anwendung deinstalliert wird.

- a Wählen Sie im Abschnitt "Clients" einen oder mehrere Client-Drucker aus.
- b Klicken Sie auf **Clients löschen**.

Neuzuweisen der Druckerrollen

- 1 Konfigurieren Sie einen neuen Masterdrucker.
 - a Greifen Sie über den Embedded Web Server des neuen Masterdruckers auf die Konfigurationsseite der Anwendung zu.
 - b Legen Sie im Bereich "Druckerbasierte Kartvalidierung" die Rolle als **Master** fest.
 - c Geben Sie Host-Namen oder IP-Adresse des Backup-Druckers ein.
 - d Klicken Sie auf **Übernehmen**.
- 2 Weisen Sie den Backup-Drucker zum neuen Masterdrucker zu.
 - a Greifen Sie über den Embedded Web Server des Backup-Druckers auf die Konfigurationsseite der Anwendung zu.
 - b Geben Sie im Abschnitt "Druckerbasierte Kartvalidierung" den Hostnamen oder die IP-Adresse des neuen Masterdruckers ein.
 - c Klicken Sie auf **Übernehmen**.
- 3 Löschen Sie den Client-Drucker aus dem aktuellen Masterdrucker.
 - a Greifen Sie über den Embedded Web Server des aktuellen Masterdruckers auf die Statusseite der Anwendung zu.
 - b Löschen Sie im Abschnitt "Clients" den Client-Drucker.
- 4 Weisen Sie den Client-Drucker wieder dem neuen Masterdrucker zu. Führen Sie einen der folgenden Schritte aus:

Verwenden der Konfigurationsseite für die Anwendung

- a Greifen Sie über den Embedded Web Server des Client-Druckers auf die Konfigurationsseite der Anwendung zu.
- b Legen Sie im Bereich "Druckerbasierte Kartvalidierung" die Rolle als **Client** fest.
- c Geben Sie Host-Namen oder IP-Adresse des neuen Masterdruckers ein.

Hinweis: Stellen Sie sicher, dass der Host-Name oder die IP-Adresse des Backup-Druckers korrekt sind.

- d Klicken Sie auf **Übernehmen**.

Verwenden der Statusseite des Master-Druckers

- a** Greifen Sie über den Embedded Web Server des neuen Masterdruckers auf die Statusseite der Anwendung zu.
- b** Klicken Sie im Abschnitt "Clients" auf **Clients hinzufügen**.
- c** Geben Sie die IP-Adresse des Client-Druckers ein, und fügen Sie diese dann hinzu.

Verwenden der Anwendung

Registrieren von Benutzern

- 1 Tippen Sie Ihre Karte an den Kartenleser.
- 2 Geben Sie in der Bedienerkonsole des Druckers Ihre Anmeldeinformationen ein.
Hinweis: Geben Sie einen Bereich an, wenn Sie Kerberos, Active Directory oder LDAP+GSSAPI für die Kartenregistrierung verwenden möchten.
- 3 Befolgen Sie die Anweisungen auf dem Display.

Registrieren einer PIN

Stellen Sie zunächst sicher, dass die Anmeldemethode so eingestellt ist, dass diese die PIN-Authentifizierung unterstützt.

- 1 Drücken Sie auf dem Druckerbedienfeld auf **PIN-Anmeldung**.
- 2 Befolgen Sie die Anweisungen auf dem Display.

Manuelle Anmeldung am Drucker

- 1 Berühren Sie auf dem Bedienfeld des Druckers eine der folgenden Schaltflächen:
 - **PIN-Anmeldung**
 - **Manuelle Anmeldung**
 - **Administratoranmeldung**

Hinweis: Wenn Sie **Administratoranmeldung** auswählen, können Sie keine anderen Benutzerinformationen vom LDAP-Server abrufen.

- 2 Geben Sie Ihre Anmeldeinformationen ein.
Hinweis: Wenn Sie Kerberos, Active Directory® oder LDAP+GSSAPI für den manuellen Login verwenden, dann wählen Sie einen Bereich aus.
- 3 Befolgen Sie die Anweisungen auf dem Display.

Fehlerbehebung

Anwendungsfehler

Probieren Sie eine oder mehrere der folgenden Methoden:

Überprüfen des Systemprotokolls

- 1 Klicken Sie im Embedded Web Server auf **Einstellungen** oder **Konfiguration**.
- 2 Führen Sie je nach Druckermodell einen der folgenden Schritte aus:
 - Klicken Sie auf **Apps > Apps-Management**.
 - Klicken Sie auf **Gerätelösungen > Lösungen (eSF)**.
 - Klicken Sie auf **Embedded Solutions**.
- 3 Klicken Sie auf **System > Protokoll**.
- 4 Wählen und übermitteln Sie die entsprechenden Filter.
- 5 Analysieren Sie das Protokoll und lösen Sie dann das Problem.

Wenden Sie sich an Ihren Ansprechpartner bei Lexmark.

Anwendung läuft mit der aktualisierten Version von SaaS Print Release nicht

Probieren Sie eine oder mehrere der folgenden Methoden:

Sicherstellen, dass Print Release ordnungsgemäß konfiguriert ist

Wenn Sie Ihre Anwendung Print Management SaaS auf Print Release V2.0 oder höher aktualisiert haben, dann deaktivieren Sie "Hintergrund und inaktiver Bildschirm". Weisen Sie die Zugriffssteuerung der Kartenauthentifizierung für Print Release zu, und achten Sie darauf, dass Print Release ordnungsgemäß konfiguriert ist. Weitere Informationen finden Sie im *Administratorhandbuch zu Print Release*.

Wenden Sie sich an Ihren Ansprechpartner bei Lexmark.

Authentifizierungsfehler

Probieren Sie eine oder mehrere der folgenden Methoden:

Erhöhen des Werts für die Druckerzeitverzögerung

Wenn Sie den Identitätsdienst zu Kartvalidierung verwenden, dann braucht der Drucker unter Umständen länger, um mit dem Identitätsdienstanbieter zu kommunizieren.

- 1 Klicken Sie im Embedded Web Server auf **Einstellungen** oder **Konfiguration**.
- 2 Klicken Sie auf **Allgemeine Einstellungen > Zeitsperren**.
- 3 Erhöhen Sie die Anzeige-Zeitsperre und den Ruhemodus.
- 4 Klicken Sie auf **Übernehmen**.

Verbindung des Druckers mit dem Netzwerk

Weitere Informationen finden Sie im *Benutzerhandbuch* des Druckers.

Sicherstellen, dass der Sicherheitsserver online und nicht überlastet ist

Weitere Informationen erhalten Sie beim Systemadministrator.

Benutzer ist gesperrt

Der Benutzer hat möglicherweise die zulässige Anzahl von fehlgeschlagenen Anmeldeversuchen überschritten.

Erhöhen der Sperrzeit und der zulässigen Anzahl an fehlgeschlagenen Anmeldeversuchen

- 1 Führen Sie je nach Druckermodell vom Embedded Web Server einen der folgenden Schritte aus:
 - Klicken Sie auf **Einstellungen > Sicherheit > Sonstige Sicherheitseinstellungen > Anmeldebeschränkungen**.
 - Klicken Sie auf **Konfiguration > Sicherheit**.
- 2 Erhöhen Sie die Sperrzeit und die zulässige Anzahl an fehlgeschlagenen Anmeldeversuchen oder die automatische Abmeldeverzögerung.
- 3 Klicken Sie auf **Übernehmen**.

Client-Drucker kann nicht registriert werden

Probieren Sie eine oder mehrere der folgenden Methoden:

Sicherstellen, dass der Masterdrucker oder der Backup-Drucker online ist

Weitere Informationen finden Sie unter ["Zugriff auf die Statusseite für die Anwendung" auf Seite 17](#).

Sicherstellen, dass der Masterdrucker und der Backup-Drucker ordnungsgemäß eingerichtet sind

Weitere Informationen finden Sie unter ["Konfigurieren der druckerbasierten Benutzerauthentifizierung" auf Seite 9.](#)

Sicherstellen, dass Sie nicht mehr als 23 Client-Drucker registrieren

Weitere Informationen finden Sie unter ["Verwalten von Benutzerkonten und Client-Druckern" auf Seite 17.](#)

Wenden Sie sich an Ihren Ansprechpartner bei Lexmark.

Überprüfen der Karte nicht möglich

Probieren Sie eine oder mehrere der folgenden Methoden:

Anmeldemethode auf Karte oder manuelle Anmeldung setzen

- 1 Greifen Sie über Embedded Web Server auf die Konfigurationsseite der Anwendung zu.
- 2 Legen Sie im Bereich "Anmeldebildschirm" die Anmeldemethode als **Karte oder Manuelle Anmeldung** fest.
- 3 Klicken Sie auf **Übernehmen**.

Wenden Sie sich an Ihren Ansprechpartner bei Lexmark.

Bereichsinformationen können nicht gefunden werden.

Probieren Sie eine oder mehrere der folgenden Methoden:

Einige Anmeldemethoden für eine manuelle Anmeldung oder Kartenregistrierung, wie lokale Konten oder LDAP, erfordern keine Bereichsauswahl. Die Anmeldemethoden, bei denen eine Auswahl des Bereichs erforderlich ist, sind Kerberos, Active Directory und LDAP+GSSAPI.

Auswahl des Bereichs deaktivieren

- 1 Greifen Sie über Embedded Web Server auf die Konfigurationsseite der Anwendung zu.
- 2 Löschen Sie im Bereich "Erweiterte Einstellungen" die Option **Ausgewählten Bereich verwenden**.
- 3 Klicken Sie auf **Übernehmen**.

Ändern Sie die Anmeldemethode

- 1 Greifen Sie über Embedded Web Server auf die Konfigurationsseite der Anwendung zu.
- 2 Legen Sie im Abschnitt "Benutzerauthentifizierung" die Option "Zugriffssteuerung der Kartenregistrierung" und "Zugriffssteuerung der manuellen Anmeldung" auf **App 1** oder **Lösung 1** fest.
- 3 Klicken Sie auf **Übernehmen**.

Wenden Sie sich an Ihren Ansprechpartner bei Lexmark.

Keine Verbindung mit dem LDAP-Server möglich

Probieren Sie eine oder mehrere der folgenden Methoden:

Überprüfen Sie die LDAP-Einstellungen

Weitere Informationen finden Sie unter ["Konfigurieren der LDAP-Einstellungen" auf Seite 15.](#)

Wenden Sie sich an Ihren Ansprechpartner bei Lexmark.

Häufig gestellte Fragen

Warum kann ich keinen Client-Drucker löschen oder hinzufügen, wenn ein Backup-Drucker als Masterdrucker agiert?

Sie können Client-Drucker nur löschen oder hinzufügen, wenn der Masterdrucker online ist.

Kann ich einen Client-Drucker entfernen und diesem seinen neuen Masterdrucker zuweisen, auch wenn der aktuelle Masterdrucker offline ist?

Ja, gehen Sie wie folgt vor:

- 1 Installieren Sie über Embedded Web Server des Client-Druckers die Anwendung.
- 2 Legen Sie die Rolle als Client-Drucker fest, und konfigurieren Sie ihn anschließend mit seinem neuen Master-Drucker und den Backup-Druckern. Weitere Informationen finden Sie unter ["Einrichten der Rolle für den Drucker" auf Seite 10](#).

Was soll ich tun, wenn ich versehentlich die Anwendung vom Drucker deinstalliert habe?

- 1 Installieren Sie über Embedded Web Server die Anwendung.
- 2 Legen Sie eine Rolle für den Drucker fest. Weitere Informationen finden Sie unter ["Einrichten der Rolle für den Drucker" auf Seite 10](#).

Hinweis: Stellen Sie sicher, dass der Masterdrucker, der Backup-Drucker und dann die Client-Drucker ordnungsgemäß eingerichtet sind.

- 3 Konfigurieren Sie den Drucker je nach Rolle.

Hinweise:

- Wenn die Anwendung erneut auf einem Masterdrucker installiert wird, weisen Sie diesem seinen Backup-Drucker zu.
- Wenn die Anwendung erneut auf einem Backup-Drucker installiert wird, weisen Sie diesem seinen Masterdrucker zu.
- Wenn die Anwendung erneut auf einem Client-Drucker installiert wird, weisen Sie diesem seinen Masterdrucker und Backup-Drucker zu.
- Weitere Informationen finden Sie unter ["Neuzuweisen der Druckerrollen" auf Seite 18](#).

Warum kann ich auf dem Sperrbildschirm die Schaltflächen "Kopie" oder "Fax" nicht sehen, obwohl ich die Option "Ohne Anmeldung" aktiviert habe?

Legen Sie die Zugriffssteuerung der Kopier- oder Faxfunktion auf **Keine Sicherheit** fest. Weitere Informationen finden Sie unter ["Konfigurieren des Anmeldebildschirms" auf Seite 9](#).

Was passiert, wenn ich die gleichen Zugriffssteuerungen für Manuelle Anmeldung und Sitzung habe?

Zum Zugreifen auf die Druckerfunktionen vom Startbildschirm aus müssen Sie bei der Anmeldung Ihre Anmeldeinformationen manuell eingeben.

Kann ich verschiedene Zugriffssteuerungen für Manuelle Anmeldung und Kartenvalidierung haben?

Ja, es sei denn, Sie verwenden eine Identitätsdienst-Authentifizierung, legen Sie dann die Zugangskontrolle für Manuelle Anmeldung und Kartenvalidierung auf **Identitätsdienst** fest.

Warum funktioniert die Funktion Administratoranmeldung nicht mit Netzwerkkonten?

Die Funktion **Administratoranmeldung** gilt nur für Sicherheitsvorlagen für Interne Konten, PIN, und Kennwort.

Hinweise

Hinweis zur Ausgabe

Dezember 2020

Der folgende Abschnitt gilt nicht für Länder, in denen diese Bestimmungen mit dem dort geltenden Recht unvereinbar sind: LEXMARK INTERNATIONAL, INC., STELLT DIESE VERÖFFENTLICHUNG OHNE MANGELGEWÄHR ZUR VERFÜGUNG UND ÜBERNIMMT KEINERLEI GARANTIE, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF, DER GESETZLICHEN GARANTIE FÜR MARKTGÄNGIGKEIT EINES PRODUKTS ODER SEINER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. In einigen Staaten ist der Ausschluss von ausdrücklichen oder stillschweigenden Garantien bei bestimmten Rechtsgeschäften nicht zulässig. Deshalb besitzt diese Aussage für Sie möglicherweise keine Gültigkeit.

Diese Publikation kann technische Ungenauigkeiten oder typografische Fehler enthalten. Die hierin enthaltenen Informationen werden regelmäßig geändert; diese Änderungen werden in höheren Versionen aufgenommen. Verbesserungen oder Änderungen an den beschriebenen Produkten oder Programmen können jederzeit vorgenommen werden.

Die in dieser Softwaredokumentation enthaltenen Verweise auf Produkte, Programme und Dienstleistungen besagen nicht, dass der Hersteller beabsichtigt, diese in allen Ländern zugänglich zu machen, in denen diese Softwaredokumentation angeboten wird. Kein Verweis auf ein Produkt, Programm oder einen Dienst besagt oder impliziert, dass nur dieses Produkt, Programm oder dieser Dienst verwendet werden darf. Sämtliche Produkte, Programme oder Dienste mit denselben Funktionen, die nicht gegen vorhandenen Beschränkungen bezüglich geistigen Eigentums verstoßen, können stattdessen verwendet werden. Bei Verwendung anderer Produkte, Programme und Dienstleistungen als den ausdrücklich vom Hersteller empfohlenen ist der Benutzer für die Beurteilung und Prüfung der Funktionsfähigkeit selbst zuständig.

Technischen Support von Lexmark erhalten Sie unter <http://support.lexmark.com>.

Informationen zur Lexmark Datenschutzrichtlinie für die Verwendung dieses Produkts finden Sie unter www.lexmark.com/privacy.

Unter www.lexmark.com erhalten Sie Informationen zu Zubehör und Downloads.

© 2014 Lexmark International, Inc.

Alle Rechte vorbehalten.

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.

Marken

Lexmark und das Lexmark Logo sind Marken oder eingetragene Warenzeichen von Lexmark International, Inc., eingetragen in den Vereinigten Staaten und/oder anderen Ländern.

Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber.

Index

A

- Administratorauthentifizierung
 - konfigurieren 8
- aktivieren eines akustischen Signals nach dem Anmelden 15
- Anmeldebildschirm
 - konfigurieren 9
- Anmeldemethode
 - konfigurieren 9
- Anmelden
 - Manuell 20
 - PIN 20
- Anmeldeprofil
 - Verwenden 15
- Anwendungseinstellungen
 - einstellen 15
- Anwendungsfehler 21
- anzeigen von Bereichen für Benutzerkonten 15
- aufrufen
 - Statusseite 17
- Authentifizierungsfehler 22

B

- Backup-Drucker
 - einrichten 10
 - Zuweisen 18
- Benutzer
 - hinzufügen 20
 - Registrieren 20
- Benutzerauthentifizierung für Identitätsdienst
 - konfigurieren 12
- Benutzerauthentifizierung für Webdienst
 - konfigurieren 11
- Benutzer ist gesperrt 22
- Benutzerkonten
 - löschen 17
- Bereichsinformationen können nicht gefunden werden. 23

C

- Client-Drucker
 - einrichten 10
 - hinzufügen 17
 - löschen 17

- Migrieren 18
- Client-Drucker kann nicht registriert werden 22

D

- Drucker
 - einrichten 10
- druckerbasierte Benutzerauthentifizierung
 - konfigurieren 9
- Druckerrollen
 - Neuzuweisen 18

E

- einrichten
 - Drucker 10
- Einrichten von Anwendungseinstellungen 15
- Einrichten von Gruppen für ein internes Benutzerkonto 5
- Embedded Web Server
 - aufrufen 5
 - erstellen einer Sicherheitsvorlage 6
- Exportieren einer Konfigurationsdatei 16

F

- Fehlerbehebung
 - Anwendungsfehler 21
 - Authentifizierungsfehler 22
 - Benutzer ist gesperrt 22
 - Bereichsinformationen können nicht gefunden werden. 23
 - Client-Drucker kann nicht registriert werden 22
 - Keine Verbindung mit dem LDAP-Server möglich 24
 - überprüfen der Karte nicht möglich 23

H

- Häufig gestellte Fragen 25
- hinzufügen
 - Benutzer 20
 - Client-Drucker 17

- hinzufügen eines internen Benutzerkontos 5

I

- Identitätsdienst-Einstellungen
 - konfigurieren 13
- Importieren einer Konfigurationsdatei 16
- interne Benutzerkonten
 - Einordnen in Gruppen 5
 - hinzufügen 5

K

- Keine Verbindung mit dem LDAP-Server möglich 24
- Konfigurationsdatei
 - Exportieren oder importieren 16
- Konfigurationsseite für die Anwendung
 - aufrufen 8
 - konfigurieren
 - Anmeldebildschirm 9
 - Anmeldemethode 9
- Konfigurieren der Administratorauthentifizierung 8
- konfigurieren der Benutzerauthentifizierung für den Webdienst 11
- konfigurieren der Benutzerauthentifizierung für Identitätsdienst 12
- konfigurieren der druckerbasierten Benutzerauthentifizierung 9
- konfigurieren der Einstellungen für Identitätsdienst 13
- konfigurieren der Einstellungen für Webdienst 11
- konfigurieren der LDAP-Benutzerauthentifizierung 14
- konfigurieren der LDAP-Einstellungen 15
- konfigurieren der PIN-Benutzerauthentifizierung 13
- konfigurieren eines neuen Masterdruckers 18
- Konfigurieren von Bereichen
 - Anmeldemethoden 15

konfigurieren von PIN-Einstellungen 14
konfigurieren von Zugriffssteuerungen 6

L

LDAP-Benutzerauthentifizierung konfigurieren 14
LDAP-Einstellungen konfigurieren 15
löschen
 Benutzerkonten 17
 Client-Drucker 17

M

Manuelle Anmeldung 20
Manuelle Anmeldung am Drucker 20
Masterdrucker einrichten 10
Migrieren
 Client-Drucker 18

N

neuen Masterdrucker konfigurieren 18
Neuzuweisen der Druckerrollen 18

P

PIN
 Registrieren 20
PIN-Anmeldung 20
PIN-Benutzerauthentifizierung konfigurieren 13
PIN-Einstellungen konfigurieren 14

R

Registrieren einer PIN 20
Registrieren von Benutzern 20
Registrierungsmeldungen einstellen 15

S

Sicherheitsvorlage Erstellen 6
Statusseite aufrufen 17

Ü

überprüfen der Karte nicht möglich 23
Übersicht 4

V

verwenden der Faxfunktion ohne Anmeldung 9
verwenden der Kopierfunktion ohne Anmeldung 9
verwenden eines Anmeldeprofils 15

W

Webdiensteinstellungen konfigurieren 11

Z

Zugreifen auf die Konfigurationsseite 8
Zugriff auf den Embedded Web Server 5
Zugriffssteuerungen konfigurieren 6
zuweisen des Backup-Druckers 18