Smart Card Authentication

Administratorhandbuch

August 2017

www.lexmark.com

Inhalt

Änderungsverlauf

August 2017

- Anweisungen zum Ändern der Anmeldemethode hinzugefügt.
- Anweisung zum Deaktivieren der Anwendung "Device Quotas" hinzugefügt.
- Support für brasilianisches Portugiesisch, Finnisch, Französisch, Deutsch, Italienisch, Vereinfachtes Chinesisch und Spanisch hinzugefügt.

Juli 2016

- Anweisungen zur Konfiguration der Anwendung "E-Mail an eigene Adresse senden" hinzugefügt.

Januar 2016

- Ursprüngliche Dokumentenveröffentlichung für Multifunktions-Produkte mit einem tabletähnlichen Touchscreen-Display.

Übersicht

Smart Card Authentication besteht aus unterschiedlichen Anwendungen, die für sicheren Zugriff auf Drucker und deren Funktionen verwendet werden. Mit den Anwendungen können Sie sich manuell bei einem Drucker anmelden oder eine Smart Card verwenden und dann sicher E-Mails versenden und Druckaufträge freigeben. Sie können in einer Anwendung auch andere Sicherheitseinstellungen konfigurieren, wie etwa das Signieren und Verschlüsseln von E-Mails.

Das "Smart Card Authentication"-Paket beinhaltet die folgenden Anwendungen:

- **Smart Card Authentication Client** – Sichert den Zugriff auf Drucker, indem Benutzer aufgefordert werden, sich über eine Smart Card oder unter Angabe von Benutzernamen und Kennwort anzumelden. Sie können den Zugang zum Startbildschirm des Druckers oder auf einzelne Anwendungen und Funktionen sichern. Zusätzlich bietet die Anwendung Optionen für die Kerberos-Authentifizierung sowie ein Kerberos-Ticket, das zum Sichern von anderen Anwendungen genutzt werden kann.
- **Smart Card-Treiber** – Ermöglicht dem Drucker mit einer unterstützten Smart Card zu kommunizieren.
- **Anpassung Display** – Ermöglicht Ihnen das Hochladen von Bildern. Sie können die Bilder nutzen, um benutzerdefinierte Diashows zu erstellen oder, um das Hintergrundbild und den Bildschirmschoner des Druckers einzustellen. Sichern Sie diese Anwendung mithilfe von "Smart Card Authentication Client", damit sich Benutzer authentifizieren müssen, bevor sie auf den Startbildschirm des Druckers zugreifen können.
- **Sichere E-Mail** – Hier können Sie E-Mails, die vom Drucker gesendet wurden, digital signieren und verschlüsseln. Diese Anwendung setzt die standardmäßige E-Mail-Funktion des Druckers außer Kraft.
- **Secure Held Print Jobs** – Lässt authentifizierte Benutzer ihre angehaltenen Druckaufträge anzeigen und freigeben.

Dieses Dokument bietet Informationen zur Konfiguration und Verwendung der Anwendungen sowie zur Fehlerbehebung dafür.

Checkliste Einsatzbereitschaft

Stellen Sie Folgendes sicher:

- ☐ Dass Sie die folgenden Punkte installiert haben:
  - Mindestens 512 MB RAM
  - Einen Smart Card-Leser und dessen Treiber
- ☐ Dass Sie die Anwendung "Device Quotas" deaktiviert haben:
  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.
     - Berühren Sie auf dem Startbildschirm des Druckers **Einstellungen** > **Netzwerk/Anschlüsse** > **Netzwerkübersicht**.
  2. Öffnen Sie einen Webbrowser, und geben Sie die IP-Adresse des Druckers ein.
  3. Klicken Sie auf **Apps** > **Device Quotas** > **Stopp**.

Sie benötigen Folgendes, um "Smart Card Authentication Client" zu konfigurieren:

- ☐ Zertifikat der Zertifizierungsstelle (.cer-Datei)
- ☐ Lightweight Directory Access Protocol (LDAP) und Active Directory® Konten

  _____
- ☐ Kerberos-Bereich, Domain und Domänen-Controller

  _____
- ☐ Kerberos-Datei (für mehrere Domänen)

Konfigurieren der Druckereinstellungen

Zur Konfiguration der Druckereinstellungen 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.
   - Berühren Sie auf dem Startbildschirm des Druckers **Einstellungen** > **Netzwerk/Anschlüsse** > **Netzwerkübersicht**.
2. Öffnen Sie einen Webbrowser, und geben Sie die IP-Adresse des Druckers ein.

Einstellung der Anzeige-Zeitsperre

Um unberechtigten Zugriff zu verhindern, können Sie den Zeitraum einschränken, den ein Benutzer am Drucker inaktiv angemeldet bleibt.

1. Klicken Sie im Embedded Web Server auf **Einstellungen** > **Gerät** > **Voreinstellungen**.
2. Geben Sie im Feld "Anzeige-Zeitsperre" an, wie viel Zeit vergehen soll, bis der Bildschirm inaktiv wird und der Benutzer abgemeldet wird. Wir empfehlen eine Einstellung auf 30 Sekunden.
3. Klicken Sie auf **Speichern**.

Manuelles Installieren von Zertifikaten

Hinweis: Informationen zum automatischen Herunterladen von CA-Zertifikaten finden Sie unter "Automatische Installation von Zertifikaten" auf Seite 8.

Vor dem Konfigurieren von Kerberos oder Domänencontroller-Einstellungen müssen Sie das CA-Zertifikat für die Domänencontroller-Validierung installieren. Wenn Sie das Zertifikat des Domänencontrollers anhand der Kettenüberprüfung überprüfen möchten, müssen Sie die gesamte Zertifikatskette installieren. Jedes Zertifikat muss sich in einer separaten PEM-Datei (".cer") befinden.

1. Klicken Sie im Embedded Web Server auf **Einstellungen** > **Sicherheit** > **Zertifikatsverwaltung**.
2. Klicken Sie im Abschnitt "CA-Zertifikate verwalten" auf **CA hochladen**, und wechseln Sie dann zur PEM (.cer) -Datei.

   Musterzertifikat:

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

3. Klicken Sie auf **Speichern**.

Automatische Installation von Zertifikaten

1 Klicken Sie im Embedded Web Server auf **Einstellungen** > **Sicherheit** > **Zertifikatsverwaltung** > **Auto-Update f. Zertifikat konfigurieren**.

2 Wenn Sie aufgefordert werden, sich bei einer Active Directory-Domäne anzumelden, klicken Sie auf **Domäne betreten** und geben dann die Domäneninformationen ein.

Hinweis: Stellen Sie sicher, dass die Active Directory-Domäne zum Kerberos-Bereich oder zur Domäne passt, die von den Einstellungen der Smartcard verwendet wird. Weitere Informationen finden Sie unter "Konfigurieren der Smartcard-Einstellungen" auf Seite 14.

3 Wählen Sie **Auto-Update aktivieren**.

Hinweis: Wenn Sie installieren das CA-Zertifikat installieren möchten, ohne die geplante Laufzeit abzuwarten, wählen Sie die Option **Sofort abrufen**.

4 Klicken Sie auf **Speichern**.

Konfigurieren der TCP/IP-Einstellungen

1 Klicken Sie im Embedded Web Server auf **Einstellungen** > **Netzwerk/Anschlüsse** > **TCP/IP**.

2 Gehen Sie wie folgt vor:

- Wenn Sie eine statische IP-Adresse verwenden, geben Sie die DNS-Serveradresse ein. Wenn ein DNS-Sicherungsserver verfügbar ist, geben Sie die Adresse des DNS-Sicherungsservers ein.
- Wenn sich der Drucker in einer anderen Domäne befindet, geben Sie im Feld "Domänensuchreihenfolge" die anderen Domänen ein. Trennen Sie mehrere Domänen durch ein Komma.

Hinweis: Verwenden Sie den Domänennamen, der den Benutzer-Arbeitsstationen zugewiesen ist.

3 Klicken Sie auf **Speichern**.

Einstellen von Datum und Uhrzeit

Stellen Sie bei der Verwendung der Kerberos-Authentifizierung sicher, dass der Zeitunterschied zwischen dem Drucker und dem Domaincontroller fünf Minuten nicht übersteigt. Sie können die Datums- und Uhrzeiteinstellungen manuell aktualisieren oder das Network Time Protocol (NTP) verwenden, um die Zeit automatisch mit dem Domaincontroller zu synchronisieren.

1 Klicken Sie im Embedded Web Server auf **Einstellungen** > **Gerät** > **Voreinstellungen** > **Datum und Uhrzeit**.

Manuelles Konfigurieren

Hinweis: Durch das manuelle Konfigurieren von Datum und Uhrzeit wird das NTP deaktiviert.

a Geben Sie im Abschnitt "Konfigurieren" im Feld "Datum und Uhrzeit manuell einstellen" das richtige Datum und die Uhrzeit ein.

b Wählen Sie Datumsformat, Uhrzeitformat und Zeitzone.

Hinweis: Wenn Sie " **(UTC+Ben.) Benutzerdefiniert** auswählen, müssen Sie die UTC (GMT)-und DST-Abweichungen eingeben.

NTP konfigurieren

a Wählen Sie im Abschnitt "Network Time Protocol" **NTP aktivieren** aus und geben Sie dann die IP-Adresse oder den Hostnamen des NTP-Servers ein.

b Wenn der NTP-Server eine Authentifizierung erfordert, wählen Sie im Menü "Authentifizierung aktivieren" die Option **MD5-Schlüssel**.

c Je nach Ihrem Druckermodell geben Sie entweder die Schlüssel-ID und das Kennwort ein, oder Sie suchen nach der Datei, die die NTP-Authentifizierungsinformationen enthält.

2 Klicken Sie auf **Speichern**.

Konfiguration der LDAP-Einstellungen für Netzwerkkonten

Ein LDAP-Netzwerkkonto ist erforderlich, um verschlüsselte E-Mails versenden zu können. Verschlüsselungszertifikate für Empfänger werden über den LDAP-Server hinzugefügt und konfiguriert. Weitere Informationen erhalten Sie beim Systemadministrator.

Hinweis: Ein Kerberos-Netzwerkkonto ist erforderlich, um ein LDAP + GSSAPI Netzwerkkonto zu erstellen.

1 Klicken Sie im Embedded Web Server auf **Einstellungen** > **Sicherheit** > **Anmeldemethoden**.

2 Klicken Sie im Abschnitt "Netzwerkkonten" auf **Anmeldemethode hinzufügen** > **LDAP**.

3 Wählen Sie **LDAP** oder **LDAP + GSSAPI**.

4 Konfigurieren Sie in der Registerkarte "Allgemeine Informationen" Folgendes:

- **Setup-Name**: Ein eindeutiger Name für das LDAP-Netzwerkkonto.
- **Serveradresse**

  Hinweis: Stellen Sie sicher, dass die Adresse identisch ist mit der Adresse des Domänencontrollers des Smart Card Authentication Client oder der KDC-Adresse in der Kerberos-Konfigurationsdatei.
- **Server-Port**: Wenn Sie mit SSL verschlüsseln, können Sie den Port **636** verwenden. Verwenden Sie andernfalls Port **389**.

5 Deaktivieren Sie im Abschnitt "Anmeldeinformationen" **Anonyme LDAP-Bindung**, und geben Sie anschließend die Authentifizierungsinformationen für die Verbindung mit dem LDAP-Server ein.

6 Wenn der LDAP-Server eine SSL-Verschlüsselung fordert, stellen Sie im Abschnitt "Erweiterte Optionen" die Option "SSL/TLS verwenden" auf **SSL/TLS** ein.

7 Wählen Sie im Abschnitt "Adressbuch-Einrichtung" die Option **Benutzeranmeldeinformationen verwenden** aus.

8 Klicken Sie auf **Speichern und überprüfen**.

Sichern des Zugriffs auf den Drucker

Sichern des Zugriffs auf den Startbildschirm

Benutzer müssen sich authentifizieren, bevor sie auf den Drucker-Startbildschirm zugreifen können.

Hinweis: Stellen Sie zunächst sicher, dass die Anwendung "Anpassung Display" auf ihrem Drucker aktiviert ist. Weitere Informationen finden Sie im *Administrator-Handbuch für Anzeigenanpassung*.

1. Klicken Sie im Embedded Web Server auf **Einstellungen** > **Sicherheit** > **Anmeldemethoden**.
2. Klicken Sie im Abschnitt "Öffentlich" auf **Berechtigungen verwalten**.
3. Erweitern Sie **Apps**, und entfernen Sie **Diashow**, **Hintergrund ändern**und **Bildschirmschoner**, und klicken Sie dann auf **Speichern**.
4. Klicken Sie im Abschnitt "Zus. Anmeldemethoden" neben Smartcard auf **Berechtigungen verwalten**.
5. Wählen Sie eine Gruppe, deren Berechtigungen Sie verwalten möchten.

   Hinweis: Die Gruppe "Alle Benutzer" wird standardmäßig erstellt. Weitere Gruppennamen werden angezeigt, wenn Sie vorhandene Active Directory-Gruppen im Feld " Gruppenautorisierungsliste" angeben. Weitere Informationen finden Sie unter "Konfigurieren erweiterter Einstellungen" auf Seite 15.
6. Erweitern Sie **Apps**, und wählen Sie **Diashow**, **Hintergrund ändern** und **Bildschirmschoner**.
7. Klicken Sie auf **Speichern**.

Sichern des Zugriffs auf einzelne Anwendungen und Funktionen

Benutzer müssen sich vor dem Zugreifen auf eine Anwendung oder eine integrierte Druckerfunktion authentifizieren.

1. Klicken Sie im Embedded Web Server auf **Einstellungen** > **Sicherheit** > **Anmeldemethoden**.
2. Klicken Sie im Abschnitt "Öffentlich" auf **Berechtigungen verwalten**.
3. Schränken Sie den öffentlichen Zugang zu den Anwendungen oder Funktionen ein, die Sie sichern möchten. Gehen Sie wie folgt vor:
   - Für "Secure E-mail", erweitern Sie **Funktionszugriff**, deaktivieren Sie **E-Mail-Funktion**, und klicken Sie dann auf **Speichern**.
   - Für "Secure Held Print Jobs", erweitern Sie **Apps**, deaktivieren Sie **Secure Held Print Jobs**, und klicken Sie dann auf **Speichern**.
   - Für andere Anwendungen oder Funktionen, erweitern Sie mindestens eine Kategorie, deaktivieren Sie die Anwendung oder Funktion, und klicken Sie dann auf **Speichern**.
4. Klicken Sie im Abschnitt "Zus. Anmeldemethoden" neben Smart Card auf **Berechtigungen verwalten**.
5. Wählen Sie eine Gruppe, deren Berechtigungen Sie verwalten möchten.

   Hinweis: Die Gruppe "Alle Benutzer" wurde standardmäßig erstellt. Wenn Sie die vorhandenen "Active Directory"-Gruppen im Feld "Gruppenautorisierungsliste" angeben, werden weitere Gruppennamen angezeigt. Weitere Informationen finden Sie unter "Konfigurieren erweiterter Einstellungen" auf Seite 15.
6. Wählen Sie die Anwendungen oder Funktionen aus, auf die authentifizierte Benutzer zugreifen können. Gehen Sie wie folgt vor:
   - Für "Sichere E-Mail", erweitern Sie **Funktionszugriff**, und wählen Sie dann **E-Mail-Funktion** aus.
   - Für "Secure Held Print Jobs", erweitern Sie **Apps**, und wählen Sie dann **Secure Held Print Jobs**.
   - Für alle anderen Anwendungen oder Funktionen, erweitern Sie mindestens eine Kategorie, und wählen Sie dann die Anwendung oder die Funktion aus.
7. Klicken Sie auf **Speichern**.

Gesicherte Anwendungen oder Funktionen auf dem Startbildschirm anzeigen

Standardmäßig werden gesicherte Anwendungen oder Funktionen auf dem Startbildschirm des Druckers ausgeblendet.

1. Klicken Sie im Embedded Web Server auf **Einstellungen** > **Sicherheit** > **Sonstiges**.
2. Im Menü "Geschützte Funktionen" **Anzeigen** auswählen.
3. Klicken Sie auf **Speichern**.

Konfigurieren der E-Mail-Einstellungen des Druckers

Diese Anwendung setzt die E-Mail-Funktion des Druckers außer Kraft.

Konfigurieren der SMTP-Einstellungen

1. Klicken Sie im Embedded Web Server auf **Einstellungen** > **E-Mail** > **E-Mail Setup**.
2. Konfigurieren Sie Folgendes:
   - **Primärer SMTP-Gateway**: Geben Sie die IP-Adresse oder den Hostnamen des Servers für den E-Mail-Versand ein.

     Hinweis: Verwenden Sie den Hostnamen für die Kerberos-Authentifizierung.
   - **Primärer SMTP-Gateway-Anschluss**
   - **Sekundärer SMTP-Gateway**: Die Server-IP-Adresse oder der Hostnamen des sekundären oder Backup-SMTP-Servers.
   - **Sekundärer SMTP-Gateway-Port**
   - **SMTP-Zeitsperre**
   - **SSL/TLS verwenden**
   - **Rückantwort an**
   - **SMTP-Server-Authentifizierung**

     Hinweise:

     - Wenn **Kerberos 5** ausgewählt ist, geben Sie den Kerberos-Bereich ein.
     - Wenn **NTLM** ausgewählt ist, geben Sie die NTLM-Domäne ein.
     - Wenn der SMTP-Server eine Authentifizierung erfordert, aber Kerberos nicht unterstützt, geben Sie im Feld "Antwortadresse" die IP-Adresse oder den Hostnamen des Druckers ein.
   - **Gerät initiierte E-Mail**: Die Geräteanmeldeinformationen sind für vom Gerät initiierte E-Mails erforderlich.

     Hinweis: Wenn **SMTP-Anmeldeinformationen des Geräts verwenden** ausgewählt ist, geben Sie die Authentifizierungsinformationen ein.
   - **Vom Benutzer initiierte E-Mail**: Die Authentifizierungsinformationen des Benutzers sind erforderlich für vom Benutzer initiierte E-Mails.

     Hinweis: Wenn Sie mit Kerberos-Authentifizierung arbeiten, wählen Sie die Option **Benutzer-ID und Kennwort verwenden**.
3. Klicken Sie auf **Speichern**.

Konfigurieren von standardmäßigen E-Mail- und Scaneinstellungen

1. Klicken Sie im Embedded Web Server auf **Einstellungen** > **E-Mail** > **E-Mail Standardeinstellungen**.
2. Konfigurieren Sie die Einstellungen.
3. Passen Sie bei Bedarf die Einstellungen der erweiterten Bildfunktionen und administrativen Steuerung an.
4. Klicken Sie auf **Speichern**.

Konfigurieren von "E-Mail an eigene Adresse"

"E-Mail an eigene Adresse" ermöglicht Benutzern das Senden einer Kopie der E-Mail an Ihre eigene E-Mail-Adresse. Weitere Informationen finden Sie im *Administratorhandbuch für "E-Mail an eigene Adresse"*.

Führen Sie je nach Druckermodell einen der folgenden Schritte aus:

Für die integrierte Version der Anwendung vorgesehen

1. Klicken Sie im Embedded Web Server auf **Einstellungen** > **E-Mail** > **E-Mail Standardeinstellungen** > **Admin-Steuerung**.
2. Wählen Sie **E-Mail-Empfänger begrenzen**.
3. Klicken Sie auf **Speichern**.

Für die Anwendung "Embedded Solutions Framework (eSF)"

1. Navigieren Sie über den Embedded Web Server zur Konfigurationsseite der Anwendung:

   Apps > **E-Mail an eigene Adresse** > **Konfigurieren**
2. Wählen Sie **Aktivieren**.
3. Klicken Sie auf **Übernehmen**.

Konfigurieren der Anwendungen

Konfigurieren des Smartcard-Authentifizierungsclients

Zur Konfiguration der Anwendung benötigen Sie möglicherweise Administratorrechte.

Konfigurieren der Einstellungen für den Anmeldebildschirm

Verwenden Sie die Einstellungen für den Anmeldebildschirm, um festzulegen, wie sich Benutzer am Drucker anmelden sollen.

1. Navigieren Sie über den Embedded Web Server zur Konfigurationsseite der Anwendung:

   Apps > **Smart Card Authentication Client** > **Konfigurieren**

2. Wählen Sie im Abschnitt "Anmeldebildschirm" die Anmeldemethode aus.
3. Wählen Sie im Menü "Benutzervalidierungsmodus" die Methode zur Überprüfung von Benutzerzertifikaten aus.
   - **Active Directory**: Das Benutzerzertifikat auf der Smartcard wird mit Kerberos-Authentifizierung validiert. Diese Einstellung erfordert eventuell LDAP-Suchen.
   - **Active Directory mit Gastzugriff**: Benutzer, die über Smartcards verfügen, aber nicht im Active Directory verzeichnet sind, können auf einige der Druckerfunktionen zugreifen. Ein korrekt konfiguriertes Online Certificate Status Protocol (OCSP)-Server ist erforderlich. Wenn die Active Directory-Authentifizierung fehlschlägt, versucht die Anwendung, die Daten beim OCSP Server abzurufen.
   - **Nur mit Pin**: Benutzer erhalten nur Zugriff auf Anwendungen oder Funktionen, die keine Kerberos-Authentifizierung erfordern.
4. Wählen Sie im Menü "Smartcard validieren" die Methode für die Authentifizierung von Benutzern nach Nutzung einer Smartcard.
5. Erlauben Sie den Benutzern gegebenenfalls, die Anmeldemethode zu ändern.
6. Klicken Sie auf **Übernehmen**.

Konfigurieren der Einstellungen für die manuelle Anmeldung

Der Drucker verwendet für die manuelle Anmeldung die in der Kerberos-Konfigurationsdatei hinterlegte Standard-Domäne. Wenn Sie eine andere Domäne nutzen, müssen Sie den Domänennamen in den Einstellungen für die manuelle Anmeldung angeben.

1. Navigieren Sie über den Embedded Web Server zur Konfigurationsseite der Anwendung:

   Apps > **Smart Card Authentication Client** > **Konfigurieren**

2. Geben Sie im Abschnitt "Einrichtung für manuelle Anmeldung" im Feld "Domänen für manuelle Anmeldung" eine oder mehrere Domänen ein.
3. Klicken Sie auf **Übernehmen**.

Konfigurieren der Smartcard-Einstellungen

Hinweis: Stellen Sie sicher, dass die Netzwerkverbindung zwischen Drucker und Authentifizierungsserver richtig konfiguriert ist. Weitere Informationen erhalten Sie beim Systemadministrator.

1. Navigieren Sie über den Embedded Web Server zur Konfigurationsseite der Anwendung:

   Apps > **Smart Card Authentication Client** > **Konfigurieren**

2. Führen Sie im Menü "Kerberos-Informationen" im Abschnitt "Smartcard-Setup" einen der folgenden Schritte aus:
   - **Kerberos-Konfigurationsdatei des Geräts verwenden**: Eine Kerberos-Konfigurationsdatei muss manuell auf dem Drucker installiert werden. Gehen Sie folgendermaßen vor:
     a. Klicken Sie im Embedded Web Server auf **Einstellungen** > **Sicherheit** > **Anmeldemethoden**.
     b. Klicken Sie im Abschnitt "Netzwerkkonten" auf **Anmeldemethode hinzufügen** > **Kerberos**.
     c. Gehen Sie vom Abschnitt "Kerberos-Datei importieren" aus zur entsprechenden Datei "krb5.conf".
     d. Wenn Ihr Netzwerk kein Reverse DNS Lookup verwendet, wählen Sie im Abschnitt "Verschiedene Einstellungen" die Option **Reverse IP Lookups deaktivieren**.
     e. Klicken Sie auf **Speichern und überprüfen**.
   - **Einfaches Kerberos-Setup verwenden**: Auf dem Drucker wird automatisch eine Kerberos-Datei erzeugt. Geben Sie Folgendes an:
     - **Bereich**: Der Bereich muss in Großbuchstaben eingegeben werden.
     - **Domänencontroller**: Trennen Sie mehrere Werte durch ein Komma. Die Domänencontroller werden in der aufgeführten Reihenfolge validiert.
     - **Domäne**: Geben Sie die Domäne an, die dem im Feld "Bereich" angegebenen Kerberos-Bereich zugeordnet werden soll. Trennen Sie mehrere Domänen durch ein Komma.

       Hinweis: Bei der Eingabe der Domäne muss die Groß- /Kleinschreibung beachtet werden.
     - **Zeitsperre**: Geben Sie einen Wert zwischen 3 und 30 Sekunden ein.

3. Wählen Sie im Menü "Domänencontrollerüberprüfung" die Methode zur Überprüfung des Domänencontrollerzertifikats aus.

   Hinweis: Bevor Sie diese Einstellung konfigurieren, müssen Sie sicherstellen, dass die entsprechenden Zertifikate auf dem Drucker installiert sind. Weitere Informationen finden Sie unter "Manuelles Installieren von Zertifikaten" auf Seite 7.
   - **Überprüfung des Gerätezertifikats verwenden**: Das auf dem Drucker installierte CA-Zertifikat wird verwendet.
   - **Überprüfung der Gerätekette verwenden**: Die gesamte auf dem Drucker installierte Zertifikatskette wird verwendet.
   - **OCSP-Überprüfung verwenden**: Der OCSP Server wird verwendet. Die gesamte Zertifikatkette muss auf dem Drucker installiert sein. Konfigurieren Sie im Abschnitt "Online Zertifikat Status Protocol (OCSP)" Folgendes:
     - **Responder-URL**: Die IP-Adresse oder der Hostname des OCSP-Responders/-Repeaters und die verwendete Port-Nummer. Trennen Sie mehrere Werte durch ein Komma.
       Zum Beispiel **`http://x:y`**, wobei ***x*** die IP-Adresse oder der Hostname und ***y*** die Port-Nummer ist.
     - **Responder-Zertifikat**: Das Zertifikat X.509 wird verwendet.

- **Responder-Zeitsperre**: Geben Sie einen Wert zwischen 5 und 30 Sekunden ein.
- **Unbekannten Status zulassen**: Benutzer können sich auch dann anmelden, wenn der Status eines oder mehrerer Zertifikate unbekannt ist.

4 Klicken Sie auf **Übernehmen**.

Konfigurieren erweiterter Einstellungen

1 Navigieren Sie über den Embedded Web Server zur Konfigurationsseite der Anwendung:

Apps > **Smart Card Authentication Client** > **Konfigurieren**

2 Wählen Sie im Bereich "Erweiterte Einstellungen" eine Benutzer-ID für diese Sitzung aus.

Hinweis: Einige Anwendungen, wie z. B. "Sichere zurückgehaltene Druckaufträge" und "Sichere E-Mail", erfordern einen Wert für die Benutzer-ID der Sitzung.

3 Im Menü "Absenderadresse der E-Mail" wählen Sie aus, wo der Drucker die Benutzer-E-Mail-Adresse abrufen soll.

4 Wählen Sie bei Bedarf **Auf Benutzerinformationen warten** aus, um alle Benutzerinformationen abzurufen, bevor der Benutzer die Erlaubnis erhält, auf den Startbildschirm oder eine sichere Anwendung zuzugreifen.

Wenn die folgenden Einstellungen auf "LDAP-Suche" eingestellt sind, wählen Sie diese Option aus.

- Benutzer-ID für Sitzung
- Absenderadresse der E-Mail

Wenn die folgenden Einstellungen nicht leer sind, wählen Sie diese Option aus.

- Andere Benutzerattribute
- Gruppenautorisierungsliste

Hinweis: Bei Verwendung der manuellen Anmeldung für "Sichere E-Mail" wählen Sie diese Option aus, um die Benutzer-E-Mail-Adresse in der Anmeldesitzung zu hinterlegen. Damit Benutzer, die sich manuell anmelden, E-Mails an sich selbst senden können, aktivieren Sie "Kopie an mich" in den E-Mail-Einstellungen des Druckers.

5 Wählen Sie ggf. **SSL für Benutzerinfo verwenden**, um Benutzerinformationen vom Domänencontroller über eine SSL-Verbindung abzurufen.

6 Geben Sie ggf. im Feld "Andere Benutzerattribute" weitere LDAP-Attribute ein, die der Sitzung hinzugefügt werden müssen. Trennen Sie mehrere Werte durch ein Komma.

7 Geben Sie in der Gruppenautorisierungsliste die Active Directory-Gruppen ein, die auf Anwendungen oder Funktionen zugreifen dürfen. Trennen Sie mehrere Werte durch ein Komma.

Hinweis: Die Gruppen müssen auf dem LDAP-Server hinterlegt sein.

8 Wenn DNS in Ihrem Netzwerk nicht aktiviert ist, laden Sie eine "hosts"-Datei hoch.

Geben Sie die Zuordnungen im folgenden Format in die Textdatei ein: ***xy***, wobei ***x*** die IP-Adresse und ***y*** der Hostname ist. Sie können einer IP-Adresse mehrere Hostnamen zuweisen. Beispiel: **`255.255.255.255.0.0 HostName1 HostName2 HostName3`**.

Einem Hostnamen können nicht mehrere IP-Adressen zugewiesen werden. Um Hostnamensgruppen IP-Adressen zuzuweisen, geben Sie jede IP-Adresse und die zugehörigen Hostnamen in eine separate Zeile der Textdatei ein.

Beispiel:

```
123.123.123.123 HostName1 HostName2
456.456.456.456 HostName3
```

9 Klicken Sie auf **Übernehmen**.

Konfigurieren von "Sichere E-Mail"

Zur Konfiguration der Anwendung benötigen Sie möglicherweise Administratorrechte.

Konfigurieren der Einstellungen für "Sichere E-Mail"

1 Navigieren Sie über den Embedded Web Server zur Konfigurationsseite der Anwendung:

Apps > **Sichere E-Mail** > **Konfigurieren**

2 Konfigurieren Sie die Einstellungen.

Hinweise:

- Zum digitalen Signieren einer E-Mail müssen Sie über ein gültiges digitales Signierungszertifikat verfügen und mit einer Smartcard angemeldet sein. Signierungszertifikate sind nur über die Smartcard verfügbar. Weitere Informationen erhalten Sie beim Systemadministrator.
- Damit ein Empfänger verschlüsselte E-Mails erhalten kann, muss er im Adressbuch des LDAP-Servers verzeichnet sein und über ein gültiges Verschlüsselungszertifikat verfügen. Weitere Informationen finden Sie unter "Konfiguration der LDAP-Einstellungen für Netzwerkkonten" auf Seite 9.
- Um eine Sicherheitskennzeichnung auf eine E-Mail anzuwenden, aktivieren Sie die Einstellung und geben dann den Text ein, den Sie verwenden möchten.
- Weitere Informationen zu den einzelnen Einstellungen finden Sie in der jeweiligen QuickInfo.

3 Klicken Sie auf **Übernehmen**.

Konfigurieren von "Angehaltene Druckaufträge sichern"

Zugriff von nicht autorisierten Benutzern auf "Angehaltene Aufträge" einschränken

Mit der integrierten Anwendung "Angehaltene Aufträge" können alle angehaltenen Aufträge im Drucker angezeigt werden. Nach dem Einrichten von "Angehaltene Druckaufträge sichern", entfernen Sie das Symbol "Angehaltene Aufträge" vom Startbildschirm des Druckers.

1 Klicken Sie im Embedded Web Server auf **Einstellungen** > **Gerät** > **Sichtbare Symbole auf Startbildschirm**.

2 **Angehaltene Aufträge** löschen.

3 Klicken Sie auf **Speichern**.

Einstellungen zum Konfigurieren von "Angehaltene Druckaufträge sichern"

1. Navigieren Sie über Embedded Web Server zur Konfigurationsseite der Anwendung.

   Apps > **Angehaltene Aufträge sicher** > **Konfigurieren**

2. Konfigurieren Sie im Abschnitt "Freigabeoptionen" die Einstellungen.
   - **Freigabemethode**—Legen Sie fest, wie Benutzer Ihre angehaltenen Aufträge drucken können.
   - **Druckaufträge anzeigen sortiert nach**—Legen Sie fest, wie die Druckaufträge auf dem Display angezeigt werden.
3. Klicken Sie auf **Übernehmen**.

Einstellung von Standard-Druckaufträge zu "Angehaltene Druckaufträge sichern" ändern

1. Klicken Sie in Embedded Web Server auf **Einstellungen** > **Sicherheit** > **Druckeinrichtung für vertrauliche Aufträge**.
2. Wählen Sie **Anhalten aller Aufträge erfordern** aus.
3. Klicken Sie auf **Speichern**.

Importieren oder Exportieren einer Konfigurationsdatei

Hinweis: Beim Importieren von Konfigurationsdateien werden die vorhandenen Anwendungskonfigurationen überschrieben.

1. Navigieren Sie über den "Embedded Web Server" zur Konfigurationsseite der Anwendung. Führen Sie einen der folgenden Schritte durch:
   - Klicken Sie auf **Apps** > **Smart Card Authentication Client** > **Konfigurieren**
   - Klicken Sie auf **Apps** > **Secure E-Mail** > **Konfigurieren**
   - Klicken Sie auf **Apps** > **Secure Held Print Jobs** > **Konfigurieren**
2. Klicken Sie auf **Importieren** oder **Exportieren**.

Verwenden der Anwendungen

E-Mail sichern

Versenden digital signierter und verschlüsselter E-Mails

Hinweise:

- Wenn Sie sich manuell anmelden, sollten Sie die Authentifizierungs-Einstellungen für den Smartcard-Authentifizierungsclient darauf konfigurieren, alle Benutzerinformationen abzurufen. Weitere Informationen finden Sie im *Administratorhandbuch zum Smartcard-Authentifizierungsclient*.
- Stellen Sie sicher, dass Ihrem Konto eine gültige E-Mail-Adresse zugewiesen ist, um eine E-Mail versenden zu können.

1. Melden Sie sich am Drucker an.
2. Drücken Sie auf dem Startbildschirm des Druckers das Anwendungssymbol.
3. Legen Sie ein Dokument in das Fach der automatischen Dokumentzuführung (ADZ) oder auf das Scannerglas.
4. Geben Sie die E-Mail-Adresse des Empfängers ein. Trennen Sie mehrere E-Mail-Adressen durch ein Komma.
5. Konfigurieren Sie bei Bedarf weitere E-Mail- und Scaneinstellungen.
6. Betätigen Sie **Senden**.
7. Signieren Sie die E-Mail digital oder verschlüsseln Sie sie.

   Hinweis: Zum digitalen Signieren einer E-Mail müssen Sie über ein gültiges digitales Signierungszertifikat verfügen und mit einer Smartcard angemeldet sein. Signierungszertifikate sind nur über die Smartcard verfügbar. Weitere Informationen erhalten Sie beim Systemadministrator.
8. Wählen Sie, sofern erforderlich, eine Sicherheitsoption aus.
9. Betätigen Sie **Senden**.
10. Wenn ein Verschlüsselungsfehler auftritt, gehen Sie folgendermaßen vor:
    - Zum Senden einer verschlüsselten E-Mail nur an Empfänger mit Verschlüsselungszertifikaten wählen Sie **Verschlüsselte senden**.
    - Zum Senden einer unverschlüsselten E-Mail an alle Empfänger wählen Sie **Unverschlüsselt senden**.
11. Betätigen Sie **Senden**.

Angehaltene Druckaufträge sichern

Drucken angehaltener Aufträge

Hinweise:

- Stellen Sie sicher, dass Sie die Einstellung von Standard-Druckaufträge zu "Angehaltene Druckaufträge sichern" ändern. Weitere Informationen finden Sie unter "Einstellung von Standard-Druckaufträge zu 'Angehaltene Druckaufträge sichern' ändern" auf Seite 17.
- Wenn Sie die Funktion "Drucken und Zurückhalten" verwenden, stellen Sie sicher, dass der Druckertreiber diese unterstützt. Weitere Informationen finden Sie in der *Druckertreiber-QuickInfo*. Sie können den Lexmark Universaldruckertreiber für Windows oder den Druckertreiber für Macintosh unter **www.lexmark.com** herunterladen.

1. Klicken Sie bei einem geöffnetem Dokument auf **Datei** > **Drucken**.
2. Wählen Sie einen Drucker aus.

   Hinweis: Passen Sie gegebenenfalls die Druckeinstellungen an.
3. Verwenden Sie gegebenenfalls die Funktion "Drucken und Zurückhalten".
   a. Aktivieren Sie die Funktion "Drucken und Zurückhalten".
      - Windows-Benutzer müssen auf **Eigenschaften**, **Einstellungen**, **Optionen** oder **Einrichtung** und dann auf **Drucken und Zurückhalten** klicken.
      - Macintosh-Benutzer wählen **Drucken und Zurückhalten** im Menü "Optionen" aus.

   b. Wählen Sie die Druckauftragsart aus.
      - **Reservieren**—Senden Sie Druckaufträge und speichern Sie sie im Druckerspeicher, um weitere Kopien später zu drucken.
      - **Überprüfen**—Druckt das erste Exemplar eines aus mehreren Exemplaren bestehenden Druckauftrags zur Überprüfung. Die restlichen Exemplare werden zurückgehalten, bis Sie sie drucken oder den Druck abbrechen.
      - **Wiederholen**—Druckt den Auftrag direkt und speichert eine Kopie im Druckerspeicher, so dass zu einem späteren Zeitpunkt weitere Kopien gedruckt werden können.

      Hinweis: Die Anwendung "Angehaltene Druckaufträge sichern" unterstützt keine vertraulichen Druckaufträge.

   c. Geben Sie den dem Druckauftrag zugeordneten Benutzernamen aus dem LDAP-Verzeichnis ein.
4. Klicken Sie auf **OK** oder **Drucken**.
5. Melden Sie sich vom Startbildschirm des Druckers bei Ihrem Konto an und drücken Sie dann auf das Anwendungssymbol.

   Hinweise:

   - Stellen Sie sicher, dass Sie bei der Anmeldung am Drucker das gleiche Konto verwenden wie beim Senden von Druckaufträgen.
   - Je nachdem, wie die Anwendung konfiguriert ist, werden alle Aufträge in der Druckfreigabe-Warteschlange möglicherweise automatisch gedruckt, sobald Sie das Anwendungssymbol drücken. Weitere Informationen finden Sie unter "Einstellungen zum Konfigurieren von 'Angehaltene Druckaufträge sichern'" auf Seite 17.

6 Geben Sie Ihre Authentifizierungsinformationen ein, sobald Sie dazu aufgefordert werden.

7 Wählen Sie die Aufträge, die Sie drucken möchten, und geben Sie die dann die Anzahl der zu druckenden Kopien an.

8 Berühren Sie **Drucken**.

Fehlerbehebung

Anwendungsfehler

Probieren Sie eine oder mehrere der folgenden Methoden:

Überprüfen Sie das Diagnoseprotokoll.

1. Öffnen Sie den Webbrowser und geben Sie dann ***IP*/se** ein, wobei ***IP*** für die IP-Adresse des Druckers steht.
2. Klicken Sie auf **Embedded Solutions**, und tun Sie dann Folgendes:
   a. Bereinigen Sie die Protokolldatei.
   b. Legen Sie die Erfassungsebene auf **Ja** fest.
   c. Erzeugen Sie die Protokolldatei.
3. Analysieren Sie das Protokoll und lösen Sie dann das Problem.

   Hinweis: Nachdem das Problem gelöst wurde, legen Sie die Erfassungsebene auf **Nein** fest.

Wenden Sie sich an Ihren Ansprechpartner bei Lexmark.

Anmeldeprobleme

Der Kartenleser oder die Smartcard wurde nicht erkannt.

Probieren Sie eine oder mehrere der folgenden Methoden:

Stellen Sie sicher, dass der Kartenleser ordnungsgemäß an den Drucker angeschlossen ist.

Stellen Sie sicher, dass der Kartenleser und die Smartcard kompatibel sind.

Stellen Sie sicher, dass der Kartenleser unterstützt wird.

Eine Liste der unterstützten Smartcard-Leser finden Sie in der *Readme*-Datei.

Stellen Sie sicher, dass der Treiber für den Kartenleser im Drucker installiert ist.

Wenden Sie sich an Ihren Ansprechpartner bei Lexmark.

Benutzer ist gesperrt

Probieren Sie eine oder mehrere der folgenden Methoden:

Erhöhen der zulässigen Anzahl von fehlgeschlagenen Anmeldeversuchen und der Zeitsperre

Hinweis: Diese Lösung kann nur bei bestimmten Druckermodellen angewendet werden.

1. Klicken Sie im Embedded Web Server auf **Einstellungen** > **Sicherheit** > **Anmeldeeinschränkungen**.
2. Erhöhen Sie die zulässigen Anzahl von fehlgeschlagenen Anmeldeversuchen und die Dauer der Zeitsperre.
3. Klicken Sie auf **Speichern**.

   Hinweis: Die neuen Einstellungen werden nach dem Ablauf der Sperrzeit wirksam.

Setzen Sie die Smartcard zurück oder tauschen Sie sie aus

PIN kann nicht überprüft werden

Probieren Sie eine oder mehrere der folgenden Methoden:

Stellen Sie sicher, dass Sie die korrekte PIN eingegeben haben.

Wenden Sie sich an Ihren Systemadministrator.

manuelle Anmeldung nicht möglich

Probieren Sie eine oder mehrere der folgenden Methoden:

Stellen Sie sicher, dass die in der Kerberos-Konfiguration angegebene Domäne korrekt ist

Geben Sie die Domänen in den Einstellungen für die manuelle Anmeldung ein.

Weitere Informationen finden Sie unter "Konfigurieren der Einstellungen für die manuelle Anmeldung" auf Seite 13.

Wenden Sie sich an Ihren Systemadministrator.

Startbildschirm des Druckers wird nicht gesperrt

Probieren Sie eine oder mehrere der folgenden Methoden:

Stellen Sie sicher, dass "Anpassung Display" aktiviert ist.

Weitere Informationen finden Sie im *Administrator-Handbuch für Anzeigenanpassung*.

Sichern Sie den Zugriffs auf den Startbildschirm

Weitere Informationen finden Sie unter "Sichern des Zugriffs auf den Startbildschirm" auf Seite 9.

Authentifizierungsprobleme

Kerberos-Authentifizierung fehlgeschlagen

Probieren Sie eine oder mehrere der folgenden Methoden:

Überprüfen Sie das Diagnoseprotokoll.

1. Öffnen Sie den Webbrowser und geben Sie dann ***IP*/se** ein, wobei ***IP*** für die IP-Adresse des Druckers steht.
2. Klicken Sie auf **Embedded Solutions**, und tun Sie dann Folgendes:
   a. Bereinigen Sie die Protokolldatei.
   b. Legen Sie die Erfassungsebene auf **Ja** fest.
   c. Erzeugen Sie die Protokolldatei.
3. Analysieren Sie das Protokoll, und lösen Sie dann das Problem.

   Hinweis: Nachdem der Analyse des Protokolls legen Sie die Erfassungsebene auf **Nein** fest.

Stellen Sie sicher, dass die Konfigurationsdatei auf dem Drucker installiert ist

- Wenn Sie die Kerberos-Konfigurationsdatei anhand des einfachen Kerberos-Setups erstellen möchten, gehen Sie folgendermaßen vor:
  1. Navigieren Sie über den Embedded Web Server zur Konfigurationsseite der Anwendung:
     Apps > **Smart Card Authentication Client** > **Konfigurieren**
  2. Stellen Sie im einfachen Kerberos-Setup sicher, dass die Werte in den Feldern "Bereich", "Domänencontroller", "Domäne" und "Zeitsperre" korrekt sind.
- Wenn Sie die Kerberos-Konfigurationsdatei des Geräts verwenden, gehen Sie folgendermaßen vor:
  1. Klicken Sie im Embedded Web Server auf **Einstellungen** > **Sicherheit** > **Anmeldemethoden**.
  2. Klicken Sie im Abschnitt "Netzwerkkonten" auf **Kerberos** > **Datei anzeigen**.
  3. Wenn die Kerberos-Konfigurationsdatei nicht installiert ist, dann gehen Sie im Abschnitt "Kerberos-Datei importieren" zur entsprechenden Datei "krb5.conf".
  4. Klicken Sie auf **Speichern und überprüfen**.

Vergewissern Sie sich, dass Inhalte und Format der Konfigurationsdatei korrekt sind

- Wenn Sie das einfache Kerberos-Setup verwenden, ändern Sie die Einstellungen für das einfache Kerberos-Setup.
- Wenn Sie die Kerberos-Konfigurationsdatei des Geräts verwenden, ändern Sie die Datei und installieren Sie sie erneut.

Stellen Sie sicher, dass der Kerberos-Bereich in Großbuchstaben angegeben ist

- Bei Verwendung des einfachen Kerberos-Setup gehen Sie folgendermaßen vor:
  1. Navigieren Sie über den Embedded Web Server zur Konfigurationsseite der Anwendung:
     Apps > **Smart Card Authentication Client** > **Konfigurieren**
  2. Stellen Sie im Abschnitt "Einfaches Kerberos-Setup" sicher, dass der Bereich richtig ist und in Großbuchstaben eingegeben wurde.

3 Klicken Sie auf **Übernehmen**.

- Wenn Sie die Kerberos-Konfigurationsdatei des Geräts verwenden, gehen Sie folgendermaßen vor:
  1 Klicken Sie im Embedded Web Server auf **Einstellungen** > **Sicherheit** > **Anmeldemethoden**.
  2 Klicken Sie im Abschnitt "Netzwerkkonten" auf **Kerberos** > **Datei anzeigen**.
  3 Stellen Sie sicher, dass die Bereiche in der Konfigurationsdatei in Großbuchstaben eingegeben wurden.

Geben Sie die Domäne des Microsoft® Windows® Betriebssystems an

- Bei Verwendung des einfachen Kerberos-Setup gehen Sie folgendermaßen vor:
  1 Navigieren Sie über den Embedded Web Server zur Konfigurationsseite der Anwendung: **Apps** > **Smart Card Authentication Client** > **Konfigurieren**
  2 Fügen Sie im Abschnitt "Einfaches Kerberos-Setup" im Domänenfeld die Windows-Domäne hinzu. Wenn der Wert im Feld "Domäne" **`DomainName,.DomainName`** und der Name der Windows-Domäne **`x.y.z`** lautet, dann ändern Sie den Wert im Feld "Domäne" in **`DomainName,.DomainName,x.y.z`**.

     Hinweis: Bei der Eingabe der Domäne muss die Groß- /Kleinschreibung beachtet werden.
  3 Klicken Sie auf **Übernehmen**.
- Wenn Sie die Kerberos-Konfigurationsdatei des Geräts verwenden, fügen Sie im Abschnitt **`domain_realm`** der Datei einen Eintrag hinzu. Geben Sie den Domänenbereich für Windows in Großbuchstaben ein, und installieren Sie dann die Datei erneut auf dem Drucker.

Wenden Sie sich an Ihren Ansprechpartner bei Lexmark.

Zertifikatsinformationen können nicht auf der Smartcard erzeugt oder gelesen werden

Probieren Sie eine oder mehrere der folgenden Methoden:

Stellen Sie sicher, dass die Zertifikatsinformationen auf der Smartcard richtig sind

Wenden Sie sich an Ihren Ansprechpartner bei Lexmark.

Domänencontroller kann nicht überprüft werden

Probieren Sie eine oder mehrere der folgenden Methoden:

Stellen Sie sicher, dass Bereich, Domänencontroller und Domäne in der Kerberos-Konfigurationsdatei korrekt sind

- Bei Verwendung des einfachen Kerberos-Setup gehen Sie folgendermaßen vor:
  1 Navigieren Sie über den Embedded Web Server zur Konfigurationsseite der Anwendung: **Apps** > **Smart Card Authentication Client** > **Konfigurieren**
  2 Stellen Sie im einfachen Kerberos-Setup sicher, dass die Werte in den Feldern "Bereich", "Domänencontroller" und "Domäne" korrekt sind.

- Wenn Sie die Kerberos-Konfigurationsdatei des Geräts verwenden, gehen Sie folgendermaßen vor:
  1. Klicken Sie im Embedded Web Server auf **Einstellungen** > **Sicherheit** > **Anmeldemethoden**.
  2. Klicken Sie im Abschnitt "Netzwerkkonten" auf **Kerberos-** > **Datei anzeigen**.
  3. Stellen Sie sicher, dass Bereich, Domänencontroller und Domäne korrekt sind.

Erhöhen Sie den Wert für die Zeitsperre des Domänencontrollers

- Bei Verwendung des einfachen Kerberos-Setup gehen Sie folgendermaßen vor:
  1. Navigieren Sie über den Embedded Web Server zur Konfigurationsseite der Anwendung:
     Apps > **Smart Card Authentication Client** > **Konfigurieren**
  2. Geben Sie aus dem Abschnitt "Einfaches Kerberos-Setup" im Feld "Zeitsperre" einen Wert von 3 bis 30 Sekunden ein.
  3. Klicken Sie auf **Übernehmen**.
- Wenn Sie die Kerberos-Konfigurationsdatei des Geräts verwenden, geben Sie einen Wert zwischen 3 und 30 Sekunden ein. Installieren Sie die Datei anschließend erneut auf dem Drucker. Weitere Informationen zum Konfigurieren der Smartcard-Einstellungen finden Sie unter "Konfigurieren der Smartcard-Einstellungen" auf Seite 14.

Stellen Sie sicher, dass der Domänencontroller verfügbar ist

Trennen Sie mehrere Werte durch ein Komma. Die Domänencontroller werden in der aufgeführten Reihenfolge validiert.

Stellen Sie sicher, dass Port 88 zwischen dem Drucker und dem Domänencontroller nicht blockiert ist

Domänencontrollerzertifikat kann nicht überprüft werden

Probieren Sie eine oder mehrere der folgenden Methoden:

Stellen Sie sicher, dass die auf dem Drucker installierten Zertifikate korrekt sind.

Weitere Informationen finden Sie unter "Manuelles Installieren von Zertifikaten" auf Seite 7.

Stellen Sie sicher, dass die Methode zur Prüfung des Domänencontrollers korrekt konfiguriert ist.

1. Navigieren Sie über den Embedded Web Server zur Konfigurationsseite der Anwendung:
   Apps > **Smart Card Authentication Client** > **Konfigurieren**
2. Wählen Sie im Abschnitt "Smartcard-Setup" im Menü "Domänencontrollerüberprüfung" die passende Überprüfungsmethode aus.
3. Klicken Sie auf **Übernehmen**.

Bereich in der Kerberos-Konfigurationsdatei nicht gefunden

Bereich hinzufügen oder ändern

- Bei Verwendung des einfachen Kerberos-Setup gehen Sie folgendermaßen vor:
  1. Navigieren Sie über den Embedded Web Server zur Konfigurationsseite der Anwendung:
     Apps > **Smart Card Authentication Client** > **Konfigurieren**
  2. Fügen Sie im Abschnitt "Einfaches Kerberos-Setup" im Feld "Bereich" den Bereich hinzu oder ändern Sie die Angabe des Bereichs. Der Bereich muss in Großbuchstaben eingegeben werden.

     Hinweis: Mehrere Einträge für den Kerberos-Bereich werden in vom Setup für das einfache Kerberos nicht unterstützt. Wenn mehrere Bereiche erforderlich sind, installieren Sie eine Kerberos-Konfigurationsdatei, in der die erforderlichen Bereiche enthalten sind.
  3. Klicken Sie auf **Übernehmen**.
- Wenn Sie die Kerberos-Konfigurationsdatei des Geräts verwenden, ändern oder ergänzen Sie den Bereich in der Datei. Der Bereich muss in Großbuchstaben eingegeben werden. Installieren Sie die Datei anschließend erneut auf dem Drucker.

Domänencontroller- und Geräteuhren sind nicht synchronisiert

Stellen Sie sicher, dass der Zeitunterschied zwischen dem Drucker und dem Domaincontroller fünf Minuten nicht übersteigt

Weitere Informationen finden Sie unter "Einstellen von Datum und Uhrzeit" auf Seite 8.

Domänencontroller-Zertifikatskette kann nicht überprüft werden

Probieren Sie eine oder mehrere der folgenden Methoden:

Stellen Sie sicher, dass alle für die Kettenüberprüfung erforderlichen Zertifikate auf dem Drucker installiert sind und dass die Angaben korrekt sind.

Weitere Informationen finden Sie unter "Manuelles Installieren von Zertifikaten" auf Seite 7.

Stellen Sie sicher, dass die Zertifikatskette vom Domänencontroller zum Root-CA verläuft.

Vergewissern Sie sich, dass keines der Zertifikate abgelaufen ist.

1. Klicken Sie im Embedded Web Server auf **Einstellungen** > **Sicherheit** > **Zertifikatsverwaltung**.
2. Stellen Sie sicher, dass die Datumsangaben "Gültig ab" und "Gültig bis" nicht abgelaufen sind.

Erlauben Sie, dass sich auch Benutzer anmelden können, wenn eines oder mehrere der Zertifikate unbekannt sind.

1. Navigieren Sie über den Embedded Web Server zur Konfigurationsseite der Anwendung:
   Apps > **Smart Card Authentication Client** > **Konfigurieren**
2. Konfigurieren Sie im Abschnitt "Online Zertifikat Status Protocol (OCSP)" die Option **Unbekannten Status zulassen**.

3 Klicken Sie auf **Übernehmen**.

Wenden Sie sich an Ihren Ansprechpartner bei Lexmark.

Keine Verbindung mit dem OCSP-Responder möglich

Probieren Sie eine oder mehrere der folgenden Methoden:

Stellen Sie sicher, dass die URL des OCSP-Responders richtig ist

1 Navigieren Sie über den Embedded Web Server zur Konfigurationsseite der Anwendung:

Apps > **Smart Card Authentication Client** > **Konfigurieren**

2 Überprüfen Sie im Abschnitt "Online Certificate Status Protocol (OCSP)", dass der Wert im Feld "Responder-URL" korrekt ist.

3 Klicken Sie auf **Übernehmen**.

Erhöhen Sie den Wert für die Responder-Zeitsperre.

1 Navigieren Sie über den Embedded Web Server zur Konfigurationsseite der Anwendung:

Apps > **Smart Card Authentication Client** > **Konfigurieren**

2 Geben Sie im Abschnitt "Online Zertifikat Status Protocol (OCSP)" im Feld "Responder-Zeitsperre" einen Wert zwischen 5 und 30 ein.

3 Klicken Sie auf **Übernehmen**.

Domänencontrollerzertifikat kann nicht gegen OCSP-Responder überprüft werden

Probieren Sie eine oder mehrere der folgenden Methoden:

Stellen Sie sicher, dass die URL des OCSP-Responder und das Responderzertifikat richtig konfiguriert sind.

1 Navigieren Sie über den Embedded Web Server zur Konfigurationsseite der Anwendung:

Apps > **Smart Card Authentication Client** > **Konfigurieren**

2 Geben Sie im Abschnitt "Online Zertifikat Status Protocol (OCSP)" im Feld "Responder URL" Folgendes an:

- IP-Adresse oder Hostnamen des OCSP-Responders/-Repeaters
- Verwendete Port-Nummer

Zum Beispiel **`http://x:y`**, wobei ***x*** die IP-Adresse und ***y*** die Port-Nummer ist.

3 Navigieren Sie im Feld "Responderzertifikat" zum entsprechenden Zertifikat.

4 Klicken Sie auf **Übernehmen**.

Stellen Sie sicher, dass vom Domänencontroller das richtige Zertifikat zurückgegeben wird.

Stellen Sie sicher, dass der OCSP-Responder das richtige Domänencontrollerzertifikat validiert.

Kein Zugriff auf einzelne Anwendungen oder Funktionen des Druckers

Probieren Sie eine oder mehrere der folgenden Methoden:

Erlauben Sie den sicheren Zugriff auf Anwendungen oder Funktionen

Weitere Informationen finden Sie unter "Sichern des Zugriffs auf einzelne Anwendungen und Funktionen" auf Seite 10.

Wenn der Benutzer einer Active Directory-Gruppe angehört, vergewissern Sie sich, dass die Gruppe für den Zugriff auf die Anwendungen und Funktionen berechtigt ist

Probleme bei "E-Mail sichern"

Senden von E-Mails mit der Anwendung nicht möglich

Stellen Sie sicher, dass die Anwendung "Device Quotas" deaktiviert ist.

Klicken Sie im Embedded Web Server auf **Apps** > **Device Quotas** > **Anhalten**.

Die Benutzer-E-Mail-Adresse kann nicht abgerufen werden.

Probieren Sie eine oder mehrere der folgenden Methoden:

Stellen Sie sicher, dass die E-Mail-Funktion des Druckers gesichert ist

Weitere Informationen finden Sie unter "Sichern des Zugriffs auf den Drucker" auf Seite 9.

Stellen Sie sicher, dass die E-Mail-Adresse korrekt abgerufen wird

1. Rufen Sie vom Embedded Web Server aus die Konfigurationsseite für den Smart Card Authentication Client auf:

   Apps > **Smart Card Authentication Client** > **Konfigurieren**
2. Im Abschnitt "Erweiterte Einstellungen" im Menü "Absenderadresse der E-Mail" wählen Sie aus, wo der Drucker die Benutzer-E-Mail-Adresse abrufen soll.
3. Aktivieren Sie **Auf Benutzerinformationen warten**.
4. Klicken Sie auf **Übernehmen**.

Wenden Sie sich an Ihren Ansprechpartner bei Lexmark.

Das Signierungszertifikat des Benutzers kann nicht abgerufen werden

Probieren Sie eine oder mehrere der folgenden Methoden:

Stellen Sie sicher, dass ein Signierungszertifikat für den Benutzer vorhanden ist.

Installieren Sie das Signierungszertifikat auf der Smartcard des Benutzers.

Vergewissern Sie sich, dass die Zertifikate richtig abgerufen werden.

1. Rufen Sie vom Embedded Web Server aus die Konfigurationsseite für den Smart Card Authentication Client auf:

   Apps > **Smart Card Authentication Client** > **Konfigurieren**
2. Wählen Sie im Abschnitt "Erweiterte Einstellungen" die Option **Auf Benutzerinformationen warten** aus.
3. Klicken Sie auf **Übernehmen**.

Wenden Sie sich an Ihren Ansprechpartner bei Lexmark.

Signierungszertifikat für den Benutzer nicht verfügbar

Probieren Sie Folgendes aus:

E-Mail ohne eine digitale Signatur versenden

Stellen Sie sicher, dass ein Signierungszertifikat für den Benutzer vorhanden ist.

Installieren Sie das Signierungszertifikat auf der Smartcard des Benutzers.

Wenden Sie sich an Ihren Systemadministrator.

Abrufen von Zertifikaten vom LDAP-Server nicht möglich

Probieren Sie eine oder mehrere der folgenden Methoden:

Vergewissern Sie sich, dass die Netzwerkkabel richtig angeschlossen und die Netzwerkeinstellungen für den Drucker ordnungsgemäß konfiguriert sind.

Weitere Informationen finden Sie im *Benutzerhandbuch* des Druckers.

Stellen Sie sicher, dass die Server- und Firewalleinstellungen so konfiguriert sind, dass der Drucker und der LDAP-Server über die Ports 389 oder 636 miteinander kommunizieren können.

Wenn Sie mit SSL verschlüsseln, können Sie Port **636** verwenden. Verwenden Sie andernfalls Port **389**.

Stellen Sie sicher, dass die LDAP-Serveradresse den Hostnamen und nicht die IP-Adresse enthält.

Weitere Informationen finden Sie unter "Konfiguration der LDAP-Einstellungen für Netzwerkkonten" auf Seite 9.

Wenn der LDAP-Server SSL-Verschlüsselung erfordert, sollten Sie darauf achten, dass die SSL-Einstellungen korrekt sind.

Weitere Informationen finden Sie unter "Konfiguration der LDAP-Einstellungen für Netzwerkkonten" auf Seite 9.

Grenzen Sie die LDAP-Suchbasis auf den kleinstmöglichen Suchbereich ein, der alle erforderlichen Benutzer umfasst.

Stellen Sie sicher, dass alle LDAP-Attribute korrekt sind.

Wenden Sie sich an Ihren Systemadministrator.

Verschlüsseln von E-Mails für einen oder mehrere Empfänger nicht möglich

Probieren Sie eine oder mehrere der folgenden Methoden:

Senden Sie eine unverschlüsselte E-Mail an Empfänger ohne Verschlüsselungszertifikat und eine verschlüsselte E-Mail an Empfänger mit einem Verschlüsselungszertifikat.

Wählen Sie **An alle senden**. Weitere Informationen finden Sie unter "Versenden digital signierter und verschlüsselter E-Mails" auf Seite 18.

Senden Sie eine verschlüsselte E-Mail nur an Empfänger mit Verschlüsselungszertifikaten.

Wählen Sie **Nur verschlüsselte senden**. Weitere Informationen finden Sie unter "Versenden digital signierter und verschlüsselter E-Mails" auf Seite 18.

Senden Sie eine unverschlüsselte E-Mail an alle Empfänger.

Wählen Sie **Unverschlüsselte senden**. Weitere Informationen finden Sie unter "Versenden digital signierter und verschlüsselter E-Mails" auf Seite 18.

Wenden Sie sich an Ihren Ansprechpartner bei Lexmark.

Keine Verbindung mit dem E-Mail-Server möglich

Probieren Sie eine oder mehrere der folgenden Methoden:

Stellen Sie sicher, dass der Drucker mit einer Domäne verbunden ist

Weitere Informationen finden Sie unter "Konfigurieren der TCP/IP-Einstellungen" auf Seite 8.

Stellen Sie sicher, dass die Einstellungen für die SMTP-Server-Authentifizierung richtig sind

1. Klicken Sie im Embedded Web Server auf **Einstellungen** > **E-Mail** > **E-Mail Setup**.
2. Führen Sie im Feld "SMTP-Server-Authentifizierung" einen der folgenden Schritte durch:
   - Wenn für den SMTP-Server Benutzeranmeldeinformationen erforderlich sind, wählen Sie **Kerberos 5**.
   - Falls Kerberos nicht unterstützt wird, wählen Sie **Keine Authentifizierung erforderlich**.
   - Wenn der SMTP-Server eine Authentifizierung erfordert, aber Kerberos nicht unterstützt, geben Sie im Feld "Antwortadresse" die IP-Adresse oder den Hostnamen des Druckers ein.
3. Klicken Sie auf **Speichern**.

Hinweis: Weitere Informationen finden Sie unter "Konfigurieren der SMTP-Einstellungen" auf Seite 11.

Wenn der SMTP-Server Kerberos verwendet, stellen Sie sicher, dass die Hostnamen des primären und sekundären SMTP-Gateways richtig sind

1. Klicken Sie im Embedded Web Server auf **Einstellungen** > **E-Mail** > **E-Mail Setup**.
2. Geben Sie in die Feldern "Primärer SMTP-Gateway" und "Sekundärer SMTP-Gateway" den Hostnamen des Gateways anstelle der IP-Adresse ein.
3. Klicken Sie auf **Speichern**.

Stellen Sie sicher, dass die Server- und Firewalleinstellungen so konfiguriert sind, dass der Drucker und der SMTP-Server über Port 25 miteinander kommunizieren können

Vergewissern Sie sich, dass die Netzwerkkabel richtig angeschlossen und die Netzwerkeinstellungen für den Drucker ordnungsgemäß konfiguriert sind.

Weitere Informationen finden Sie im *Benutzerhandbuch* des Druckers.

Wenden Sie sich an Ihren Systemadministrator.

Senden einer Kopie an die eigene Adresse nicht möglich

Probieren Sie eine oder mehrere der folgenden Methoden:

Stellen Sie sicher, dass sämtliche Benutzerinformationen in der Anmeldesitzung eingegeben sind.

Stellen Sie sicher, dass der Drucker zum Abruf aller Benutzerinformationen konfiguriert ist.

1. Rufen Sie vom Embedded Web Server aus die Konfigurationsseite für den Smart Card Authentication Client auf:

   Apps > **Smart Card Authentication Client** > **Konfigurieren**
2. Wählen Sie im Abschnitt "Erweiterte Einstellungen" die Option **Auf Benutzerinformationen warten** aus.
3. Klicken Sie auf **Übernehmen**.

Vergewissern Sie sich, dass der "E-Mail an eigene Adresse" richtig konfiguriert ist.

Weitere Informationen finden Sie unter "Konfigurieren von 'E-Mail an eigene Adresse'" auf Seite 12.

Wenden Sie sich an Ihren Ansprechpartner bei Lexmark.

Probleme bei "Angehaltene Druckaufträge sichern"

Kann die Benutzer-ID nicht ermitteln

Dieser Fehler weist darauf hin, dass das lokale Konto, Netzwerk-Konto, oder eine Anmeldemethode mit Authentifizierungsmodul nicht die Benutzer-ID für die Sitzung festlegt. Probieren Sie eine oder mehrere der folgenden Methoden:

Stellen Sie sicher, dass die Anwendung gesichert ist

Weitere Informationen finden Sie unter "Einstellungen zum Konfigurieren von 'Angehaltene Druckaufträge sichern'" auf Seite 17.

Vergewissern Sie sich, dass die Benutzer-ID der Sitzung ordnungsgemäß festgelegt ist

Führen Sie vom Embedded Web Server einen der folgenden Schritte aus:

Verwenden einer Anmeldemethode mit einem lokalen Konto

1. Klicken Sie auf **Einstellungen** > **Sicherheit** > **Anmeldmethoden**.
2. Klicken Sie im Abschnitt "Lokale Konten" auf den lokalen Kontotyp und stellen Sie dann sicher, dass das Konto über einen Benutzernamen verfügt.
3. Klicken Sie auf **Speichern**.

Verwenden einer Anmeldemethode mit einem Netzwerk-Konto

1. Klicken Sie auf **Einstellungen** > **Sicherheit** > **Anmeldmethoden**.
2. Klicken Sie im Abschnitt "Netzwerk-Konten" auf den Netzwerk-Kontotyp und stellen Sie dann sicher, dass das Konto über die korrekte Benutzer-ID verfügt. Weitere Informationen erhalten Sie beim Systemadministrator.
3. Klicken Sie auf **Speichern**.

Verwenden eines Authentifizierungsmoduls

1. Klicken Sie auf **Apps**.
2. Wählen Sie Authentifizierungsmodul aus, und klicken Sie dann auf **Konfigurieren**.
3. Legen Sie die entsprechenden Einstellungen für die Benutzer-ID dieser Sitzung fest.
4. Klicken Sie auf **Speichern** oder **Anwenden**.

Wenden Sie sich an Ihren Lösungsanbieter.

Wenn Sie das Problem weiterhin nicht lösen können, wenden Sie sich an den Anbieter Ihrer Lösung.

Es sind keine Druckaufträge für den Benutzer verfügbar

Probieren Sie eine oder mehrere der folgenden Methoden:

Vergewissern Sie sich, dass die Aufträge an den richtigen Drucker gesendet werden und nicht abgelaufen sind

Möglicherweise wurden die Aufträge vom Benutzer an einen anderen Drucker gesendet oder automatisch gelöscht, da sie nicht innerhalb der Frist gedruckt wurden.

Vergewissern Sie sich, dass die Benutzer-ID der Sitzung ordnungsgemäß festgelegt ist

Führen Sie vom Embedded Web Server einen der folgenden Schritte aus:

Verwenden einer Anmeldemethode mit einem lokalen Konto

1. Klicken Sie auf **Einstellungen** > **Sicherheit** > **Anmeldmethoden**.
2. Klicken Sie im Abschnitt "Lokale Konten" auf den lokalen Kontotyp und stellen Sie dann sicher, dass das Konto über einen Benutzernamen verfügt.
3. Klicken Sie auf **Speichern**.

Verwenden einer Anmeldemethode mit einem Netzwerk-Konto

1. Klicken Sie auf **Einstellungen** > **Sicherheit** > **Anmeldmethoden**.
2. Klicken Sie im Abschnitt "Netzwerk-Konten" auf den Netzwerk-Kontotyp und stellen Sie dann sicher, dass dem Konto die korrekte Benutzer-ID zugewiesen wird. Weitere Informationen erhalten Sie beim Systemadministrator.
3. Klicken Sie auf **Speichern**.

Verwenden eines Authentifizierungsmoduls

1. Klicken Sie auf **Apps**.
2. Wählen Sie Authentifizierungsmodul aus, und klicken Sie dann auf **Konfigurieren**.
3. Legen Sie die entsprechenden Einstellungen für die Benutzer-ID dieser Sitzung fest.
4. Klicken Sie auf **Speichern** oder **Anwenden**.

Wenden Sie sich an Ihren Lösungsanbieter.

Wenn Sie das Problem weiterhin nicht lösen können, wenden Sie sich an den Anbieter Ihrer Lösung.

LDAP-Probleme

Fehler bei LDAP-Suchen

Probieren Sie eine oder mehrere der folgenden Methoden:

Stellen Sie sicher, dass die Server- und Firewalleinstellungen so konfiguriert sind, dass der Drucker und der LDAP-Server über Port 389 und 636 miteinander kommunizieren können.

Deaktivieren Sie "Reverse-DNS-Lookup" in den Kerberos-Einstellungen, wenn es in Ihrem Netzwerk nicht verwendet wird.

1. Klicken Sie im Embedded Web Server auf **Einstellungen** > **Sicherheit**.
2. Klicken Sie im Abschnitt "Netzwerkkonten" auf **Kerberos**.
3. Wählen Sie im Abschnitt "Erweiterte Einstellungen" die Option **Reverse-IP-Lookups deaktivieren**.
4. Klicken Sie auf **Speichern und überprüfen**.

Wenn für den LDAP-Server SSL erforderlich ist, aktivieren Sie SSL für die LDAP-Suche

1. Navigieren Sie über den Embedded Web Server zur Konfigurationsseite der Anwendung:
   Apps > **Smart Card Authentication Client** > **Konfigurieren**
2. Wählen Sie im Abschnitt "Erweiterte Einstellungen" die Option **SSL für Benutzerinfo verwenden**.
3. Klicken Sie auf **Übernehmen**.

Grenzen Sie die LDAP-Suchbasis auf den kleinstmöglichen Suchbereich ein, der alle erforderlichen Benutzer umfasst.

Stellen Sie sicher, dass alle LDAP-Attribute korrekt sind.

Lizenzfehler

Wenden Sie sich an Ihren Ansprechpartner bei Lexmark

Hinweise

Hinweis zur Ausgabe

August 2017

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.

Den technischen Support von Lexmark finden Sie unter **http://support.lexmark.com**.

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

Marken

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

Microsoft, Windows und Active Directory sind eingetragene Marken oder Marken der Microsoft-Unternehmensgruppe in den USA und anderen Ländern.

Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber.

Index

F

G

H

I

K