Smart Card Authentication Client

Version 2.1

Administratorhandbuch

August 2017 **www.lexmark.com**

Inhalt

Änderungsverlauf

August 2017

- Hinzugefügte Anweisungen zum Ändern der Anmeldemethode.
- Hinzugefügte Unterstützung für brasilianisches Portugiesisch, Finnisch, Französisch, Deutsch, Italienisch, vereinfachtes Chinesisch und Spanisch.

Januar 2016

- Ursprüngliche Dokumentenveröffentlichung für Multifunktions-Produkte mit einem Tablet-ähnlichen Touchscreen-Display.

Übersicht

Nutzen Sie diese Anwendung zur Sicherung des Zugriffs auf Drucker, indem Benutzer aufgefordert werden, sich über eine Smartcard oder unter Angabe von Benutzernamen und Kennwort anzumelden. Sie können den Zugriff auf den Startbildschirm des Druckers bzw. auf einzelne Anwendungen und Funktionen absichern.

Zusätzlich bietet die Anwendung Optionen für die Kerberos-Authentifizierung sowie ein Kerberos-Ticket, das für die Sicherung anderer Anwendungen genutzt werden kann.

Dieses Dokument bietet Anleitungen zur Konfiguration und Fehlerbehebung dieser Anwendung.

Checkliste Einsatzbereitschaft

Stellen Sie Folgendes sicher:

- ☐ Im Drucker sind mindestens 512 MB RAM installiert.
- ☐ Im Drucker sind ein Smartcard-Leser und die zugehörigen Treiber installiert.

Zum Konfigurieren der Anwendung haben Sie die folgenden Informationen:

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

  _____
- ☐ Kerberos-Bereich, Domäne und Domänencontroller

  _____
- ☐ 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 7.

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 11.
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**.

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 12.

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 Zugriff auf eine Anwendung oder Druckerfunktion authentifizieren.

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

2 Klicken Sie im Abschnitt "Öffentlich" auf **Berechtigungen verwalten**.

3 Erweitern Sie eine oder mehrere Kategorien, entfernen Sie die Anwendung oder Funktion, die Sie sichern wollen, 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 12.

6 Erweitern Sie eine oder mehrere Kategorien, und wählen Sie die Anwendungen oder Funktionen aus, die für authentifizierte Benutzer verfügbar sein sollen.

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 Anwendung

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 6.

   - **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**.

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:

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

2 Klicken Sie auf **Importieren** oder **Exportieren**.

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.

Probleme bei der Anmeldung

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 10.

Wenden Sie sich an Ihren Systemadministrator.

Benutzer wird sofort nach der Anmeldung abgemeldet

Erhöhen Sie den Wert für die Anzeige-Zeitsperre.

Weitere Informationen finden Sie unter "Einstellung der Anzeige-Zeitsperre" auf Seite 6.

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 8.

Probleme bei der Authentifizierung

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 11.

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 6.

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 7.

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 6.

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 8.

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

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.

GNU Lesser General Public License

Weitere Informationen zur GNU Lesser General Public License finden Sie im Internet unter **http://www.gnu.org/licenses/lgpl.html**.

Additional copyrights

This product includes software developed by:

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

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

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

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

Index