



Uwierzytelnianie w chmurze

Podręcznik administratora

Zawartość

Historia zmian.....	4
Informacje ogólne.....	5
Lista kontrolna gotowości do wdrożenia.....	6
Konfigurowanie aplikacji.....	7
uzyskiwanie dostępu do wbudowanego serwera WWW.....	7
Ustawianie aplikacji jako domyślnej metody logowania.....	7
Konfigurowanie logowania administratora.....	7
Uzyskiwanie dostępu do strony konfiguracji aplikacji.....	8
Konfigurowanie ustawień uwierzytelnienia użytkownika.....	9
Konfigurowanie identyfikatora i tajnego klucza klienta.....	10
Konfigurowanie ustawień ekranu logowania.....	10
Włączanie dostępu publicznego do aplikacji oraz funkcji kopiowania i faksu.....	11
Konfigurowanie opóźnienia wylogowania karty.....	12
Konfigurowanie limitów czasu połączeń.....	12
Importowanie lub eksportowanie pliku konfiguracyjnego.....	13
Aktualizowanie okresu odpytywania.....	14
Konfigurowanie ustawień proxy drukarki.....	14
Korzystanie z aplikacji.....	16
Rejestrowanie karty.....	16
Uzyskiwanie kodu logowania.....	17
Ręczne logowanie się do drukarki.....	17
Uzyskiwanie kodu PIN.....	18
Rozwiązywanie problemów.....	19
Błąd aplikacji.....	19
Błąd uwierzytelniania.....	19
Rejestracja karty dostępu jest zabroniona.....	19
Nie można wysłać wiadomości e-mail z instrukcjami dotyczącymi kodu logowania.....	20
Przycisk Ręczne logowanie pojawia się w przypadku ujednoliconego uwierzytelniania organizacji.....	20
Nie można zalogować się przy użyciu kodu logowania.....	20

Nie można zarejestrować karty dostępu przez łącze do rejestracji z wiadomości e-mail.....	21
Nie otrzymano wiadomości e-mail z łączem do rejestracji karty dostępu.....	21
Nie można się połączyć z dostawcą usługi zarządzania tożsamościami.....	21
Kod PIN stracił ważność.....	21
Zbyt wiele nieudanych prób.....	22
Uwagi.....	23
Indeks.....	24

Historia zmian

Grudzień 2023

- Dodano informacje na temat obsługi współwystępowania Cloud Authentication i innych aplikacji uwierzytelniających innych firm.

Wrzesień 2021

- Usunięto obsługę ręcznego logowania.

Kwiecień 2021

- Dodano informacje na temat funkcji logowania administratora.

Grudzień 2019

- Dodano informacje na temat ostrzegania użytkownika w przypadku, gdy czytnik kart nie jest podłączony.
- Dodano informacje dotyczące resetowania kodu PIN.
- Zaktualizowano informacje na temat konfiguracji ustawień uwierzytelnionego serwera proxy.

Grudzień 2018

Zaktualizowano poniższe informacje:

- Konfigurowanie ustawień uwierzytelnienia użytkownika
- Ręczne logowanie się do drukarki

Dodano poniższe informacje:

- Konfigurowanie okresu odpytywania
- Konfigurowanie ustawień proxy drukarki
- Rejestrowanie karty dostępu przez łącze do rejestracji z wiadomości e-mail

Czerwiec 2018

- Zaktualizowano informacje dotyczące konfigurowania identyfikatora i tajnego klucza klienta.
- Zaktualizowano informacje dotyczące importowania i eksportowania plików konfiguracji.
- Dodano informacje dotyczące ustawiania aplikacji jako domyślnej metody logowania.

Styczeń 2018

- Wydanie pierwsze dokumentu.

Informacje ogólne

Użyj aplikacji, aby zabezpieczyć drukarkę za pomocą czytnika kart. Gdy użytkownicy rejestrują się przy użyciu karty, ich poświadczenia są uwierzytelniane za pomocą dostawcy usługi tożsamości wykorzystującego potencjał chmury.

Aplikacja została skonfigurowana oraz wdrożona na stronie Lexmark™ Cloud Platform. Ustawienia można także skonfigurować ręcznie, korzystając ze strony konfiguracji aplikacji.

W tym dokumencie zawarto informacje o konfigurowaniu i użytkowaniu aplikacji oraz o rozwiązywaniu problemów z aplikacją.

Lista kontrolna gotowości do wdrożenia

Zanim rozpoczniesz, upewnij się że:

- Któryś z obsługiwanych czytników kart i jego sterownik są zainstalowane w drukarce:
 - omnikey5427ckdriver-1.2.9.flis lub nowsza wersja
 - keyboardreader-2.4.8.flis lub nowsza wersja
 - omnikeydriver-2.4.5.flis lub nowsza wersja
- Znasz nazwę hosta lub adres IP następujących dostawców, które są wymagane w celu konfiguracji ustawień uwierzytelniania użytkownika:
 - Dostawcy usługi tożsamości
 - Dostawcy usługi karty
- Jeśli aplikacja nie jest wdrażana poprzez usługi przetwarzania w chmurze zarządzania flotą Lexmark, wówczas posiadasz identyfikator oraz tajny klucz klienta. Aby uzyskać więcej informacji, należy skontaktować się z przedstawicielem handlowym firmy Lexmark.
- Aplikacja Uwierzytelnianie kartą nie jest zainstalowana. Aby uzyskać więcej informacji, zapoznaj się z *Podręcznikiem administratora uwierzytelniania kartą*.

Uwagi:

- Podczas tworzenia konfiguracji dla aplikacji Cloud Print Management, Translation Assistant lub Cloud Scan Management należy upewnić się, że ustawienie Dołączany moduł uwierzytelniający zostało prawidłowo skonfigurowane. Jeśli drukarka nie jest zarządzana przez inną aplikację uwierzytelniającą, włącz to ustawienie. To ustawienie pozwala korzystać z Cloud Authentication jako głównej aplikacji uwierzytelniającej do zarządzania bezpieczeństwem drukarki.
 - Jeśli drukarka ma inną aplikację uwierzytelniającą zarządzającą jej bezpieczeństwem, pamiętaj o wyłączeniu ustawienia Dołączany moduł uwierzytelniający .
 - Więcej informacji na temat konfigurowania dołączanego modułu uwierzytelniającego można znaleźć w *Podręczniku administratora platformy Lexmark Cloud Services*.
 - Aplikacje Cloud Print Management mogą nie działać z niektórymi aplikacjami uwierzytelniającymi. Więcej informacji na temat ograniczeń znajdziesz w pliku *Cloud Authentication ReadMe*.
- W zależności od modelu drukarki wyłączone zostało jedno z następujących:
 - Funkcja Wygaszacz ekranu w aplikacji Dostosowywanie wyświetlacza. Aby uzyskać więcej informacji, zapoznaj się z *Podręcznikiem administratora dotyczącym dostosowywania wyświetlacza*.

Uwaga: Instalacja aplikacji Uwierzytelnianie w chmurze automatycznie wyłącza funkcję Wygaszacz ekranu w aplikacji Dostosowywanie wyświetlacza.

 - Aplikacja Tło i ekran oczekiwania. Aby uzyskać więcej informacji, zapoznaj się z *Podręcznikiem administratora dotyczącym tła i ekranu oczekiwania*.

Konfigurowanie aplikacji

Aby skonfigurować aplikację, mogą być wymagane uprawnienia administratora. Aplikacja jest wstępnie skonfigurowana z poziomu strony WWW Lexmark Cloud Platform. Ustawienia można skonfigurować ręcznie na stronie konfiguracji aplikacji.

Informacje dotyczące wersji aplikacji Embedded Solutions Framework (eSF) zainstalowanej w drukarce są dostępne w [dokumentacji pomocy](#).

uzyskiwanie dostępu do wbudowanego serwera WWW

- 1 Uzyskaj adres IP drukarki. Wykonaj jedną z następujących czynności:
 - Zlokalizuj adres IP na ekranie głównym drukarki.
 - Wyświetl adres IP w sekcji Przegląd sieci lub TCP/IP menu Sieć/Porty.
- 2 Uruchom przeglądarkę internetową, a następnie wpisz adres IP drukarki.

Ustawianie aplikacji jako domyślnej metody logowania

Ustawienia te mają zastosowanie tylko w przypadku drukarek z eSF w wersji 5.0 lub nowszej. Uwierzytelnienie w chmurze musi być ustawione jako domyślna metoda logowania.

Uwaga: Informacje dotyczące wersji aplikacji Embedded Solutions Framework (eSF) zainstalowanej w drukarce są dostępne w [dokumentacji pomocy](#).

- 1 W oknie wbudowanego serwera WWW kliknij **Ustawienia > Bezpieczeństwo > Metody logowania**.
- 2 Kliknij **Zmień** obok domyślnej metody logowania do panelu sterowania.
- 3 W menu panelu sterowania wybierz **Uwierzytelnienie w chmurze**.
- 4 Kliknij przycisk **Zapisz**.

Konfigurowanie logowania administratora

Uwagi:

- Ustawienia logowania administratora umożliwiają użytkownikom logowanie się przy użyciu autoryzowanego konta lokalnego, nawet jeśli drukarki z ekranem blokady uwierzytelniania w chmurze są odłączone od sieci.
- Podczas tworzenia konfiguracji w usługach zarządzania flotą usług w chmurze Lexmark w sekcji Ustawienia wybierz aplikację **Cloud Print Management**. W sekcji Ustawienia zaawansowane kliknij opcję **Pokaż opcję logowanie administratora na ekranie blokady**.
- Aby uzyskać więcej informacji na temat tworzenia konfiguracji logowania i wdrażania jej do drukarki, zapoznaj się z *Podręcznikiem administratora usług w chmurze Lexmark*.
- Aby zastosować konfigurację w wielu drukarkach lub we flocie, wyeksportuj konfigurację z drukarki, a następnie zastosuj tę samą konfigurację we flocie urządzeń.

Korzystanie z wbudowanego serwera WWW

W przypadku eSF w wersji 5.0 lub nowszej

1 Na serwerze Embedded Web Server przejdź do strony konfiguracji aplikacji:

Apps > Cloud Authentication > Configure

2 W sekcji Uwierzytelnianie użytkownika, Ustawienia logowania administratora ustaw Logowania administratora jako preferowaną metodę logowania.

Uwagi:

- Upewnij się, że skonfigurowano konto administratora lokalnego dla drukarki oraz że skonfigurowano uprawnienia dla grupy administratora urządzenia. W oknie wbudowanego serwera WWW kliknij kolejno opcje **Ustawienia > Bezpieczeństwo > Zarządzaj grupami/uprawnieniami**.
- Domyślnie funkcje i menu nie są dozwolone dla tej grupy.

3 Wybierz autoryzowaną grupę, która może korzystać z funkcji logowania administratora.

Uwaga: To ustawienie dotyczy tylko kont z nazwami użytkowników oraz kont z nazwami użytkowników i hasłami.

4 Wybierz opcję **Pokaż na wygaszaczu ekranu**, aby wyświetlić przycisk Logowanie administratora na wygaszaczu ekranu.

5 Kliknij **Zapisz**.

W przypadku eSF w wersji 4.0 lub starszej

Uwaga: W przypadku korzystania z funkcji Logowanie administratora należy upewnić się, że skonfigurowano szablon zabezpieczeń dla kont wewnętrznych, kodu PIN lub hasła. Więcej informacji można znaleźć w sekcji [„Konfigurowanie ustawień uwierzytelnienia użytkownika” na str. 9](#).

1 Z serwera Embedded Web Server otwórz stronę konfiguracji aplikacji.

2 W sekcji Uwierzytelnianie użytkowników ustaw funkcję Kontrola dostępu w przypadku logowania administratora dla preferowanej metody logowania.

Uwagi:

- Upewnij się, że wybrana kontrola dostępu została skonfigurowana za pomocą szablonu zabezpieczeń. Więcej informacji można znaleźć w sekcji [„Konfigurowanie ustawień uwierzytelnienia użytkownika” na str. 9](#).
- Aby ukryć opcję Logowanie administratora na panelu sterowania drukarki, wybierz opcję **Wyłącz**.

3 Kliknij **Zastosuj**.

Uzyskiwanie dostępu do strony konfiguracji aplikacji

1 Z poziomu wbudowanego serwera WWW wykonaj jedną z następujących czynności (w zależności od modelu drukarki):

- Kliknij **Aplikacje**.
- Kliknij opcję **Ustawienia > Aplikacje > Zarządzanie aplikacjami**.
- Kliknij kolejno **Ustawienia > Rozwiązania urządzenia > Rozwiązania (eSF)**.
- Kliknij kolejno **Konfiguracja > Rozwiązania wbudowane**.

2 Kliknij kolejno **Uwierzytelnianie w chmurze > Konfiguruj**.

Konfigurowanie ustawień uwierzytelnienia użytkownika

Uwagi:

- Począwszy od wersji eSF 5.2.x i 2.2.x ustawienia uwierzytelniania użytkownika dziedziczą ustawienia konfiguracji logowania do drukarki zdefiniowane dla organizacji, do której drukarka jest zapisana.
- Więcej informacji dotyczących wersji aplikacji Embedded Solutions Framework (eSF) zainstalowanej w drukarce jest dostępne w [dokumentacji pomocy](#).
- Aby uzyskać więcej informacji na temat konfigurowania logowania do drukarki, zapoznaj się z *Podręcznikiem administratora usług w chmurze Lexmark*.
- Ustawienia drukarki można zaktualizować poprzez dostawcę usług tożsamości albo używając identyfikatora klienta lub tajnego klucza klienta przypisanego do organizacji. Aby wyświetlić zaktualizowane ustawienia, po określeniu identyfikatora dostawcy usług tożsamości, zapisz ustawienia, a następnie odśwież stronę.

1 Z serwera Embedded Web Server otwórz stronę konfiguracji aplikacji.

2 W sekcji Ustawienia usług tożsamości wybierz opcję **Włącz ekran blokady** lub **Włącz ekran oczekiwania**.

3 Wprowadź adres IP, nazwę hosta lub adres URL dostawcy usługi tożsamości i dostawcy usługi karty.

4 Ustaw zasady dostępu aplikacji.

- **Kontynuuj** — jeśli połączenie z dostawcą usługi tożsamości nie powiedzie się, użytkownik może kontynuować korzystanie z drukarki.
- **Niepowodzenie** — jeśli połączenie z dostawcą usługi tożsamości nie powiedzie się, drukarka powróci do ekranu logowania.

5 Aby korzystać z bezpiecznego połączenia, prześlij identyfikator SSL dostawcy usługi tożsamości.

Uwaga: Więcej informacji na temat tworzenia certyfikatu SSL można znaleźć w dokumentacji przeglądarki internetowej.

6 Aby umożliwić użytkownikom logowanie się do drukarki za pomocą osobnego konta usługi, zaznacz opcję **Użyj konta usługi** i wprowadź poświadczenia konta usługi.

Uwaga: To ustawienie nie jest stosowane, gdy aplikacja jest skonfigurowana na dostęp ujednociony. Więcej informacji można znaleźć w sekcji „[Konfigurowanie identyfikatora i tajnego klucza klienta](#)” na [str. 10](#).

7 Spróbuj poniższych rozwiązań:

W przypadku eSF w wersji 5.0 lub nowszej

a W sekcji Ustawienia rejestracji karty wybierz wartość **Usługa tożsamości** dla ustawienia Rejestracja karty.

Uwaga: Jeśli Rejestracja karty jest ustawiona na **Wyłączona**, użytkownicy nie mogą rejestrować swoich kart.

b Kliknij **Zapisz**.

Dla eSF w wersji 3.x i 4.x

- a W sekcji Uwierzytelnianie użytkownika wybierz wartość **Usługa tożsamości** dla ustawienia Uwierzytelnianie kartą.
- b Ustaw wartość ustawienia Kontrola dostępu w przypadku rejestracji karty na **Usługa tożsamości**.
- c Kliknij **Zastosuj**.
- d Z poziomu wbudowanego serwera www kliknij **Ustawienia > Zabezpieczenia > Konfiguracja zabezpieczeń > Kontrola dostępu > Rozwiązania dla urządzenia**.
- e Ustaw Kontrolę dostępu do sesji na szablon zabezpieczeń skonfigurowany za pomocą usługi uwierzytelnienia w chmurze.
Uwaga: Domyślny szablon zabezpieczeń to Rozwiązanie 2.
- f Kliknij **Zastosuj**.

Konfigurowanie identyfikatora i tajnego klucza klienta

Identyfikator klienta i tajny klucz klienta są wykorzystywane do sprawdzania, czy dany użytkownik i drukarka są częścią tej samej organizacji.

Identyfikator klienta i tajny klucz klienta mogą być generowane z poziomu platformy Lexmark Cloud. Więcej informacji można znaleźć w *Podręczniku administratora platformy Lexmark Cloud*.

- 1 Na wbudowanym serwerze WWW przejdź do strony konfiguracji aplikacji.
- 2 W sekcji Ustawienia zaawansowane wpisz identyfikator klienta i tajny klucz klienta.
- 3 Kliknij przycisk **Zapisz**.

Konfigurowanie ustawień ekranu logowania

- 1 Z serwera Embedded Web Server otwórz stronę konfiguracji aplikacji.
- 2 Skonfiguruj ustawienia.

W przypadku eSF w wersji 5.0 lub nowszej

- a Kliknij opcję **Ustawienia ekranu logowania**, a następnie wykonaj dowolną z następujących czynności:
 - Dostosuj komunikat logowania.
 - Ustaw kolor niestandardowego tekstu logowania na czarny lub biały.
 - Prześlij obraz tła ekranu logowania.
 - Włącz kopiowanie i faksowanie bez logowania się.

Uwaga: Więcej informacji można znaleźć w sekcji [„Włączanie dostępu publicznego do aplikacji oraz funkcji kopiowania i faksu” na str. 11](#).

 - Wyłącz ostrzeżenie, gdy czytnik kart nie jest podłączony.
 - W sekcji Ustawienia ekranu blokady wykonaj jedną z poniższych czynności:
 - Wybierz położenie tekstu logowania.
 - Wpisz nazwę profilu, który ma zostać automatycznie uruchomiony po pomyślnym zalogowaniu się.

- W sekcji Profil niestandardowy wykonaj dowolną z następujących czynności:
 - Wprowadź nazwę profilu lub funkcji drukarki, do której użytkownicy mogą uzyskać dostęp z poziomu ekranu blokady.
Uwaga: Upewnij się, że dostęp publiczny do określonej aplikacji jest włączony. Więcej informacji można znaleźć w sekcji „[Włączanie dostępu publicznego do aplikacji oraz funkcji kopiowania i faksu](#)” na str. 11.
 - Dostosuj nazwę ikony wyświetlanej na ekranie blokady.
 - Prześlij niestandardowy obraz ikony.

b Kliknij **Zapisz**.

W przypadku eSF w wersji 4.0 lub starszej

a W sekcji Ekran logowania wykonaj dowolną z następujących czynności:

- Włącz przezroczystość tła.
- Dostosuj komunikat logowania.
- Prześlij obraz tła ekranu logowania.
- Włącz kopiowanie i faksowanie bez logowania się.

Uwaga: Więcej informacji można znaleźć w sekcji „[Włączanie dostępu publicznego do aplikacji oraz funkcji kopiowania i faksu](#)” na str. 11.

- Wyłącz ostrzeżenie, gdy czytnik kart nie jest podłączony.
- W polu Profil niestandardowy wprowadź nazwę aplikacji lub funkcję drukarki, do której użytkownicy mogą uzyskać dostęp z poziomu ekranu blokady.

Uwaga: Upewnij się, że dostęp publiczny do określonej aplikacji jest włączony. Więcej informacji można znaleźć w sekcji „[Włączanie dostępu publicznego do aplikacji oraz funkcji kopiowania i faksu](#)” na str. 11.

- Dostosuj nazwę ikony wyświetlanej na ekranie blokady.
- Wybierz położenie tekstu logowania.
- Wybierz ikonę i położenie jej tekstu.

Uwaga: Aby uzyskać więcej informacji na temat poszczególnych ustawień, zapoznaj się z pomocą otwieraną za pomocą myszy.

b Kliknij **Zastosuj**.

Włączanie dostępu publicznego do aplikacji oraz funkcji kopiowania i faksu

Uwaga: Więcej informacji na temat kontroli dostępu można znaleźć w *Podręczniku administratora bezpieczeństwa wbudowanego serwera WWW* dla danej drukarki.

W przypadku eSF w wersji 5.0 lub nowszej

- 1** W oknie wbudowanego serwera WWW kliknij **Ustawienia > Bezpieczeństwo > Metody logowania**.
- 2** W sekcji Publiczne kliknij **Zarządzaj uprawnieniami**.
- 3** Rozwiń **Dostęp do funkcji**, a następnie wybierz **Funkcja kopiowania i Funkcja faksu**.

4 Rozwiń **Aplikacje**, a następnie wybierz aplikację.

5 Kliknij przycisk **Zapisz**.

W przypadku eSF w wersji 4.0 lub starszej

1 W oknie wbudowanego serwera WWW kliknij **Ustawienia** lub **Konfiguracja**.

2 W zależności od modelu drukarki wykonaj jedną z następujących czynności:

- Kliknij **Bezpieczeństwo** > **Konfiguracja bezpieczeństwa** > **Kontrola dostępu** > **Dostęp do funkcji**.
- Kliknij **Bezpieczeństwo** > **Edytuj konfiguracje zabezpieczeń** > **Kontrola dostępu**.

3 Wybierz wartość **Brak zabezpieczeń** dla aplikacji oraz funkcji kopiowania i faksu.

4 Kliknij opcję **Wyślij**.

Konfigurowanie opóźnienia wylogowania karty

Ustaw czas, po którym drukarka zarejestruje następujące po sobie kliknięcia jako wylogowanie.

1 Na wbudowanym serwerze WWW przejdź do strony konfiguracji aplikacji.

2 Wykonaj jedną z następujących czynności:

W przypadku eSF w wersji 5.0 lub nowszej

a Kliknij **Ustawienia zaawansowane**, a następnie dostosuj opóźnienie wylogowania karty.

b Kliknij przycisk **Zapisz**.

W przypadku eSF w wersji 4.0 lub starszej

a W sekcji Ekran główny wprowadź wartość opóźnienia wylogowania karty.

b Kliknij przycisk **Zastosuj**.

Konfigurowanie limitów czasu połączeń

1 Na wbudowanym serwerze WWW przejdź do strony konfiguracji aplikacji.

2 Wykonaj jedną z następujących czynności:

W przypadku eSF w wersji 5.0 lub nowszej

a W sekcji Ustawienia usługi tożsamości dostosuj limity czasu sieci i gniazda.

b Kliknij przycisk **Zapisz**.

W przypadku eSF w wersji 4.0 lub starszej

a W sekcji Ustawienia zaawansowane wprowadź limity czasu sieci i gniazda.

b Kliknij przycisk **Zastosuj**.

Importowanie lub eksportowanie pliku konfiguracyjnego

Importowanie plików konfiguracyjnych nadpisuje istniejące konfiguracje aplikacji.

- 1 Na wbudowanym serwerze WWW przejdź do strony konfiguracji aplikacji.
- 2 Wykonaj jedną z następujących czynności:

W przypadku eSF w wersji 5.0 lub nowszej

- a Kliknij opcję **Konfiguracja importowania/eksportowania**.
- b Wykonaj jedną z następujących czynności:

Wyeksportuj plik konfiguracyjny

Kliknij przycisk **Eksportuj**.

Uwaga: Wyeksportowany plik konfiguracyjny nie zawiera tajnego klucza klienta ani wartości hasła konta w usłudze.

Importuj plik konfiguracyjny

- 1 Należy określić identyfikator klienta i tajny klucz klienta. Otwórz plik konfiguracyjny za pomocą edytora tekstu, a następnie dokonaj edycji wartości następujących ustawień:
 - `esf.cloudAuth.settings_identityserver_client_id`
 - `esf.cloudAuth.settings_identityserver_client_secret`

W przypadku hasła i nazwy użytkownika konta w usłudze dokonaj edycji wartości następujących ustawień:

- `esf.cloudAuth.settings_deviceAuth_userId`
- `esf.cloudAuth.settings_deviceAuth_password`

Uwaga: Pamiętaj, żeby ująć wartości w podwójny cudzysłów.

- 2 Przejdź do pliku konfiguracji, a następnie kliknij przycisk **Importuj**.

W przypadku eSF w wersji 4.0 lub starszej

- a Kliknij opcję **Konfiguracja importowania/eksportowania**.
- b Wykonaj jedną z następujących czynności:

Wyeksportuj plik konfiguracyjny

Kliknij przycisk **Eksportuj**.

Uwaga: Wyeksportowany plik konfiguracyjny nie zawiera tajnego klucza klienta ani wartości hasła konta w usłudze.

Importuj plik konfiguracyjny

- 1 Należy określić identyfikator klienta i tajny klucz klienta. Otwórz plik konfiguracyjny za pomocą edytora tekstu, a następnie dokonaj edycji wartości następujących ustawień:
 - `esf.cloudauth.settings.identityserver.client.id`
 - `esf.cloudauth.settings.identityserver.client.secret`

W przypadku hasła i nazwy użytkownika konta w usłudze dokonaj edycji wartości następujących ustawień:

- `esf.cloudauth.settings.identityserver.deviceAuth.userId`
- `esf.cloudauth.settings.identityserver.deviceAuth.password`

Uwaga: Pamiętaj, żeby ująć wartości w podwójny cudzysłów.

- 2 Kliknij przycisk **Importuj**.
- 3 Przejdź do pliku konfiguracji, a następnie kliknij przycisk **Start**.

Aktualizowanie okresu odpytywania

Jeśli po wdrożeniu aplikacji zostaną wprowadzone zmiany w konfiguracji logowania do drukarki, nowe ustawienia zaczną obowiązywać po upływie następnego okresu odpytywania.

Domyślnie aplikacja sprawdza dostępność aktualizacji co 15 minut (900 sekund).

Można zaktualizować okres odpytywania za pomocą pliku konfiguracyjnego aplikacji.

- 1 Wyeksportuj plik konfiguracyjny.

Uwaga: Więcej informacji można znaleźć w sekcji [„Importowanie lub eksportowanie pliku konfiguracyjnego” na str. 13](#).

- 2 Otwórz plik konfiguracyjny za pomocą edytora tekstu, a następnie dokonaj edycji wartości następujących ustawień:

Uwaga: Wartość należy wprowadzać w sekundach. Na przykład: zamiast 15 minut wprowadzić wartość **900**.

eSF w wersji 5.0 lub nowszej
`esf.cloudAuth.pollingInterval`

eSF w wersji 4.0 lub nowszej
`esf.cloudauth.pollingInterval`

- 3 Zapisz, a następnie zaimportuj plik konfiguracyjny.

Konfigurowanie ustawień proxy drukarki

Korzystając z wbudowanego serwera WWW

Jeżeli organizacja używa adresu IP dla serwera proxy do komunikacji, skonfiguruj ustawienia HTTP/FTP.

- 1 Wykonaj jedną z poniższych czynności z poziomu serwera Embedded Web Server:

W przypadku eSF w wersji 5.0 lub nowszej

- a Kliknij przycisk **Urządzenie > Sieć/Porty > Ustawienia HTTP/FTP**.
- b Wpisz adres IP serwera proxy HTTP.

W przypadku eSF w wersji 4.0 lub starszej

- a Kliknij opcje **Ustawienia > Sieć/Porty > TCP/IP**.
- b W sekcji Ustawienia HTTP/FTP wpisz adres IP serwera proxy HTTP.

2 Zapisz ustawienia.

Konfigurowanie uwierzytelnionego serwera proxy

Jeśli serwer proxy został skonfigurowany za pomocą nazwy hosta lub wymaga nazwy użytkownika i hasła, wykonaj następujące czynności:

1 Wykonaj jedną z poniższych czynności z poziomu serwera Embedded Web Server:

W przypadku eSF w wersji 5.0 lub nowszej

- a Kliknij przycisk **Aplikacje > Konfiguracja aplikacji platformy**.
- b W sekcji Konfiguracja platformy usuń zaznaczenie opcji **Użyj ustawień proxy drukarki**.
- c Wpisz nazwę hosta serwera proxy HTTP i poświadczenia serwera proxy.

W przypadku eSF w wersji 4.0 lub starszej

- a W zależności od modelu drukarki wykonaj jedną z następujących czynności:
 - Kliknij kolejno **Ustawienia > Aplikacje > Zarządzanie aplikacjami > System > Konfiguruj**.
 - Kliknij kolejno **Ustawienia > Rozwiązania urządzenia > Rozwiązania (eSF) > System > Konfiguruj**.
 - Kliknij kolejno **Ustawienia > Embedded Solutions > System > Skonfiguruj**.
- b Usuń zaznaczenie opcji **Użyj ustawień proxy drukarki**.
- c Wpisz nazwę hosta serwera proxy HTTP i poświadczenia serwera proxy.

2 Zapisz ustawienia.

Korzystanie z pliku konfiguracyjnego

Zaimportuj plik UCF lub VCC zawierający następujące ustawienia:

```
<setting name="settings.useprinterproxy">
<setting name="settings.http.proxyurl">
<setting name="settings.http.proxyport">
<setting name="settings.proxyurl">
<setting name="settings.proxyport">
```

Przykładowe wartości

```
<?xml version="1.0" encoding="UTF-8"?>
<esfSettings>
  <app name="systemManagerImpl" settingVersion="6.2.0">
    <global>
      <setting name="settings.useprinterproxy">false</setting>
      <setting name="settings.http.proxyurl">http.proxy1.fmr.com</setting>
      <setting name="settings.http.proxyport">80</setting>
      <setting name="settings.proxyurl">http.proxy.fmr.com</setting>
      <setting name="settings.proxyport">8000</setting>
    </global>
  </app>
</esfSettings>
```

Korzystanie z aplikacji

Rejestrowanie karty

- 1 Dotknij kartą czytnika.
- 2 W panelu sterowania drukarki wykonaj jedną z następujących czynności (w zależności od konfiguracji uwierzytelnienia):
 - Wprowadź kod logowania.
 - Wprowadź poświadczenia użytkownika.

Uwagi:

- Więcej informacji można znaleźć w sekcji „[Uzyskiwanie kodu logowania](#)” na str. 17.
- Możesz także wysłać instrukcje w wiadomości e-mail lub wydrukować je.

- 3 Dotknij opcji **Zarejestruj**.

Uwagi:

- W zależności od konfiguracji logowania do drukarki na platformie usług w chmurze Lexmark może zostać wyświetlony monit o wprowadzenie kodu PIN w celu kontynuowania rejestracji. Aby uzyskać więcej informacji na temat konfigurowania logowania do drukarki, zapoznaj się z *Podręcznikiem administratora usług w chmurze Lexmark*.
- Karta dostępu może być ustawiona jako tymczasowa lub stała.

Za pomocą łącza do rejestracji otrzymanego w wiadomości e-mail

Jeśli **Bezpieczne logowanie** jest wyłączone dla organizacji, użytkownicy mogą jedynie rejestrować karty dostępu z poziomu panelu sterowania drukarki za pomocą łącza do rejestracji otrzymanego w wiadomości e-mail.

Aby uzyskać więcej informacji na temat konfigurowania logowania do drukarki, zapoznaj się z *Podręcznikiem administratora usług w chmurze Lexmark*.

- 1 W zależności od modelu drukarki dotknij opcji **E-mail** lub **Rejestracja przez e-mail**.
- 2 Dotknij przycisku **Dalej**, a następnie wpisz swój adres e-mail.
Wiadomość e-mail zawierającą adres URL zostanie wysłana na Twój adres e-mail.
- 3 Kliknij adres URL podany w wiadomości.
- 4 Wprowadź dane uwierzytelniające na platformie usług w chmurze Lexmark.

Uzyskiwanie kodu logowania

Kod logowania jest wymagany, jeśli aplikacja została skonfigurowana w taki sposób, by uwierzytelniać użytkowników w ujednoczony sposób z wykorzystaniem logowania SSO.

Korzystanie z portalu internetowego

- 1 Wykonaj jedną z następujących czynności:
 - Uruchom przeglądarkę internetową, a następnie wpisz **cloud.lexmark.com/device**.
 - Skorzystaj z aplikacji czytnika kodów QR w urządzeniu przenośnym, aby zeskanować kod QR z panelu sterowania drukarki.
- 2 Wprowadź poświadczenia użytkownika.
- 3 Zanotuj kod logowania.

Korzystanie z aplikacji Lexmark Mobile Print

Aby uzyskać więcej informacji w kontekście swojego urządzenia przenośnego, zapoznaj się z *Podręcznikiem użytkownika usługi Lexmark Mobile Print*.

- 1 Kliknij pozycję **Kod logowania** na ekranie głównym aplikacji.
- 2 Zanotuj kod logowania.

Korzystanie z platformy Lexmark Cloud Services

Więcej informacji można znaleźć w *Podręczniku użytkownika platformy Lexmark Cloud Services*.

- 1 Na platformie Lexmark Cloud Services kliknij swoją nazwę użytkownika w prawym górnym rogu strony, a następnie kliknij przycisk **Moje konto**.
- 2 W sekcji Dane osobowe kliknij przycisk **Wygeneruj kod logowania**.
- 3 Zanotuj kod logowania.

Uwagi:

- Kod logowania automatycznie odświeża się co 15 minut.
- Kodu logowania można użyć tylko raz.

Ręczne logowanie się do drukarki

Aby uzyskać więcej informacji na temat konfigurowania logowania do drukarki, zapoznaj się z *Podręcznikiem administratora usług w chmurze Lexmark*.

- 1 W panelu sterowania drukarki wykonaj jedną z następujących czynności (w zależności od konfiguracji logowania do drukarki):
 - Dotknij opcji **Bezpieczne logowanie** i wprowadź kod logowania.

Uwagi:

- Więcej informacji można znaleźć w sekcji [„Uzyskiwanie kodu logowania” na str. 17](#).

- Przycisk ten pojawia się wyłącznie wtedy, gdy skonfigurowane jest uwierzytelnianie organizacji z dostępem ujednoczonym.
 - Dotknij przycisku **Logowanie za pomocą kodu PIN**, a następnie wprowadź kod PIN.
- Uwaga:** Przed zalogowaniem należy posiadać kod PIN. Więcej informacji można znaleźć w sekcji [„Uzyskiwanie kodu PIN” na str. 18](#).
- Dotknij przycisku **Logowanie administratora**, a następnie wprowadź poświadczenia administratora.

Uwagi:

- Ten przycisk jest wyświetlany tylko wtedy, gdy podczas tworzenia konfiguracji w usługach zarządzania flotą usług w chmurze Lexmark wybrano opcję Pokaż opcję logowanie administratora na ekranie blokady.
- Aby uzyskać więcej informacji na temat logowania administratora, patrz [„Konfigurowanie logowania administratora” na str. 7](#).

2 Dotknij opcji **Zaloguj się**.

Logowanie do drukarki z użyciem karty i uwierzytelniania dwuetapowego

1 Dotknij kartą czytnika.

2 Wprowadź numer PIN.

Uwaga: Przed zalogowaniem należy posiadać kod PIN. Więcej informacji można znaleźć w sekcji [„Uzyskiwanie kodu PIN” na str. 18](#).

Uzyskiwanie kodu PIN

Ustawienie to jest dostępne tylko, jeśli opcja generowania kodu PIN na platformie Lexmark Cloud Services jest ustawiona na **Ustawiane przez użytkownika**. Więcej informacji można znaleźć w *Podręczniku administratora platformy Lexmark Cloud Services*.

- 1 Na platformie Lexmark Cloud Services kliknij swoją nazwę użytkownika w prawym górnym rogu strony, a następnie kliknij przycisk **Moje konto**.
- 2 W sekcji Logowanie do drukarki kliknij opcję **Ustaw kod PIN**.
- 3 Wprowadź numer PIN.
- 4 Kliknij opcję **Generuj kod PIN**.

Resetowanie kodu PIN

- 1 Na platformie Lexmark Cloud Services kliknij swoją nazwę użytkownika w prawym górnym rogu strony, a następnie kliknij przycisk **Moje konto**.
- 2 W sekcji Logowanie do drukarki kliknij opcję **Resetuj kod PIN**.
- 3 Wprowadź nowy kod PIN.
- 4 Kliknij opcję **Generuj kod PIN**.

Rozwiązywanie problemów

Błąd aplikacji

Spróbuj następujących rozwiązań:

Sprawdź dziennik diagnostyki

- 1 Uruchom przeglądarkę internetową, a następnie wpisz **IP/se**, gdzie **IP** to adres IP drukarki.
- 2 Kliknij opcję **Wbudowane rozwiązania**, a następnie wykonaj następujące czynności:
 - a Wyczyść plik dziennika.
 - b Jako poziom rejestrowania ustaw wartość **Tak**.
 - c Wygeneruj plik dziennika.
- 3 Przeanalizuj dziennik, a następnie rozwiąż problem.

Uwaga: Po rozwiązaniu problemu, jako poziom rejestrowania ustaw wartość **Nie**.

Skontaktuj się z przedstawicielem firmy Lexmark

Błąd uwierzytelniania

Spróbuj następujących rozwiązań:

Upewnij się, że drukarka jest podłączona do sieci komputerowej

Więcej informacji można znaleźć w *Podręczniku użytkownika* drukarki.

Upewnij się, że dostawca usługi tożsamości jest aktywny i nie jest zajęty

Aby uzyskać więcej informacji, skontaktuj się z administratorem systemu.

Rejestracja karty dostępu jest zabroniona

Upewnij się, że dostawca usługi tożsamości i dostawca usługi etykiety są skonfigurowani poprawnie.

Aby uzyskać więcej informacji, zobacz [„Konfigurowanie ustawień uwierzytelnienia użytkownika” na str. 9.](#)

Nie można wysłać wiadomości e-mail z instrukcjami dotyczącymi kodu logowania

Upewnij się, że serwer SMTP jest skonfigurowany poprawnie.

Funkcję wysyłania wiadomości e-mail z drukarki należy skonfigurować przy użyciu prawidłowego adresu serwera SMTP. Aby uzyskać więcej informacji, skontaktuj się z administratorem systemu.

Przycisk Ręczne logowanie pojawia się w przypadku ujednoliconego uwierzytelniania organizacji

Spróbuj następujących rozwiązań:

Upewnij się, że drukarka jest podłączona do sieci komputerowej

Drukarka mogła zostać odłączona od sieci lub serwer jest niedostępny podczas instalacji. Więcej informacji można znaleźć w *Podręczniku użytkownika* drukarki.

Dotknij pozycji **Logowanie ręczne**. Jeśli serwer jest dostępny, proces uwierzytelniania jest taki sam, jak w przypadku uwierzytelniania bezpiecznego logowania. Po wylogowaniu pojawi się przycisk Bezpieczne logowanie.

Ponownie skonfiguruj ustawienia na stronie konfiguracji aplikacji

Upewnij się, że identyfikator i tajny klucz klienta są prawidłowo skonfigurowane

Więcej informacji można znaleźć w sekcji [„Konfigurowanie identyfikatora i tajnego klucza klienta” na str. 10](#).

Nie można zalogować się przy użyciu kodu logowania

Upewnij się, że kod logowania nie był używany i jest nadal ważny.

Uwagi:

- Kod logowania automatycznie odświeża się co 15 minut.
- Kodu logowania można użyć tylko raz.

Nie można zarejestrować karty dostępu przez łącze do rejestracji z wiadomości e-mail

Zarejestruj swoją kartę dostępu tylko raz

Jest możliwe, że karta dostępu oczekuje na zarejestrowanie. Nie można zarejestrować karty dostępu za pomocą łącza do rejestracji z wiadomości e-mail więcej niż jeden raz.

Uwaga: Jeśli pierwsza wiadomość e-mail została usunięta lub nie została otrzymana, musisz zarejestrować się ponownie.

Nie otrzymano wiadomości e-mail z łączem do rejestracji karty dostępu

Spróbuj następujących rozwiązań:

Upewnij się, że wprowadzono poprawny adres e-mail

Upewnij się, że adres e-mail jest poprawny

Skontaktuj się z przedstawicielem firmy Lexmark

Mógł wystąpić błąd aplikacji lub serwera Cloud.

Nie można się połączyć z dostawcą usługi zarządzania tożsamościami

Wydłuż limity czasu połączeń

Więcej informacji można znaleźć w sekcji [„Konfigurowanie limitów czasu połączeń” na str. 12.](#)

Upewnij się, że konfiguracja serwera proxy jest poprawna

Więcej informacji można znaleźć w sekcji [„Konfigurowanie ustawień proxy drukarki” na str. 14.](#)

Kod PIN stracił ważność

Resetuj kod PIN

Więcej informacji można znaleźć w sekcji [„Uzyskiwanie kodu PIN” na str. 18.](#)

Skontaktuj się z administratorem organizacji

Zbyt wiele nieudanych prób

Poczekaj, aż upłynie czas blokowania

Odczekaj około pięciu minut przed ponowną próbą.

Skontaktuj się z administratorem organizacji

Uwagi

Informacje o wydaniu

December 2023

Niniejsze oświadczenie nie ma zastosowania w krajach, w których podobne postanowienia są niezgodne z obowiązującym prawem: FIRMA LEXMARK INTERNATIONAL, INC. DOSTARCZA TĘ PUBLIKACJĘ „W STANIE, W JAKIM SIĘ ZNAJDUJE”, BEZ JAKICHKOLWIEK WYRAŻNYCH LUB DOMNIEMANYCH RĘKOJMI I GWARANCJI, W TYM BEZ DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ I UŻYTECZNOŚCI DO OKREŚLONYCH CELÓW. W niektórych krajach wykluczenie gwarancji wyraźnych lub domniemanych w przypadku określonych transakcji jest niedozwolone, dlatego to oświadczenie może nie dotyczyć wszystkich użytkowników.

Niniejsza publikacja może zawierać nieścisłości techniczne lub błędy drukarskie. Przedstawione informacje podlegają okresowym zmianom; zmiany te będą uwzględniane w kolejnych wydaniach. Udoskonalenia lub zmiany opisanych tutaj produktów lub programów mogą być wprowadzane w dowolnym czasie.

Znajdujące się w niniejszej publikacji odnośniki do produktów, programów lub usług nie oznaczają, że ich producent zamierza udostępnić je we wszystkich krajach, w których działa. Umieszczenie odnośnika do produktu, programu lub usługi nie oznacza, że dozwolone jest używanie wyłącznie tego produktu, programu lub usługi. Zamiast tego produktu, programu lub usługi można użyć funkcjonalnie równoważnego zamiennika, pod warunkiem jednak, że nie narusza to niczyjej własności intelektualnej. Ocena i testowanie współdziałania z innymi produktami, programami lub usługami, poza jawnie wymienionymi przez wytwórcę, odbywa się na odpowiedzialność użytkownika.

Aby uzyskać pomoc techniczną firmy Lexmark, należy odwiedzić stronę <http://support.lexmark.com>.

Informacje na temat zasad ochrony prywatności firmy Lexmark regulujące korzystanie z tego produktu znajdują się na stronie www.lexmark.com/privacy.

Informacje o materiałach eksploatacyjnych oraz pliki do pobrania można znaleźć w witrynie www.lexmark.com.

© 2018 Lexmark International, Inc.

Wszelkie prawa zastrzeżone.

Znaki towarowe

Lexmark oraz logo Lexmark są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Lexmark International, Inc. w Stanach Zjednoczonych i/lub w innych krajach.

Wszystkie pozostałe znaki towarowe są własnością odpowiednich firm.

Oświadczenia dotyczące licencji

Wszystkie oświadczenia dotyczące licencji związane z tym produktem można znaleźć w pakiecie aplikacji lub witrynie pomocy technicznej Lexmark.

Indeks

A

uzyskiwanie dostępu do strony konfiguracji aplikacji 8
Embedded Web Server, uzyskiwanie dostępu 7
ustawienia logowania administratora konfiguracja 7
błąd aplikacji 19
aplikacje włączanie publicznego dostępu 11
ustawienia uwierzytelniania proxy konfiguracja 14
błąd uwierzytelniania 19

B

opóźnienie wylogowania karty konfiguracja 12
rejestracja karty dostępu jest zabroniona 19

C

nie można się połączyć z dostawcą usług zarządzania tożsamościami 21
nie można wysłać wiadomości e-mail z instrukcjami dotyczącymi kodu logowania 20
nie można zalogować się przy użyciu kodu logowania 20
nie można zarejestrować karty dostępu przez łącze do rejestracji z wiadomości e-mail 21
karta rejestrowanie 16
historia zmian 4
wykaz czynności kontrolnych gotowość do wdrożenia 6
identyfikator klienta konfiguracja 10
tajny klucz klienta konfiguracja 10
plik konfiguracyjny eksportowanie 13

importowanie 13
strona konfiguracji aplikacji dostęp 8
konfigurowanie ustawień logowania administratora 7
konfigurowanie ustawień ekranu logowania 10
konfigurowanie opóźnienia wylogowania karty 12
konfigurowanie identyfikatora i tajnego klucza klienta 10
konfigurowanie limitów czasu połączeń 12
konfigurowanie ustawień proxy drukarki 14
konfigurowanie ustawień uwierzytelniania użytkownika 9
limity czasu połączeń konfiguracja 12
funkcje kopiowania i faksu włączanie publicznego dostępu 11
funkcja kopiowania włączanie publicznego dostępu 11

D

domyślna metoda logowania 7
ustawianie 7
lista kontrolna gotowości do wdrożenia 6

E

Embedded Web Server dostęp 7
włączanie dostępu publicznego do aplikacji oraz funkcji kopiowania i faksu 11
eksportowanie pliku konfiguracyjnego 13

F

funkcja faksu włączanie publicznego dostępu 11

I

importowanie pliku konfiguracyjnego 13

L

ręczne logowanie się do drukarki 17
logowanie ręczna 17
kod logowania pozyskiwanie 17
ustawienia ekranu logowania konfiguracja 10

M

logowanie ręczne 17
przycisk Ręczne logowanie pojawia się w przypadku ujednoliconego uwierzytelniania organizacji 20

N

limit czasu sieci konfiguracja 12
nie otrzymano wiadomości e-mail z łączem do rejestracji karty dostępu 21

O

uzyskiwanie kodu logowania 17
informacje ogólne 5

P

kod PIN przywracanie 18
ustawianie 18
kod PIN stracił ważność 21
okres odpytywania aktualizowanie 14
ustawienia proxy drukarki konfiguracja 14

R

rejestrowanie karty 16
resetowanie kodu PIN 18

S

ustawianie kodu PIN 18
limit czasu gniazda
konfiguracja 12

T

zbyt wiele nieudanych prób 22
rozwiązywanie problemów
błąd aplikacji 19
błąd uwierzytelniania 19
rejestracja karty dostępu jest
zabroniona 19
nie można się połączyć z
dostawcą usług zarządzania
tożsamościami 21
nie można wysłać wiadomości
e-mail z instrukcjami
dotyczącymi kodu
logowania 20
nie można zalogować się przy
użyciu kodu logowania 20
nie można zarejestrować karty
dostępu przez łącze do
rejestracji z wiadomości e-
mail 21
przycisk Ręczne logowanie
pojawia się w przypadku
ujednoliczonego
uwierzytelniania
organizacji 20
nie otrzymano wiadomości e-
mail z łączem do rejestracji
karty dostępu 21
kod PIN stracił ważność 21
zbyt wiele nieudanych prób 22

U

aktualizowanie okresu
odpytywania 14
ustawienia uwierzytelnienia
użytkownika
konfiguracja 9