Uwierzytelnianie kartą

Podręcznik administratora

Grudzień 2020

www.lexmark.com

Zawartość

Przegląd

Użyj aplikacji, aby zabezpieczyć dostęp do drukarki za pomocą czytnika kart. Gdy użytkownicy rejestrują się za pomocą karty, ich poświadczenia są uwierzytelniane za pomocą:

- drukarki głównej. Jeżeli drukarka główna jest niedostępna, drukarka zapasowa działa jako drukarka główna do momentu, gdy drukarka główna nie będzie znów dostępna.

  Uwaga: W trakcie konfigurowania drukarek upewnij się, czy są podłączone do tej samej sieci.
- Lightweight Directory Access Protocol (LDAP), serwery Lexmark™ Document Distributor (LDD) lub dostawcy usługi tożsamości zależnie od uwierzytelniania ustawionego przez organizację.

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

Konfigurowanie wymagań wstępnych

Aby skonfigurować aplikację, mogą być wymagane uprawnienia administratora.

Dostęp do wbudowanego serwera WWW.

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

Dodawanie wewnętrznego konta użytkownika

W przypadku korzystania z uwierzytelniania za pomocą drukarki wymagane jest wewnętrzne konto użytkownika.

1. W oknie wbudowanego serwera WWW kliknij **Ustawienia** lub **Konfiguracja**.
2. W zależności od modelu drukarki wykonaj jedną z następujących czynności:
   - Kliknij kolejno **Bezpieczeństwo** > **Konfiguracja bezpieczeństwa** > **Konta wewnętrzne** > **Dodaj konto wewnętrzne**.
   - Kliknij kolejno **Bezpieczeństwo** > **Edytuj konfiguracje zabezpieczeń** > **Konta wewnętrzne** > **Dodaj konto wewnętrzne**.
3. Wprowadź dane konta, a następnie kliknij przycisk **Wyślij**.
4. Jeżeli to konieczne, w sekcji Zarządzanie kontami wewnętrznymi wprowadź własną nazwę bloku funkcjonalnego i określ wymagane poświadczenia użytkownika.
5. Kliknij opcję **Wyślij**.

Konfigurowanie grup kont użytkowników wewnętrznych

1. W oknie wbudowanego serwera WWW kliknij **Ustawienia** lub **Konfiguracja**.
2. W zależności od modelu drukarki wykonaj jedną z następujących czynności:
   - Kliknij **Zabezpieczenia** > **Konfiguracja zabezpieczeń** > **Konta wewnętrzne** > **Skonfiguruj grupy do pracy z kontami wewnętrznymi**.
   - Kliknij **Zabezpieczenia** > **Edytuj konfiguracje zabezpieczeń** > **Konta wewnętrzne** > **Skonfiguruj grupy do pracy z kontami wewnętrznymi**.
3. Wprowadź nazwę grupy, a następnie kliknij opcję **Dodaj**.
4. Dodaj konta wewnętrzne do grupy.
5. Kliknij opcję **Wyślij**.

Tworzenie szablonu zabezpieczeń

Szablon zabezpieczeń składa się z bloków funkcjonalnych zabezpieczeń, takich jak konta wewnętrzne, Kerberos, LDAP, LDAP+GSSAPI oraz Active Directory. Szablony te są stosowane względem kontroli dostępu w celu zabezpieczenia funkcji drukarek oraz aplikacji.

1. W oknie wbudowanego serwera WWW kliknij **Ustawienia** lub **Konfiguracja**.
2. W zależności od modelu drukarki wykonaj jedną z następujących czynności:
   - Kliknij kolejno opcje **Bezpieczeństwo** > **Konfiguracja bezpieczeństwa** > **Szablon zabezpieczeń** > **Dodaj szablon zabezpieczeń**.
   - Kliknij kolejno opcje **Bezpieczeństwo** > **Edytuj konfiguracje zabezpieczeń** > **Szablony zabezpieczeń** > **Dodaj szablon zabezpieczeń**.
3. Wprowadź nazwę szablonu zabezpieczeń, a następnie wybierz jedną z poniższych konfiguracji uwierzytelniania:
   - W celu uzyskania uwierzytelniania za pomocą drukarki w przypadku samodzielnej konfiguracji, wybierz blok funkcjonalny kont wewnętrznych.
   - W celu uzyskania uwierzytelniania za pomocą rozwiązania bezserwerowego zwalniania wydruków Lexmark Print Management (LPM) w przypadku konfiguracji Active Directory, wybierz blok funkcjonalny LDAP+GSSAPI.
   - W celu uzyskania uwierzytelniania LDAP, wybierz blok funkcjonalny LDAP.
4. Kliknij przycisk **Zapisz szablon**.

Uwaga: Aby zmodyfikować istniejący szablon zabezpieczeń, kliknij szablon zabezpieczeń, a następnie dodaj lub zmodyfikuj uprawnienia do szablonu.

Konfiguracja kontroli dostępu

Uwaga: W przypadku korzystania z funkcji **Logowanie administratora** należy upewnić się, że skonfigurowano szablon zabezpieczeń dla kont wewnętrznych. Więcej informacji można znaleźć w sekcji „Tworzenie szablonu zabezpieczeń” na str. 6.

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**.
   - Kliknij **Bezpieczeństwo** > **Edytuj konfiguracje zabezpieczeń** > **Kontrola dostępu**.
3. Kliknij **Aplikacje urządzenia** lub **Rozwiązania urządzenia**, a następnie wykonaj poniższe czynności:
   - Dla ustawienia Aplikacja 1 lub Rozwiązanie 1 wybierz szablon zabezpieczeń konta wewnętrznego, LDAP+GSSAPI lub Active Directory.
   - Dla ustawienia Aplikacja 2 lub Rozwiązanie 2 wybierz szablon zabezpieczeń aplikacji.

     Uwaga: Szablon zabezpieczeń aplikacji jest szablonem z opcją CardAuth jako konfiguracją uwierzytelniania. Więcej informacji można znaleźć w sekcji „Tworzenie szablonu zabezpieczeń” na str. 6.
   - Dla ustawienia Aplikacja 3 lub Rozwiązanie 3 wybierz szablon zabezpieczeń LDAP.

Uwagi:

- Jeżeli zainstalowano funkcję Zwalnianie wydruków LPM, dla kontroli dostępu funkcji Zwalnianie wydruków ustaw szablon zabezpieczeń aplikacji.
- Drukarki Embedded Solutions Framework (eSF) w wersji 2.x wymagają aplikacji eSF Security Manager w celu konfiguracji kontroli dostępu. Aby uzyskać listę tych drukarek, zobacz plik *Readme*.

4 Kliknij opcję **Wyślij**.

Konfigurowanie aplikacji

Przed rozpoczęciem wykonaj następujące czynności:

- Wyłącz tło i wygaszacz ekranu oraz wszelkie istniejące aplikacje uwierzytelniania.
- Zainstaluj poniższe:
  - Instalator uwierzytelniania kartą
  - Sterownik czytnika kart
  - Czytnik kart
  - eSF Security Manager

    Uwaga: Drukarki eSF w wersji 2.x wymagają aplikacji eSF Security Manager w celu konfiguracji kontroli dostępu. Aby uzyskać listę tych drukarek, zobacz plik *Readme*.

Uzyskiwanie dostępu do strony konfiguracji aplikacji

1. W oknie wbudowanego serwera WWW kliknij **Ustawienia** lub **Konfiguracja**.
2. W zależności od modelu drukarki wykonaj jedną z następujących czynności:
   - Kliknij opcje **Aplikacje** > **Zarządzanie aplikacjami**.
   - Kliknij opcje **Rozwiązania urządzenia** > **Rozwiązania (eSF)**.
   - Kliknij **Embedded Solutions**.
3. Kliknij kolejno **Uwierzytelnianie kartą** > **Konfiguruj**.

Konfigurowanie uwierzytelniania administratora

Uwaga: W przypadku korzystania z funkcji **Logowanie administratora** należy upewnić się, że skonfigurowano szablon zabezpieczeń dla kont wewnętrznych, kodu PIN i hasła. Więcej informacji można znaleźć w sekcji „Tworzenie szablonu zabezpieczeń” na str. 6.

1. Na wbudowanym serwerze WWW przejdź do strony 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 „Tworzenie szablonu zabezpieczeń” na str. 6.
   - Wybranie opcji **Wyłączone** powoduje ukrycie opcji **Logowanie administratora** z panelu drukarki.
3. Kliknij przycisk **Zastosuj**.

Konfigurowanie ekranu logowania

Ekran logowania można skonfigurować tak, by można było wykonać poniższe czynności:

- Korzystać z funkcji kopiowania i faksowania bez konieczności logowania.
- Wybrać metodę logowania.
- Dodać tło ekranu logowania i dostosować komunikat logowania.
- Wyłącz ostrzeżenie, gdy czytnik kart nie jest podłączony.

1. Na wbudowanym serwerze WWW przejdź do strony konfiguracji aplikacji.
2. Skonfiguruj ustawienia w sekcji Ekran logowania.

   Uwaga: Aby uzyskać więcej informacji na temat poszczególnych ustawień, zapoznaj się z pomocą otwieraną za pomocą myszy.
3. Kliknij przycisk **Zastosuj**.

Włączanie kopiowania i faksowania bez logowania się

Jeżeli włączona jest opcja „Zezwól na kopiowanie bez logowania się” lub „Zezwól na faksowanie bez logowania się”, wykonaj poniższe czynności:

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. Dla funkcji kopiowania lub faksowania wybierz wartość **Bez zabezpieczeń**.
4. Kliknij opcję **Wyślij**.

Uwierzytelnianie za pomocą drukarki

Korzystaj z uwierzytelniania za pomocą drukarki podczas weryfikacji użytkowników za pośrednictwem drukarki głównej.

Konfigurowanie uwierzytelniania użytkownika za pomocą drukarki

Zanim rozpoczniesz, upewnij się że:

- Jako kontrolę dostępu ustawień Aplikacja 1 lub Rozwiązania 1 ustawiono szablon zabezpieczeń konta wewnętrznego, LDAP+GSSAPI lub Active Directory.
- Dla ustawienia Aplikacja 2 lub Rozwiązanie 2 wybrano szablon zabezpieczeń aplikacji.

  Uwaga: Więcej informacji można znaleźć w sekcji „Konfiguracja kontroli dostępu” na str. 6.

1. Na serwerze Embedded Web Server przejdź do strony konfiguracji aplikacji.
2. W sekcji Ekran logowania dla opcji Metoda logowania wybierz wartość **Karta lub logowanie ręczne**.

3 W sekcji Uwierzytelnianie użytkownika wykonaj poniższe czynności:
- Wybierz wartość **Za pomocą drukarki** dla ustawienia Uwierzytelnianie karty.
- Dla ustawienia Kontrola dostępu w przypadku rejestracji karty wybierz opcję **Aplikacja 1** lub **Rozwiązanie 1**.
- Dla opcji Kontrola dostępu w przypadku logowania ręcznego wybierz wartość **Aplikacja 1** lub **Rozwiązanie 1**.
- Dla ustawienia Kontrola dostępu do sesji wybierz opcję **Aplikacja 2** lub **Rozwiązanie 2**.

Uwagi:
- Jeżeli dla ustawienia Kontrola dostępu w przypadku rejestracji karty wybrano wartość **Brak**, nie można zarejestrować karty w drukarce.
- Wybranie dla ustawienia Kontrola dostępu w przypadku logowania ręcznego wartości **Brak** wymaga tylko karty do zalogowania się nawet, gdy w ustawieniu Metoda logowania wybrano wartość **Karta lub logowanie ręczne**.
- Aby uzyskać więcej informacji na temat poszczególnych ustawień, zapoznaj się z pomocą otwieraną za pomocą myszy.

4 Kliknij przycisk **Zastosuj**.

Konfiguracja roli drukarki

Uwaga: Drukarka-klient wymaga drukarki głównej i zapasowej.

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

2 W sekcji Uwierzytelnianie karty przy użyciu drukarki wybierz rolę dla drukarki.
- **Główna** – drukarka przechowuje listę zarejestrowanych użytkowników.
- **Zapasowa** – jeżeli drukarka główna zostanie wyłączona, drukarka zapasowa przejmie jej rolę do czasu, gdy drukarka główna znów będzie dostępna.
- **Klient** – ta drukarka nie przechowuje informacji o użytkownikach. Drukarka główna lub drukarka zapasowa są wymagane do weryfikacji poświadczeń użytkowników.

Uwagi:
- Jeśli używasz tylko jednej drukarki, ustaw ją jako główną.
- Jeśli używasz dwóch drukarek, wtedy jedną ustaw jako główną, a drugą jako zapasową.
- Jeśli używasz trzech lub więcej drukarek, wtedy jedną ustaw jako główną, jedną jako zapasową, a resztę jako klienty.

3 Wpisz nazwy hostów lub adresy IP drukarki głównej i zapasowej.

Uwagi:
- W trakcie konfigurowania drukarki zapasowej wymagana jest nazwa hosta lub adres IP drukarki głównej.
- W trakcie konfigurowania drukarek-klientów wymagane są nazwy hostów lub adresy IP drukarki głównej i drukarki zapasowej.
- Przed przypisaniem drukarki-klienta do nowej drukarki głównej, usuń ją z poprzedniej drukarki głównej.

4 Kliknij przycisk **Zastosuj**.

Uwierzytelnianie za pomocą usługi WWW

Korzystaj z uwierzytelniania za pomocą usługi WWW podczas weryfikacji użytkowników za pośrednictwem serwera LDD.

Konfigurowanie uwierzytelniania użytkownika usługi WWW

Przed rozpoczęciem upewnij się, że dla ustawienia Aplikacja 2 lub Rozwiązanie 2 wybrano szablon zabezpieczeń aplikacji. Więcej informacji można znaleźć w sekcji „Konfiguracja kontroli dostępu” na str. 6.

1. Na wbudowanym serwerze WWW przejdź do strony konfiguracji aplikacji.
2. W sekcji Ekran logowania dla opcji Metoda logowania wybierz wartość **Karta lub logowanie ręczne**.
3. W sekcji Uwierzytelnianie użytkownika wykonaj poniższe czynności:
   - Wybierz wartość **Usługa WWW** dla ustawienia Uwierzytelnianie karty.
   - Wybierz preferowany typ kontroli dostępu w ustawieniach Kontrola dostępu w przypadku rejestracji karty i Kontrola dostępu w przypadku logowania ręcznego.
   - Dla ustawienia Kontrola dostępu do sesji wybierz opcję **Aplikacja 2** lub **Rozwiązanie 2**.

   Uwagi:

   - Jeżeli dla ustawienia Kontrola dostępu w przypadku rejestracji karty wybrano wartość **Brak**, nie można zarejestrować karty w drukarce.
   - Wybranie dla ustawienia Kontrola dostępu w przypadku logowania ręcznego wartości **Brak** wymaga tylko karty do zalogowania się, nawet gdy w ustawieniu Metoda logowania wybrano wartość **Karta lub logowanie ręczne**.
   - Aby uzyskać więcej informacji na temat poszczególnych ustawień, zapoznaj się z pomocą otwieraną za pomocą myszy.
4. Wybierz opcję **Sprawdź certyfikat**, aby sprawdzić poprawność wszystkich połączeń z serwerem. Jeśli opcja Sprawdź certyfikat nie jest zaznaczona, urząd certyfikacji nie zostanie sprawdzony.

   Uwaga: Ustawienie Zweryfikuj certyfikat dotyczy tylko sprawdzania poprawności usługi tożsamości i usługi WWW.
5. W menu Tryb weryfikacji wybierz opcję **łańcuch** lub **element równorzędny**.

   Uwaga: Wartość domyślna to łańcuch.
6. Prześlij certyfikat SSL serwera, aby w bezpieczny sposób nawiązać połączenie z serwerem.
7. W polu SprawdzanieHostów wpisz dodatkowe nazwy hostów (inne niż domyślny adres URL serwera), aby zweryfikować wpisy w certyfikacie. Jeżeli istnieje wiele nazw hostów, oddziel je przecinkami.

   Uwaga: Domyślnie biała lista zawiera tylko adres URL serwera. Wpisz dodatkowe nazwy hostów w polu SprawdzanieHostów, aby umieścić je na białej liście.
8. Kliknij przycisk **Zastosuj**.

Konfigurowanie ustawień usługi WWW

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

2 Skonfiguruj ustawienia w sekcji Ustawienia usługi WWW.

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

3 Kliknij przycisk **Zastosuj**.

Uwierzytelnianie za pomocą usługi tożsamości

Korzystaj z uwierzytelniania za pomocą usługi tożsamości podczas weryfikacji użytkowników za pośrednictwem serwera usługi tożsamości, takiego jak serwer LPM Software as a Service (SaaS).

Konfigurowanie uwierzytelniania użytkownika usługi tożsamości

Przed rozpoczęciem upewnij się, że dla ustawienia Aplikacja 2 lub Rozwiązanie 2 wybrano szablon zabezpieczeń aplikacji. Więcej informacji można znaleźć w sekcji „Konfiguracja kontroli dostępu” na str. 6.

1 Na wbudowanym serwerze WWW przejdź do strony konfiguracji aplikacji.

2 W sekcji Ekran logowania dla opcji Metoda logowania wybierz wartość **Karta lub logowanie ręczne**.

3 W sekcji Uwierzytelnianie użytkownika wykonaj poniższe czynności:

- Wybierz wartość **Usługa tożsamości** dla ustawienia Uwierzytelnianie karty.
- Ustaw wartość ustawienia Kontrola dostępu w przypadku rejestracji karty na **Usługa tożsamości**.
- Ustaw wartość ustawienia Kontrola dostępu w przypadku logowania ręcznego na **Usługa tożsamości**.
- Dla ustawienia Kontrola dostępu do sesji wybierz opcję **Aplikacja 2** lub **Rozwiązanie 2**.

Uwagi:

- Jeżeli dla ustawienia Kontrola dostępu w przypadku rejestracji karty wybrano wartość **Brak**, nie można zarejestrować karty w drukarce.
- Wybranie dla ustawienia Kontrola dostępu w przypadku logowania ręcznego wartości **Brak** wymaga tylko karty do zalogowania się, nawet gdy w ustawieniu Metoda logowania wybrano wartość **Karta lub logowanie ręczne**.
- Aby uzyskać więcej informacji na temat poszczególnych ustawień, zapoznaj się z pomocą otwieraną za pomocą myszy.

4 Wybierz opcję **Sprawdź certyfikat**, aby sprawdzić poprawność wszystkich połączeń z serwerem. Jeśli opcja Sprawdź certyfikat nie jest zaznaczona, urząd certyfikacji nie zostanie sprawdzony.

Uwaga: Ustawienie Zweryfikuj certyfikat dotyczy tylko sprawdzania poprawności usługi tożsamości i usługi WWW.

5 W menu Tryb weryfikacji wybierz opcję **łańcuch** lub **element równorzędny**.

Uwaga: Wartość domyślna to łańcuch.

6 Prześlij certyfikat SSL serwera, aby w bezpieczny sposób nawiązać połączenie z serwerem.

7 W polu SprawdzanieHostów wpisz dodatkowe nazwy hostów (inne niż domyślny adres URL serwera), aby zweryfikować wpisy w certyfikacie. Jeżeli istnieje wiele nazw hostów, oddziel je przecinkami.

Uwaga: Domyślnie biała lista zawiera tylko adres URL serwera. Wpisz dodatkowe nazwy hostów w polu SprawdzanieHostów, aby umieścić je na białej liście.

8 Kliknij przycisk **Zastosuj**.

Konfigurowanie ustawień usługi tożsamości

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

2 Jeżeli to konieczne, w sekcji Ustawienia usługi tożsamości zaznacz opcję **Włącz ekran oczekiwania**.

Uwaga: Drukarki eSF w wersji 2.x wymagają aplikacji eSF Security Manager, gdy opcja **Włącz ekran oczekiwania** jest wyłączona. Aby uzyskać listę tych drukarek, zobacz plik *Readme*.

3 Wpisz nazwę hosta lub adres IP dostawcy usługi tożsamości.

4 Jeżeli to konieczne, wprowadź nazwę hosta lub adres IP dostawcy usługi kart dostępu.

5 Prześlij certyfikat SSL serwera, aby w bezpieczny sposób nawiązać połączenie z serwerem.

6 Jeśli posiadasz identyfikator klienta oraz tajny klucz klienta od dostawcy usługi tożsamości, wprowadź te informacje w odpowiednich polach.

7 Ustaw zasady dostępu aplikacji.
- **Kontynuuj** – kontynuacja korzystania z drukarki nawet, gdy nie powiedzie się połączenie z serwerem usługi tożsamości.
- **Niepowodzenie** – przejście z powrotem do ekranu logowania, gdy nie powiedzie się połączenie z serwerem usługi tożsamości.

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

9 Kliknij przycisk **Zastosuj**.

Uwierzytelnianie PIN

Konfigurowanie uwierzytelniania użytkownika za pomocą numeru PIN

Przed rozpoczęciem upewnij się, że dla ustawienia Aplikacja 2 lub Rozwiązanie 2 wybrano szablon zabezpieczeń aplikacji. Więcej informacji można znaleźć w sekcji „Konfiguracja kontroli dostępu” na str. 6.

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

2 W sekcji Ekran logowania w ustawieniu Metoda logowania wybierz opcję, która obsługuje uwierzytelnianie za pomocą numeru PIN.

3 W sekcji Uwierzytelnianie użytkownika wykonaj poniższe czynności:
- Wybierz uwierzytelnianie karty jako preferowaną metodę uwierzytelniania.
- W ustawieniu Kontrola dostępu w przypadku rejestracji karty wybierz preferowaną metodę kontroli dostępu.

- Dla ustawienia Kontrola dostępu w przypadku numeru PIN wybierz opcję **Aplikacja 1** lub **Rozwiązanie 1**.
- W ustawieniu Kontrola dostępu w przypadku logowania ręcznego wybierz preferowaną metodę kontroli dostępu.
- Dla ustawienia Kontrola dostępu do sesji wybierz opcję **Aplikacja 2** lub **Rozwiązanie 2**.

Uwagi:

- Jeżeli dla ustawienia Kontrola dostępu w przypadku numeru PIN wybrano wartość **Brak**, nie można zarejestrować numeru PIN w drukarce.
- Aby uzyskać więcej informacji na temat poszczególnych ustawień, zapoznaj się z pomocą otwieraną za pomocą myszy.

4 Kliknij przycisk **Zastosuj**.

Konfigurowanie ustawień PIN

1 Na wbudowanym serwerze WWW przejdź do strony konfiguracji aplikacji.

2 Wybierz metodę logowania w sekcji Ustawienia kodu PIN menu Wymagane dane.
- Identyfikator i kod PIN użytkownika – wymaga podania nazwy użytkownika i kodu PIN w celu uwierzytelnienia.
- Tylko kod PIN – wymaga podania numeru PIN w celu uwierzytelnienia.

3 Wprowadź adres serwera WWW i wybierz minimalną długość numeru PIN.

4 Wprowadź treść komunikatów o wprowadzeniu błędnego numeru PIN.

5 Kliknij przycisk **Zastosuj**.

Uwierzytelnianie za pomocą LDAP

Korzystaj z uwierzytelniania za pomocą LDAP podczas weryfikacji użytkowników za pośrednictwem serwera LDAP.

Konfigurowanie uwierzytelniania użytkownika LDAP

Zanim rozpoczniesz, upewnij się że:
- Dla ustawienia Aplikacja 2 lub Rozwiązanie 2 wybrano szablon zabezpieczeń aplikacji.
- Dla ustawienia Aplikacja 3 lub Rozwiązanie 3 wybrano szablon zabezpieczeń LDAP.

Uwaga: Więcej informacji można znaleźć w sekcji „Konfiguracja kontroli dostępu” na str. 6.

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

2 W sekcji Ekran logowania dla opcji Metoda logowania wybierz wartość **Karta lub logowanie ręczne**.

3 W sekcji Uwierzytelnianie użytkownika wykonaj poniższe czynności:
- Dla ustawienia Uwierzytelnianie karty wybierz wartość **LDAP**.
- Dla ustawienia Kontrola dostępu w przypadku rejestracji karty wybierz opcję **Aplikacja 3** lub **Rozwiązanie 3**.

- Dla opcji Kontrola dostępu w przypadku logowania ręcznego wybierz wartość **Aplikacja 3** lub **Rozwiązanie 3**.
- Dla ustawienia Kontrola dostępu do sesji wybierz opcję **Aplikacja 2** lub **Rozwiązanie 2**.

Uwagi:

- Jeżeli dla ustawienia Kontrola dostępu w przypadku rejestracji karty wybrano wartość **Brak**, nie można zarejestrować karty w drukarce.
- Wybranie dla ustawienia Kontrola dostępu w przypadku logowania ręcznego wartości **Brak** wymaga tylko karty do zalogowania się nawet, gdy w ustawieniu Metoda logowania wybrano wartość **Karta lub logowanie ręczne**.
- Aby uzyskać więcej informacji na temat poszczególnych ustawień, zapoznaj się z pomocą otwieraną za pomocą myszy.

4 Kliknij przycisk **Zastosuj**.

Konfigurowanie ustawień LDAP

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

2 Skonfiguruj ustawienia w sekcji Ustawienia LDAP.

Uwagi:

- Jeżeli zaznaczono opcję **Użyj książki adresowej**, aplikacja korzysta z ustawień LDAP, które skonfigurowano już na kontach sieciowych drukarki.
- Aby uzyskać więcej informacji na temat poszczególnych ustawień, zapoznaj się z pomocą otwieraną za pomocą myszy.

3 Kliknij przycisk **Zastosuj**.

Ustawianie preferencji aplikacji

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

2 Wykonaj co najmniej jedną spośród następujących czynności:

- Aby dostosować ekran główny drukarki, skonfiguruj ustawienia ekranu głównego.
- Aby wyświetlić komunikaty rejestracji, w sekcji Ustawienia zaawansowane zaznacz opcje **Wyświetl komunikat rozpoczęcia rejestracji** i **Wyświetl komunikat o zakończeniu rejestracji**.
- Aby usłyszeć *sygnał dźwiękowy* po pomyślnym zalogowaniu, w sekcji Ustawienia zaawansowane zaznacz opcję **Włącz sygnał dźwiękowy dla pomyślnego logowania** i dostosuj częstotliwość sygnału dźwiękowego.
- Aby skorzystać z profilu po pomyślnym zalogowaniu, w sekcji Ustawienia zaawansowane w polu Profil logowania wpisz nazwę profilu.

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

3 Kliknij przycisk **Zastosuj**.

Wyświetlanie dostępnych profili

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

2 Kliknij kolejno **Zarządzaj skrótami** > **Zarządzaj skrótami profili**.

Wyświetlanie obszarów kont użytkowników

Funkcja Użyj wybranego obszaru ma zastosowanie tylko wtedy, gdy metody logowania w przypadku rejestrowania karty i logowania ręcznego to Kerberos, Active Directory lub LDAP+GSSAPI. Funkcja ta ma również zastosowanie tylko w przypadku wybrania wartości Usługa sieciowa lub Za pomocą drukarki dla ustawienia uwierzytelniania kartą.

W przypadku rejestracji karty, jeżeli funkcja ta jest włączona, identyfikator zarejestrowanej karty dostępu ma format nazwa_użytkownika@obszar.

W przypadku logowania ręcznego, jeżeli funkcja ta jest włączona, nazwa użytkownika wyświetlana w panelu sterowania drukarki ma format nazwa_użytkownika@obszar.

Ustawienia te nie mają zastosowania w stosunku do logowania za pomocą numeru PIN i rejestracji numeru PIN.

Aby włączyć tę funkcję, wykonaj poniższe instrukcje:

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

2 W sekcji Ustawienia zaawansowane zaznacz opcję **Użyj wybranego obszaru**.

3 Kliknij przycisk **Zastosuj**.

Eksportowanie lub importowanie pliku konfiguracyjnego

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

2 Wyeksportuj lub zaimportuj plik konfiguracyjny.

Uwagi:

- W przypadku wystąpienia błędu **braku pamięci wirtualnej maszyny Java** należy powtarzać eksport, aż do momentu zapisania pliku konfiguracji.
- W przypadku przekroczenia limitu czasu i pojawieniu się pustego ekranu należy odświeżyć przeglądarkę i kliknąć przycisk **Zastosuj**.

Zarządzanie aplikacją

Uwaga: Strona stanu dla danej aplikacji dostępna jest tylko w przypadku korzystania z uwierzytelniania za pomocą drukarki.

Uzyskiwanie dostępu do strony stanu aplikacji

Za pomocą strony stanu można monitorować działanie drukarki.

1. W oknie wbudowanego serwera Embedded Web Server kliknij opcje **Aplikacje** > **Uwierzytelnianie kartą**.
2. Należy pamiętać poniższe informacje:
   - **Stan** – przedstawia stan działania drukarki.
     - **Nie skonfigurowano** – drukarka nie została skonfigurowana.
     - **Tryb offline** – brak komunikacji lub działania drukarki.
     - **Tryb online** – drukarka jest aktywna.
   - **Czas pracy bez przerw** – wskazuje czas pracy aplikacji.
   - **(ta drukarka)** – bieżąca drukarka.
   - **Ostatnie działanie** – ostatnie działanie drukarki głównej.
   - **Liczba użytkowników** – całkowita liczba zarejestrowanych użytkowników.
   - **Status rejestracji** – wskazuje, czy drukarka jest w stanie offline lub online.
   - **Ostatnia synchronizacja z drukarką główną** – czas ostatniej aktualizacji drukarki zapasowej.
   - **Ostatni kontakt z drukarką główną** – czas ostatniej komunikacji drukarki zapasowej z drukarką główną.
   - **Ostatnia synchronizacja jako drukarki głównej** – wskazuje kiedy drukarka zapasowa funkcjonowała jako główna.
   - **Ostatnie działanie jako drukarka główna** – ostatnie działanie drukarki zapasowej, gdy funkcjonowała jako główna.
   - **Czas jako drukarka główna** – wskazuje czas, przez który drukarka zapasowa działała jako główna.
   - **Aktualnie obsługiwany przez** – drukarka-klient ostatnio kontaktująca się z drukarką główną lub zapasową.
   - **Ostatnie działanie jako drukarka zapasowa** – czas ostatniego kontaktu drukarki-klienta z drukarką zapasową.

Zarządzanie kontami użytkowników i drukarkami-klientami

Uwaga: Ta opcja pojawia się tylko, gdy drukarka działa jako drukarka główna.

1. Na serwerze Embedded Web Server przejdź do strony stanu aplikacji.
2. Spróbuj poniższych rozwiązań:

Usuwanie kont użytkowników

a W sekcji Główna kliknij przycisk **Usuń użytkowników**.

b Wpisz jeden lub więcej identyfikatorów użytkowników i usuń je.

Dodawanie drukarek-klientów

a W sekcji Klienci kliknij **Dodaj klientów**.

b Wprowadź jeden lub więcej adresów IP drukarek i dodaj je.

Usuwanie drukarek-klientów

Uwaga: Nie można usuwać drukarek-klientów, gdy drukarka główna jest odłączona od sieci lub gdy odinstalowano aplikację.

a Wybierz z sekcji Klienci jedną lub więcej drukarek-klientów.

b Kliknij przycisk **Usuń klientów**.

Ponowne przydzielanie ról drukarek

1 Skonfiguruj nową drukarkę główną.

a Na serwerze Embedded Web Server nowej drukarki głównej przejdź do strony konfiguracji aplikacji.

b W sekcji Uwierzytelnianie kartą za pomocą drukarki dla ustawienia Rola wybierz wartość **Główna**.

c Wpisz nazwę hosta lub adres IP drukarki zapasowej.

d Kliknij przycisk **Zastosuj**.

2 Przypisz drukarkę zapasową do nowej drukarki głównej.

a Na serwerze Embedded Web Server drukarki zapasowej przejdź do strony konfiguracji aplikacji.

b W sekcji Uwierzytelnianie karty przy użyciu drukarki wpisz nazwę hosta lub adres IP nowej drukarki głównej.

c Kliknij przycisk **Zastosuj**.

3 Usuń drukarkę-klienta z bieżącej drukarki głównej.

a Na serwerze Embedded Web Server bieżącej drukarki głównej przejdź do strony stanu aplikacji.

b W sekcji Klienci usuń drukarkę-klienta.

4 Przypisz ponownie drukarkę-klienta do nowej drukarki głównej. Wykonaj jedną z następujących czynności:

Korzystanie ze strony konfiguracji aplikacji

a Na serwerze Embedded Web Server drukarki-klienta przejdź do strony konfiguracji aplikacji.

b W sekcji Uwierzytelnianie kartą za pomocą drukarki dla ustawienia Rola wybierz wartość **Klient**.

c Wpisz nazwę hosta lub adres IP nowej drukarki głównej.

Uwaga: Upewnij się, że nazwa hosta lub adres IP drukarki zapasowej są prawidłowe.

d Kliknij przycisk **Zastosuj**.

Korzystanie ze strony stanu drukarki głównej

a Na serwerze Embedded Web Server nowej drukarki głównej przejdź do strony stanu aplikacji.

b W sekcji Klienci kliknij **Dodaj klientów**.

c Wpisz adres IP drukarki-klienta, a następnie dodaj ją.

Korzystanie z aplikacji

Rejestrowanie użytkowników

1 Dotknij kartą czytnika.

2 Na panelu sterowania drukarki wprowadź swoje dane uwierzytelniające.

Uwaga: Jeżeli korzystasz z rozwiązania Kerberos, Active Directory lub LDAP+GSSAPI do rejestracji karty, wybierz obszar.

3 Postępuj według instrukcji widocznych na wyświetlaczu.

Rejestrowanie umeru PIN

Przed rozpoczęciem upewnij się, że metoda logowania obsługuje uwierzytelnianie za pomocą numeru PIN.

1 Na panelu sterowania drukarki dotknij opcji **Logowanie za pomocą PIN**.

2 Postępuj według instrukcji widocznych na wyświetlaczu.

Ręczne logowanie się do drukarki

1 Na panelu sterowania drukarki przejdź do jednej z następujących opcji:

- **Logowanie za pomocą kodu PIN**
- **Logowanie ręczne**
- **Logowanie administratora**

Uwaga: Po wybraniu opcji **Logowanie administratora** pozyskiwanie innych informacji o użytkowniku z serwera LDAP nie będzie możliwe.

2 Wprowadź swoje dane logowania.

Uwaga: Jeśli używasz protokołu Kerberos, Active Directory®lub LDAP+GSSAPI w celu ręcznego logowania, wybierz obszar.

3 Postępuj według instrukcji widocznych na wyświetlaczu.

Rozwiązywanie problemów

Błąd aplikacji

Spróbuj następujących rozwiązań:

Sprawdzanie dziennika systemu

1. W oknie wbudowanego serwera WWW kliknij **Ustawienia** lub **Konfiguracja**.
2. W zależności od modelu drukarki wykonaj jedną z następujących czynności:
   - Kliknij opcje **Aplikacje** > **Zarządzanie aplikacjami**.
   - Kliknij opcje **Rozwiązania urządzenia** > **Rozwiązania (eSF)**.
   - Kliknij **Embedded Solutions**.
3. Kliknij opcje **System** > **Dziennik**.
4. Wybierz i prześlij odpowiednie filtry.
5. Przeanalizuj dziennik, a następnie rozwiąż problem.

Skontaktuj się z przedstawicielem firmy Lexmark

Aplikacja nie działa w przypadku zaktualizowanej wersji Zwalniania wydruków SaaS.

Spróbuj następujących rozwiązań:

Upewnij się, że zwalnianie wydruków jest skonfigurowane poprawnie.

Jeżeli zaktualizowano aplikację Print Management SaaS do wersji 2.0 lub nowszej funkcji Zwalnianie wydruków, należy pamiętać o wyłączeniu opcji Tło i wygaszacz ekranu. Przypisz metodę kontroli dostępu Uwierzytelnianie kartą do funkcji Zwalnianie wydruków i upewnij się, że funkcja Zwalnianie wydruków została poprawnie skonfigurowana. Aby uzyskać więcej informacji, zapoznaj się z *Podręcznikiem administratora zwalniania wydruków*.

Skontaktuj się z przedstawicielem firmy Lexmark

Błąd uwierzytelniania

Spróbuj następujących rozwiązań:

Wydłużenie limitu czasu oczekiwania na drukarkę

Jeżeli korzystasz z usługi tożsamości jako metody uwierzytelniania karty, drukarka może potrzebować więcej czasu na komunikację z dostawcą usługi tożsamości.

1. W oknie wbudowanego serwera WWW kliknij **Ustawienia** lub **Konfiguracja**.
2. Kliknij kolejno **Ustawienia ogólne** > **Limity czasu**.
3. Zwiększ czas wygaszania ekranu i przejścia w tryb uśpienia.
4. Kliknij opcję **Wyślij**.

Upewnij się, że drukarka jest podłączona do sieci komputerowej

Więcej informacji można znaleźć w *Podręczniku użytkownika* drukarki.

Sprawdź, czy serwer zabezpieczeń jest włączony i nie jest zajęty

Aby uzyskać więcej informacji, skontaktuj się z administratorem systemu.

Użytkownik jest zablokowany

Użytkownik prawdopodobnie osiągnął maksymalną liczbę dozwolonych nieudanych prób logowania.

Zwiększenie czasu blokady oraz dozwolonej liczby nieudanych prób logowania

1. W zależności od modelu drukarki w serwerze Embedded Web Server wykonaj jedną z poniższych czynności:
   - Kliknij kolejno opcje **Ustawienia** > **Bezpieczeństwo** > **Różne ustawienia zabezpieczeń** > **Ograniczenia logowania**.
   - Kliknij kolejno **Konfiguracja** > **Bezpieczeństwo**.
2. Zwiększ czas blokady oraz dozwoloną liczbę nieudanych prób logowania lub opóźnienie automatycznego logowania.
3. Kliknij opcję **Wyślij**.

Nie można zarejestrować drukarki-klienta

Spróbuj następujących rozwiązań:

Upewnij się, że drukarka główna (lub zapasowa) jest włączona

Więcej informacji można znaleźć w sekcji „Uzyskiwanie dostępu do strony stanu aplikacji” na str. 17.

Upewnij się, że drukarka główna i zapasowa zostały poprawnie skonfigurowane

Więcej informacji można znaleźć w sekcji „Konfigurowanie uwierzytelniania użytkownika za pomocą drukarki” na str. 9.

Należy pamiętać o limicie 23 zarejestrowanych drukarek-klientów

Więcej informacji można znaleźć w sekcji „Zarządzanie kontami użytkowników i drukarkami-klientami” na str. 17.

Skontaktuj się z przedstawicielem firmy Lexmark

Nie można zweryfikować karty

Spróbuj następujących rozwiązań:

Ustaw metodę logowania na Karta lub logowanie ręczne

1. Na serwerze Embedded Web Server przejdź do strony konfiguracji aplikacji.
2. W sekcji Ekran logowania dla opcji Metoda logowania wybierz wartość **Karta lub logowanie ręczne**.
3. Kliknij przycisk **Zastosuj**.

Skontaktuj się z przedstawicielem firmy Lexmark

Informacje o obszarze niedostępne

Spróbuj następujących rozwiązań:

Niektóre metody logowania dla logowania ręcznego lub rejestracji karty, takie jak konta lokalne lub LDAP, nie wymagają wyboru obszaru. Metody logowania, które wymagają wyboru obszaru to Kerberos, Active Directory i LDAP+GSSAPI.

Wyłączanie wyboru obszaru

1. Na serwerze Embedded Web Server przejdź do strony konfiguracji aplikacji.
2. W sekcji Ustawienia zaawansowane usuń zaznaczenie opcji **Użyj wybranego obszaru**.
3. Kliknij przycisk **Zastosuj**.

Zmiana metody logowania

1. Na serwerze Embedded Web Server przejdź do strony konfiguracji aplikacji.
2. W sekcji Uwierzytelnianie użytkownika wybierz wartość **Aplikacja 1** lub **Rozwiązanie 1** dla ustawień Kontrola dostępu w przypadku rejestracji karty i Kontrola dostępu w przypadku logowania ręcznego.
3. Kliknij przycisk **Zastosuj**.

Skontaktuj się z przedstawicielem firmy Lexmark

Nie można połączyć się z serwerem LDAP

Spróbuj następujących rozwiązań:

Upewnij się, że ustawienia LDAP są skonfigurowane poprawnie

Więcej informacji można znaleźć w sekcji „Konfigurowanie ustawień LDAP” na str. 15.

Skontaktuj się z przedstawicielem firmy Lexmark

Najczęściej zadawane pytania

Dlaczego nie można dodać lub usunąć drukarki-klienta, gdy drukarka zapasowa działa jako główna?

Drukarkę-klienta można usunąć lub dodać tylko wtedy, gdy drukarka główna jest włączona.

Czy mogę usunąć drukarkę-klienta i ponownie przypisać ją do nowej drukarki głównej, jeśli bieżąca drukarka główna jest wyłączona?

Tak, wykonaj poniższe czynności:

1. Zainstaluj aplikację na wbudowanym serwerze WWW drukarki-klienta.
2. Ustaw rolę drukarki-klienta i ustaw dla niej nową drukarkę główną i zapasową. Więcej informacji można znaleźć w sekcji „Konfiguracja roli drukarki” na str. 10.

Co zrobić, gdy na drukarce przypadkowo odinstalowano aplikację?

1. Zainstaluj daną aplikację na wbudowanym serwerze WWW.
2. Ustaw rolę drukarki. Więcej informacji można znaleźć w sekcji „Konfiguracja roli drukarki” na str. 10.

   Uwaga: Upewnij się, że najpierw konfigurowana jest drukarka główna, następnie drukarka zapasowa, a potem drukarki-klienty.
3. Skonfiguruj drukarkę w zależności od jej roli.

   Uwagi:

   - Jeżeli aplikacja zostanie ponownie zainstalowana na drukarce głównej, przypisz ją do drukarki zapasowej.
   - Jeżeli aplikacja zostanie ponownie zainstalowana na drukarce zapasowej, przypisz ją do drukarki głównej.
   - Jeżeli aplikacja zostanie ponownie zainstalowana na drukarce-kliencie, przypisz ją do drukarki głównej i drukarki zapasowej.
   - Więcej informacji można znaleźć w sekcji „Ponowne przydzielanie ról drukarek” na str. 18.

Dlaczego nie widać przycisków kopiowania i faksowania na ekranie blokady, jeżeli włączono dostęp do nich bez konieczności logowania?

Ustaw kontrolę dostępu do funkcji kopiowania i faksowania na **Bez zabezpieczeń**. Więcej informacji można znaleźć w sekcji „Konfigurowanie ekranu logowania” na str. 9.

Co stanie się, jeżeli ustawiono tę samą kontrolę dostępu dla ustawień Kontrola dostępu w przypadku logowania ręcznego i Kontrola dostępu do sesji?

Aby uzyskać dostęp do funkcji drukarki z poziomu ekranu głównego, konieczne jest wprowadzenie poświadczeń podczas ręcznego logowania.

Czy mogę korzystać z różnej kontroli dostępu dla ustawień Kontrola dostępu w przypadku logowania ręcznego i Uwierzytelnianie karty?

Tak, za wyjątkiem sytuacji, gdy korzystasz z uwierzytelniania za pomocą usługi tożsamości. Wtedy należy skonfigurować wartość ustawień Kontrola dostępu w przypadku logowania ręcznego i Uwierzytelnianie karty na **Usługa tożsamości**.

Dlaczego funkcja Logowanie administratora nie działa z kontami sieciowymi?

Funkcja **Logowanie administratora** działa jedynie w przypadku kont wewnętrznych, kodu PIN i hasła szablonów zabezpieczeń.

Informacje

Informacje o wydaniu

Grudzień 2020

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 WYRAŹNYCH 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**.

GOVERNMENT END USERS

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

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.

Indeks