Card Authentication

Administratörshandbok

December 2020

www.lexmark.com

Innehåll

Översikt

Använd programmet för säker åtkomst till en skrivare med en kortläsare. När en användare trycker autentiseras användarens uppgifter på något av följande sätt:

- Med en masterskrivare. Om masterskrivaren är offline fungerar reservskrivaren som masterskrivare tills masterenheten är online.

  Obs! Se till att skrivarna är anslutna till samma nätverk när du konfigurerar dem.
- LDAP (Lightweight Directory Access Protocol), LDD-servrar (Lexmark™ Document Distributor) eller identitetstjänsteleverantörer beroende på autentiseringen som angetts i organisationen.

Det här dokumentet innehåller instruktioner om hur du konfigurerar, använder och felsöker programmet.

Krav vid konfigurering

Du kan behöva administratörsbehörighet för att konfigurera programmet.

Öppna den inbyggda webbservern

1. Hämta skrivarens IP-adress. Gör något av följande:
   - Leta upp skrivarens IP-adress på skrivarens startskärm.
   - Visa IP-adressen i TCP/IP-avsnittet på menyn Nätverk/portar.
2. Öppna en webbläsare och skriv skrivarens IP-adress.

Lägga till ett internt användarkonto

Ett internt användarkonto krävs när du använder skrivarbaserad autentisering.

1. Från den inbäddade webbservern klickar du på **Inställningar** eller **Konfiguration**.
2. Beroende på skrivarmodell gör du något av följande:
   - Klicka på **Säkerhet** > **Säkerhetsinställningar** > **Interna konton** > **Lägg till ett internt konto**.
   - Klicka på **Säkerhet** > **Redigera säkerhetsinställningar** > **Interna konton** > **Lägg till ett internt konto**.
3. Skriv kontouppgifterna och klicka på **Skicka**.
4. Vid behov kan du skriva namnet på ett anpassat byggblock i avsnittet Hantera interna konton och sedan ange rätt användaruppgifter.
5. Klicka på **Skicka**.

Konfigurera grupper för interna användarkonton

1. I Embedded Web Server klickar du på **Inställningar** eller **Konfiguration**.
2. Beroende på skrivarmodell gör du något av följande:
   - Klicka på **Säkerhet** > **Säkerhetsinställningar** > **Interna konton** > **Konfigurera grupper för användning med interna konton**.
   - Klicka på **Säkerhet** > **Redigera säkerhetsinställningar** > **Interna konton** > **Konfigurera grupper för användning med interna konton**.
3. Ange ett gruppnamn och klicka sedan på **Lägg till**.
4. Lägg till interna konton i gruppen.
5. Klicka på **Skicka**.

Skapa en säkerhetsmall

En säkerhetsmall består av byggblock för t.ex. interna konton, Kerberos, LDAP, LDAP+GSSAPI och Active Directory. Dessa mallar används vid åtkomstkontroll för att skydda skrivarfunktionerna och programmen.

1. I Embedded Web Server klickar du på **Inställningar** eller **Konfiguration**.
2. Beroende på skrivarmodell gör du något av följande:
   - Klicka på **Säkerhet** > **Säkerhetsinställningar** > **Säkerhetsmall** > **Lägg till en säkerhetsmall**.
   - Klicka på **Säkerhet** > **Redigera säkerhetsinställningar** > **Säkerhetsmallar** > **Lägg till en säkerhetsmall**.
3. Skriv ett namn på en säkerhetsmall och välj sedan en av följande autentiseringsmetoder:
   - Välj ett byggblock för ett internt konto för skrivarbaserad autentisering i en fristående installation.
   - För skrivarbaserad autentisering med Lexmark Print Management (LPM) Serverless Print Release i en Active Directory-konfiguration väljer du byggblocket LDAP+GSSAPI.
   - För LDAP-autentisering väljer du ett LDAP-byggblock.
4. Klicka på **Spara mall**.

Obs! För att ändra en befintlig säkerhetsmall klickar du på säkerhetsmallen och lägger till eller ändrar en behörighet för mallen.

Konfigurera åtkomstkontroll

Obs! Säkerställ att du har konfigurerat säkerhetsmallen för interna konton när du använder funktionen **Administratörsinloggning**. Mer information finns i “Skapa en säkerhetsmall” på sidan 6.

1. I Embedded Web Server klickar du på **Inställningar** eller **Konfiguration**.
2. Beroende på skrivarmodell gör du något av följande:
   - Klicka på **Säkerhet** > **Säkerhetsinställningar** > **Åtkomstkontroll**.
   - Klicka på **Säkerhet** > **Redigera säkerhetsinställningar** > **Åtkomstkontroll**.
3. Klicka på **Enhetsprogram** eller **Enhetslösningar** och gör sedan följande:
   - Ställ in Program 1 eller Lösning 1 på ett internt konto eller en säkerhetsmall för LDAP+GSSAPI eller Active Directory.
   - Ställ in Program 2 eller Lösning 2 på programmets säkerhetsmall.

     Obs! Programmets säkerhetsmall är mallen med CardAuth som autentiseringsinställning. Mer information finns i “Skapa en säkerhetsmall” på sidan 6.
   - Ställ in Program 3 eller Lösning 3 på en LDAP-säkerhetsmall.

   Anmärkningar:

   - Om LPM Print Release är installerat ställer du in åtkomstkontroll för Print Release på programmets säkerhetsmall.
   - Skrivare med eSF (Embedded Solutions Framework) version 2.x måste ha programmet eSF Security Manager för att konfigurera åtkomstkontroll. En lista över sådana skrivare finns i filen *Viktigt*.
4. Klicka på **Skicka**.

Konfigurera programmet

Gör så här innan du börjar:

- Avaktivera Bakgrund och Inaktiv skärm samt eventuella autentiseringsprogram.
- Installera följande:
  - Installationsprogrammet för Card Authentication
  - Drivrutinen för kortläsaren
  - Kortläsaren
  - eSF Security Manager

    Obs! Skrivare med eSF version 2.x måste ha programmet eSF Security Manager för att konfigurera åtkomstkontroll. En lista över sådana skrivare finns i filen *Viktigt*.

Öppna programmets konfigurationssida

1. Från den inbäddade webbservern klickar du på **Inställningar** eller **Konfiguration**.
2. Beroende på skrivarmodellen gör du något av följande:
   - Klicka på **Program** > **Hantering av program**.
   - Klicka på **Enhetslösningar** > **Lösningar (eSF)**.
   - Klicka på **Inbäddade lösningar**.
3. Klicka på **Kortautentisering** > **Konfigurera**.

Konfigurera administratörsautentisering

Obs! Säkerställ att du har konfigurerat säkerhetsmallen för Interna konton, PIN-kod och Lösenord när du använder funktionen **Administratörsinloggning**. Mer information finns i “Skapa en säkerhetsmall” på sidan 6.

1. Öppna programmets konfigurationssida genom Embedded Web Server.
2. I avsnittet Användarautentisering konfigurerar du **Åtkomstkontroll för administratörsinloggning** till önskad inloggningsmetod.

   Anmärkningar:

   - Säkerställ att den valda åtkomstkontrollen är konfigurerad med en säkerhetsmall. Mer information finns i “Skapa en säkerhetsmall” på sidan 6.
   - Om du väljer **Inaktiverad** döljs alternativet **Administratörsinloggning** på skrivarpanelen.
3. Klicka på **Verkställ**.

Konfigurera inloggningsskärmen

Inloggningsskärmen kan konfigureras att göra följande:

- Tillåt användarna att använda kopierings- och faxfunktionerna utan att inloggning krävs.
- Tillåt användarna att välja vilken inloggningsmetod som ska användas.

- Lägga till en bakgrund på inloggningsskärmen och anpassa inloggningsmeddelandet.
- Inaktivera varningen när ingen kortläsare är ansluten.

1 Öppna programmets konfigurationssida genom Embedded Web Server.

2 Konfigurera inställningarna i avsnittet Inloggningsskärm.

Obs! Mer information om inställningarna visas om du för pekaren över hjälpen.

3 Klicka på **Verkställ**.

Aktivera kopiering eller faxning utan inloggning

Om Tillåt kopiering utan inloggning eller Tillåt faxning utan inloggning är aktiverat kan du göra följande:

1 I Embedded Web Server klickar du på **Inställningar** eller **Konfiguration**.

2 Beroende på skrivarmodell gör du något av följande:
- Klicka på **Säkerhet** > **Säkerhetsinställningar** > **Åtkomstkontroll** > **Funktionsbehörighet**.
- Klicka på **Säkerhet** > **Redigera säkerhetsinställningar** > **Åtkomstkontroll**.

3 Ställ in kopierings- eller faxfunktionen på **Ingen säkerhet**.

4 Klicka på **Skicka**.

Skrivarbaserad autentisering

Använd skrivarbaserad autentisering när användare valideras via en masterskrivare.

Konfigurera skrivarbaserad användarautentisering

Innan du börjar ser du till att:
- Åtkomstkontroll för App 1 eller Lösning 1 är inställt på ett internt konto eller en säkerhetsmall för LDAP +GSSAPI eller Active Directory.
- Åtkomstkontroll för App 2 eller Lösning 2 är inställt på programmets säkerhetsmall.

Obs! Mer information finns i “Konfigurera åtkomstkontroll” på sidan 6.

1 Öppna programmets konfigurationssida från den inbyggda webbservern.

2 I avsnittet Inloggningsskärm ställer du in Inloggningsmetod på **Kortinloggning eller manuell inloggning**.

3 I avsnittet Användarautentisering gör du följande:
- Ställ in Kortvalidering på **Skrivarbaserad**.
- Ställ in åtkomstkontroll för kortregistrering på **App 1** eller **Lösning 1**.
- Ställ in åtkomstkontroll för manuell inloggning på **App 1** eller **Lösning 1**.
- Ange sessionens åtkomstkontroll som **App 2** eller **Lösning 2**.

Anmärkningar:

- Om åtkomstkontroll för kortregistrering är inställt på **Ingen** kan du inte registrera kortet på skrivaren.
- Om du ställer in åtkomstkontroll för manuell inloggning på **Ingen** krävs bara ett kort för inloggning även om Inloggningsmetod är inställt på **Kortinloggning eller manuell inloggning**.

- Mer information om inställningarna visas om du för pekaren över hjälpen.

4 Klicka på **Verkställ**.

Konfigurera skrivarens roll

Obs! En klientskrivare måste ha en masterskrivare och en reservskrivare.

1 Öppna programmets konfigurationssida från den inbyggda webbservern.

2 Ange skrivarens roll i avsnittet Skrivarbaserad kortvalidering.

- **Master** – skrivaren har en lista över registrerade användare.
- **Reserv** – om masterskrivaren är offline antar reservskrivaren rollen som masterskrivare tills masterskrivaren är online.
- **Klient** – ingen information om användarna lagras i skrivaren. En master- eller reservskrivare krävs för att validera användarnas uppgifter.

Anmärkningar:

- Om du använder endast en skrivare anger du den som masterskrivare.
- Om du använder två skrivare anger du en som masterskrivare och den andra som reservskrivare.
- Om du använder tre eller fler skrivare anger du en som masterskrivare, en som reservskrivare och övriga som klientskrivare.

3 Skriv värdnamnet eller IP-adressen för masterskrivaren och reservskrivaren.

Anmärkningar:

- Vid konfigureringen av en reservskrivare krävs att du anger masterskrivarens värdnamn eller IP-adress.
- Vid konfigureringen av klientskrivare krävs att du anger både masterskrivarens och reservskrivarens värdnamn eller IP-adress.
- Innan du tilldelar en klientskrivare till en ny masterskrivare tar du bort den från den gamla masterskrivaren.

4 Klicka på **Verkställ**.

Autentisering med webbtjänst

Använd autentisering med en webbtjänst när användare valideras via en LDD-server.

Konfigurera användarautentisering med en webbtjänst

Innan du börjar kontrollerar du att åtkomstkontroll för Program 2 eller Lösning 2 är inställt på programmets säkerhetsmall. Mer information finns i “Konfigurera åtkomstkontroll” på sidan 6.

1 Öppna programmets konfigurationssida genom Embedded Web Server.

2 I avsnittet Inloggningsskärm ställer du in Inloggningsmetod på **Kortinloggning eller manuell inloggning**.

3 I avsnittet Användarautentisering gör du följande:
   - Ställ in Kortvalidering på **Webbtjänst**.
   - Ställ in Åtkomstkontroll för kortregistrering och Åtkomstkontroll för manuell inloggning på önskad metod för åtkomstkontroll.
   - Ange Sessionens åtkomstkontroll som **Program 2** eller **Lösning 2**.

   Anmärkningar:

   - Om Åtkomstkontroll för kortregistrering är inställt på **Ingen** kan du inte registrera kortet på skrivaren.
   - Om du ställer in Åtkomstkontroll för manuell inloggning på **Ingen** krävs bara ett kort för inloggning även om Inloggningsmetod är inställt på **Kortinloggning eller manuell inloggning**.
   - Mer information om inställningarna visas om du för pekaren över hjälpen.

4 Välj **Verifiera certifikat** för att validera alla anslutningar till servern. Om du inte väljer Verifiera certifikat kommer CA inte att valideras.

   Obs! Inställningen Verifiera certifikat gäller endast för validering av identitetstjänst och webbtjänst.

5 I menyn Verifieringsläge väljer du antingen **kedja** eller **peer** .

   Obs! Standardvärdet är kedja.

6 Överför serverns SSL-certifikat för säker anslutning till servern.

7 I fältet Kontrollvärdar skriver du in de ytterligare värdnamnen (förutom standardserverns URL) för att verifiera posterna i certifikatet. Använd kommatecken för att skilja flera värdnamn åt.

   Obs! Som standard innehåller den vitlistan bara serverns URL. Skriv in ytterligare värdnamn i fältet Kontrollvärdar för att inkludera dem i vitlistan.

8 Klicka på **Verkställ**.

Konfigurera webbtjänstinställningar

1 Öppna programmets konfigurationssida från den inbyggda webbservern.

2 Konfigurera inställningarna i avsnittet Webbtjänstinställningar.

   Obs! Mer information om inställningarna visas om du för pekaren över hjälpen.

3 Klicka på **Verkställ**.

Autentisering med identitetstjänst

Använd autentisering med en identitetstjänst när användare valideras via en identitetstjänsteserver, t.ex. LPM SaaS-server.

Konfigurera användarautentisering med en identitetstjänst

Innan du börjar kontrollerar du att åtkomstkontroll för Program 2 eller Lösning 2 är inställt på programmets säkerhetsmall. Mer information finns i “Konfigurera åtkomstkontroll” på sidan 6.

1 Öppna programmets konfigurationssida genom Embedded Web Server.

2 I avsnittet Inloggningsskärm ställer du in Inloggningsmetod på **Kortinloggning eller manuell inloggning**.

3 I avsnittet Användarautentisering gör du följande:
   - Ställ in Kortvalidering på **Identitetstjänst**.
   - Ställ in Åtkomstkontroll för kortregistrering på **Identitetstjänst**.
   - Ställ in Åtkomstkontroll för manuell inloggning på **Identitetstjänst**.
   - Ange Sessionens åtkomstkontroll som **Program 2** eller **Lösning 2**.

   Anmärkningar:

   - Om Åtkomstkontroll för kortregistrering är inställt på **Ingen** kan du inte registrera kortet på skrivaren.
   - Om du ställer in Åtkomstkontroll för manuell inloggning på **Ingen** krävs bara ett kort för inloggning även om Inloggningsmetod är inställt på **Kortinloggning eller manuell inloggning**.
   - Mer information om inställningarna visas om du för pekaren över hjälpen.

4 Välj **Verifiera certifikat** för att validera alla anslutningar till servern. Om du inte väljer Verifiera certifikat kommer CA inte att valideras.

   Obs! Inställningen Verifiera certifikat gäller endast för validering av identitetstjänst och webbtjänst.

5 I menyn Verifieringsläge väljer du antingen **kedja** eller **peer** .

   Obs! Standardvärdet är kedja.

6 Överför serverns SSL-certifikat för säker anslutning till servern.

7 I fältet Kontrollvärdar skriver du in de ytterligare värdnamnen (förutom standardserverns URL) för att verifiera posterna i certifikatet. Använd kommatecken för att skilja flera värdnamn åt.

   Obs! Som standard innehåller den vitlistan bara serverns URL. Skriv in ytterligare värdnamn i fältet Kontrollvärdar för att inkludera dem i vitlistan.

8 Klicka på **Verkställ**.

Konfigurera inställningar för identitetstjänsten

1 Öppna programmets konfigurationssida från den inbyggda webbservern.

2 Vid behov kan du klicka på avsnittet Inställningar för identitetstjänst och välja **Aktivera inaktiv skärm**.

   Obs! Skrivare med eSF version 2.x måste använda programmet eSF Security Manager när **Aktivera inaktiv skärm** är inaktiverat. En lista över sådana skrivare finns i filen *Viktigt*.

3 Skriv värdnamnet eller IP-adressen till identitetstjänstens leverantör.

4 Om det behövs skriver du värdnamnet eller IP-adressen till bricktjänstens leverantör.

5 Överför serverns SSL-certifikat för säker anslutning till servern.

6 Om du har fått ett klient-ID och en hemlig nyckel från identitetstjänstens leverantör skriver du informationen i motsvarande fält.

7 Ställ in åtkomstprinciper för programmet.
   - **Fortsätt** – fortsätt att använda skrivaren även om det inte går att ansluta till identitetstjänstens server.
   - **Fel** – gå tillbaka till inloggningsskärmen om det inte går att ansluta till identitetstjänstens server.

8 Om du vill tillåta att användare loggar in på skrivaren med separata tjänstekonton väljer du **Använd tjänstkontot** och anger sedan kontouppgifter för tjänsten.

9 Klicka på **Verkställ**.

PIN-autentisering

Konfigurera användarautentisering med PIN

Innan du börjar kontrollerar du att åtkomstkontroll för App 2 eller Lösning 2 är inställt på programmets säkerhetsmall. Mer information finns i “Konfigurera åtkomstkontroll” på sidan 6.

1. Öppna programmets konfigurationssida från den inbyggda webbservern.
2. I avsnittet Inloggningsskärm ställer du in Inloggningsmetod på ett alternativ som har stöd för PIN-autentisering.
3. I avsnittet Användarautentisering gör du följande:
   - Ställ in Kortvalidering på önskad autentiseringsmetod.
   - Ställ in åtkomstkontroll för kortregistrering på önskad autentiseringsmetod.
   - Ställ in PIN-åtkomstkontroll på **App 1** eller **Lösning 1**.
   - Ställ in åtkomstkontroll för manuell inloggning på önskad autentiseringsmetod.
   - Ange sessionens åtkomstkontroll som **App 2** eller **Lösning 2**.

   Anmärkningar:

   - Om PIN-åtkomstkontroll är inställt på **Ingen** kan du inte registrera din PIN-kod på skrivaren.
   - Mer information om inställningarna visas om du för pekaren över hjälpen.
4. Klicka på **Verkställ**.

Konfigurera PIN-inställningar

1. Öppna programmets konfigurationssida från Embedded Web Server.
2. På menyn Nödvändiga inloggningsuppgifter i avsnittet PIN-inställningar väljer du en inloggningsmetod.
   - Användar-ID och PIN-kod – Användarnamn och PIN-kod krävs för autentisering.
   - Endast PIN-kod – PIN-kod krävs för autentisering.
3. Ange webbserverns adress och välj sedan minsta PIN-kodslängd.
4. Skriv felmeddelanden för ogiltiga PIN-koder.
5. Klicka på **Verkställ**.

LDAP-autentisering

Använd LDAP-autentisering när användare valideras via en LDAP-server.

Konfigurera LDAP-användarautentisering

Innan du börjar ser du till att:

- Åtkomstkontroll för App 2 eller Lösning 2 är inställt på programmets säkerhetsmall.
- Åtkomstkontroll för App 3 eller Lösning 3 är inställt på en LDAP-säkerhetsmall.

Obs! Mer information finns i “Konfigurera åtkomstkontroll” på sidan 6.

1. Öppna programmets konfigurationssida från den inbyggda webbservern.
2. I avsnittet Inloggningsskärm ställer du in Inloggningsmetod på **Kortinloggning eller manuell inloggning**.
3. I avsnittet Användarautentisering gör du följande:
   - Ställ in Kortvalidering på **LDAP**.
   - Ställ in åtkomstkontroll för kortregistrering på **App 3** eller **Lösning 3**.
   - Ställ in åtkomstkontroll för manuell inloggning på **App 3** eller **Lösning 3**.
   - Ange sessionens åtkomstkontroll som **App 2** eller **Lösning 2**.

   Anmärkningar:

   - Om åtkomstkontroll för kortregistrering är inställt på **Ingen** kan du inte registrera kortet på skrivaren.
   - Om du ställer in åtkomstkontroll för manuell inloggning på **Ingen** krävs bara ett kort för inloggning även om Inloggningsmetod är inställt på **Kortinloggning eller manuell inloggning**.
   - Mer information om inställningarna visas om du för pekaren över hjälpen.
4. Klicka på **Verkställ**.

Konfigurera LDAP-inställningar

1. Öppna programmets konfigurationssida från den inbyggda webbservern.
2. Konfigurera inställningarna i avsnittet LDAP-inställningar.

   Anmärkningar:

   - Om **Använd adressbok** är valt använder programmet LDAP-inställningarna som redan konfigurerats i skrivarnätverkets konton.
   - Mer information om inställningarna visas om du för pekaren över hjälpen.
3. Klicka på **Verkställ**.

Ställa in programinställningar

1. Öppna programmets konfigurationssida från den inbyggda webbservern.
2. Prova något/några av följande alternativ:
   - Konfigurera startskärmens inställningar när du vill anpassa skrivarens startskärm.
   - Om du vill visa registreringsmeddelanden väljer du **Visa inledande registreringsmeddelande** och **Visa meddelande om slutförd registrering** i avsnittet Avancerade inställningar.
   - Om du vill aktivera ett *pipljud* efter en lyckad inloggning väljer du **Aktivera pipljud efter inloggning** i avsnittet Avancerade inställningar och justerar sedan signalens frekvens.
   - Om du vill använda en profil efter inloggningen skriver du ett profilnamn i fältet Inloggningsprofil i avsnittet Avancerade inställningar.

   Obs! Mer information om inställningarna visas om du för pekaren över hjälpen.
3. Klicka på **Verkställ**.

Visa tillgängliga profiler

1 Från den inbäddade webbservern klickar du på **Inställningar** eller **Konfiguration**.

2 Klicka på **Hantera genvägar** > **Hantera profilgenvägar**.

Visar sfärer för användarkonton

Funktionen Använd vald sfär kan bara användas om inloggningsmetoderna för kortregistrering och manuell inloggning är Kerberos, Active Directory eller LDAP+GSSAPI. Den här funktionen kan också användas om kortvalidering är inställt på webbtjänst eller skrivarbaserad.

Om den här funktionen är aktiverad för kortregistrering registreras brick-ID:t i formatet användarnamn@sfär.

Om den här funktionen är aktiverad för manuell inloggning visas användarnamnet på skrivarens kontrollpanel i formatet användarnamn@sfär.

Inställningarna gäller inte inloggning och registrering med PIN.

Så här aktiverar du funktionen:

1 Öppna programmets konfigurationssida från den inbyggda webbservern.

2 I avsnittet Avancerade inställningar väljer du **Använd vald sfär**.

3 Klicka på **Verkställ**.

Exportera eller importera en konfigurationsfil

1 Öppna programmets konfigurationssida från den inbyggda webbservern.

2 Exportera eller importera konfigurationsfilen.

Anmärkningar:

- Om felet **`JVM minnesbrist`** uppstår upprepar du exporten tills konfigureringsfilen har sparats.
- Om en tidsgräns överskrids inträffar och en tom skärmbild visas uppdaterar du webbläsaren och klickar sedan på **Verkställ**.

Hantera programmet

Obs! Programmets statussida är bara tillgänglig när du använder skrivarbaserad autentisering.

Öppna programmets statussida

Använd statussidan när du vill övervaka utskriftsaktiviteterna.

1. Från den inbyggda webbservern klickar du på **Program** > **Kortautentisering**.
2. Lägg märke till följande:
   - **Status** – visar skrivarens aktivitetsstatus.
     - **Inte konfigurerad** – skrivaren har inte konfigurerats.
     - **Offline** – ingen skrivaraktivitet eller kommunikation.
     - **Online** – skrivaren är aktiv.
   - **Drifttid** – visar hur länge programmet har körts.
   - **(denna skrivare)** – den aktuella skrivaren.
   - **Senaste aktivitet** – masterskrivarens senaste aktivitet.
   - **Antal användare** – det totala antalet registrerade användare.
   - **Registreringsstatus** – anger om skrivaren är offline eller online.
   - **Senaste synkroniseringen med master** – när reservskrivaren senast uppdaterades mot masterskrivaren.
   - **Senaste kontakten med master** – när reservskrivaren senast kommunicerade med masterskrivaren.
   - **Senaste synkroniseringen som master** – när reservskrivaren senast fungerade som masterskrivare.
   - **Senaste aktivitet som master** – reservskrivarens senaste aktivitet som masterskrivare.
   - **Varaktighet som master** – hur länge reservskrivaren har fungerat som masterskrivare.
   - **Får för närvarande service av** – klientskrivaren som nyligen haft kontakt med master- eller reservskrivaren.
   - **Senaste aktivitet med reserv** – när klientskrivaren senast hade kontakt med reservskrivaren.

Hantera användarkonton och klientskrivare

Obs! Den här funktionen visas endast om skrivaren är masterskrivare.

1. Öppna programmets statussida från den inbäddade webbservern.
2. Gör något av följande:

Ta bort användarkonton

a. I avsnittet Master klickar du på **Ta bort användare**.

b. Ange ett eller flera användar-ID:n och ta bort dem.

Lägga till klientskrivare

a I avsnittet Klienter klickar du på **Lägg till klienter**.

b Ange en eller flera IP-adresser till skrivare och lägg sedan till dem.

Ta bort klientskrivare

Obs! Du kan inte ta bort klientskrivare när masterskrivaren är offline eller när programmet är avinstallerat.

a Välj en eller flera klientskrivare i avsnittet Klienter.

b Klicka på **Ta bort klienter**.

Tilldela skrivarroller på nytt

1 Konfigurera en ny masterskrivare.

a Öppna programmets konfigurationssida från den inbyggda webbservern på den nya masterskrivaren.

b Ställ in rollen på **Master** i avsnittet Skrivarbaserad kortvalidering.

c Skriv reservskrivarens värdnamn eller IP-adress.

d Klicka på **Verkställ**.

2 Tilldela reservskrivaren till den nya masterskrivaren.

a Öppna programmets konfigurationssida från den inbyggda webbservern på reservskrivaren.

b Skriv värdnamnet eller IP-adressen för den nya masterskrivaren i avsnittet Skrivarbaserad kortvalidering.

c Klicka på **Verkställ**.

3 Ta bort klientskrivaren från den aktuella masterskrivaren.

a Öppna programmets statussida från den inbyggda webbservern på den aktuella masterskrivaren.

b Ta bort klientskrivaren från avsnittet Klienter.

4 Klientskrivaren tilldelas till den nya masterskrivaren. Gör något av följande:

Använda programmets konfigurationssida

a Öppna programmets konfigurationssida från den inbyggda webbservern på klientskrivaren.

b Ställ in rollen på **Klient** i avsnittet Skrivarbaserad kortvalidering.

c Skriv den nya masterskrivarens värdnamn eller IP-adress.

Obs! Kontrollera att reservskrivarens värdnamn eller IP-adress är korrekt.

d Klicka på **Verkställ**.

Använda masterskrivarens statussida

a Öppna programmets statussida från den inbyggda webbservern på den nya masterskrivaren.

b I avsnittet Klienter klickar du på **Lägg till klienter**.

c Ange klientskrivarens IP-adress och lägg sedan till den.

Använda programmet

Registrera användare

1. Håll kortet mot kortläsaren.
2. Ange dina användaruppgifter på skrivarens kontrollpanel.

   Obs! Om du använder Kerberos, Active Directory eller LDAP+GSSAPI för kortregistrering väljer du en sfär.
3. Följ instruktionerna på skärmen.

Registrera en PIN-kod

Innan du börjar kontrollerar du att inloggningsmetoden har stöd för PIN-autentisering.

1. På skrivarens kontrollpanel trycker du på **PIN-inloggning**.
2. Följ instruktionerna på skärmen.

Logga in på skrivaren manuellt

1. Tryck på något av följande på skrivarens kontrollpanel:
   - **PIN-inloggning**
   - **Manuell inloggning**
   - **Administratörsinloggning**

   Obs! När du väljer **Administratörsinloggning** går det inte att hämta annan användarinformation från LDAP-servern.
2. Ange dina inloggningsuppgifter.

   Obs! Om du använder Kerberos, Active Directory® eller LDAP+GSSAPI för manuell inloggning väljer du en sfär.
3. Följ instruktionerna på skärmen.

Felsökning

Programfel

Prova något/några av följande alternativ:

Kontrollera systemloggen

1. Från den inbäddade webbservern klickar du på **Inställningar** eller **Konfiguration**.
2. Beroende på skrivarmodellen gör du något av följande:
   - Klicka på **Program** > **Hantering av program**.
   - Klicka på **Enhetslösningar** > **Lösningar (eSF)**.
   - Klicka på **Inbäddade lösningar**.
3. Klicka på **System** > **Logg**.
4. Välj och skicka lämpliga filter.
5. Analysera loggen och lös sedan problemet.

Kontakta Lexmarkrepresentanten

Programmet kan inte köras med den uppdaterade versionen av SaaS Print Release

Prova något/några av följande alternativ:

Se till att Print Release är rätt konfigurerat

Om du har uppgraderat Print Management SaaS-programmet till Print Release v2.0 eller senare ser du till att Bakgrund och Inaktiv skärm är avaktiverat. Tilldela åtkomstkontroll med kortautentisering till Print Release och kontrollera sedan att Print Release är rätt konfigurerat. Mer information finns i *administratörshandboken för Print Release*.

Kontakta Lexmarkrepresentanten

Autentiseringsfel

Prova något/några av följande alternativ:

Öka tidsgränsen för skrivaren

Om du använder en identitetstjänst som kortvalideringsmetod kan det hända att skrivaren behöver mer tid att kommunicera med identitetstjänsteleverantören.

1. Från den inbäddade webbservern klickar du på **Inställningar** eller **Konfiguration**.
2. Klicka på **Allmänna inställningar** > **Tidsgränser**.
3. Öka tidsgränsen för skärm och viloläge.
4. Klicka på **Skicka**.

Kontrollera att skrivaren är ansluten till nätverket

Mer information finns i skrivarens *Användarhandbok*.

Kontrollera att säkerhetsservern är online och att den inte är upptagen

Om du vill ha mer information kan du kontakta systemadministratören.

Användare utelåst

Användaren kan ha uppnått tillåtet antal inloggningsförsök.

Öka utelåsningstiden och antalet tillåtna inloggningsförsök

1. Beroende på skrivarmodell gör du något av följande via den inbyggda webbservern:
   - Klicka på **Inställningar** > **Säkerhet** > **Övriga säkerhetsinställningar** > **Inloggningsbegränsningar**.
   - Klicka på **Konfiguration** > **Säkerhet**.
2. Öka utelåsningstiden och antalet tillåtna inloggningsförsök eller fördröjningen för automatisk utloggning.
3. Klicka på **Skicka**.

Det går inte att registrera en klientskrivare

Prova något/några av följande alternativ:

Se till att masterskrivaren eller reservskrivaren är online

Mer information finns i “Öppna programmets statussida” på sidan 15.

Se till att masterskrivaren och reservskrivaren är korrekt konfigurerade

Mer information finns i “Konfigurera skrivarbaserad användarautentisering” på sidan 8.

Kontrollera att det inte finns fler än 23 registrerade klientskrivare

Mer information finns i “Hantera användarkonton och klientskrivare” på sidan 15.

Kontakta Lexmarkrepresentanten

Det går inte att validera kortet

Prova något/några av följande alternativ:

Ställ in Inloggningsmetod på Kort eller Manuell inloggning

1. Öppna programmets konfigurationssida från den inbyggda webbservern.
2. I avsnittet Inloggningsskärm ställer du in Inloggningsmetod på **Kortinloggning eller manuell inloggning**.
3. Klicka på **Verkställ**.

Kontakta Lexmarkrepresentanten

Ingen sfärinformation hittades

Prova något/några av följande alternativ:

Du behöver inte välja sfär för vissa inloggningsmetoder för manuell inloggning eller kortregistrering, t.ex. lokala konton eller LDAP. För inloggningsmetoderna Kerberos, Active Directory och LDAP+GSSAPI måste du välja sfär.

Avaktivera val av sfär

1. Öppna programmets konfigurationssida från den inbyggda webbservern.
2. I avsnittet Avancerade inställningar rensar du **Använd vald sfär**.
3. Klicka på **Verkställ**.

Ändra inloggningsmetod

1. Öppna programmets konfigurationssida från den inbyggda webbservern.
2. I avsnittet Användarautentisering ställer du in åtkomstkontroll för kortregistrering och manuell inloggning på **App 1** eller **Lösning 1**.
3. Klicka på **Verkställ**.

Kontakta Lexmarkrepresentanten

Det går inte att ansluta till LDAP-servern

Prova något/några av följande alternativ:

Kontrollera att LDAP-inställningarna är konfigurerade på rätt sätt

Mer information finns i “Konfigurera LDAP-inställningar” på sidan 13.

Kontakta Lexmarkrepresentanten

Vanliga frågor

Varför kan jag inte lägga till eller ta bort en klientskrivare när en reservskrivare fungerar som master?

Du kan endast ta bort eller lägga till en klientskrivare när masterskrivaren är online.

Kan jag ta bort en klientskrivare och tilldela den till en ny masterskrivare även om den aktuella masterskrivaren är offline?

Ja. Gör följande:

1. Installera om programmet från Embedded Web Server på klientskrivaren.
2. Ange rollen som klientskrivare och konfigurera den med de nya master- och reservskrivarna. Mer information finns i “Konfigurera skrivarens roll” på sidan 9.

Vad händer om jag av misstag har avinstallerat programmet i skrivaren?

1. Installera om programmet från Embedded Web Server.
2. Ange skrivarens roll. Mer information finns i “Konfigurera skrivarens roll” på sidan 9.

   Obs! Kom ihåg att konfigurera masterskrivaren, reservskrivaren och klientskrivarna i den ordningen.
3. Konfigurera skrivaren beroende på dess roll.

   Anmärkningar:

   - Om programmet installeras om på masterskrivaren tilldelar du den sedan till reservskrivaren.
   - Om programmet installeras om på en reservskrivare tilldelar du den sedan till masterskrivaren.
   - Om programmet installeras om på en klientskrivare tilldelar du den sedan till masterskrivaren och reservskrivaren.
   - Mer information finns i “Tilldela skrivarroller på nytt” på sidan 16.

Varför kan jag inte se kopierings- eller faxknappen på låsskärmen utan att logga in även om jag aktiverat funktionen?

Ställ in åtkomstkontrollen för kopierings- eller faxfunktionen på **Ingen säkerhet**. Mer information finns i “Konfigurera inloggningsskärmen” på sidan 7.

Vad händer om jag använder samma åtkomstkontroller för manuell inloggning och sessioner?

För att komma åt skrivarfunktionerna på startskärmen måste du ange dina inloggningsuppgifter när du loggar in manuellt.

Kan jag ha olika åtkomstkontroller för manuell Inloggning och kortvalidering?

Ja, utom när du använder autentisering med Identitetstjänst, då ska du ställa in Åtkomstkontroll för manuell inloggning och Kortvalidering på **Identitetstjänst**.

Varför fungerar inte funktionen Administratörsinloggning med nätverkskonton?

Funktionen **Administratörsinloggning** gäller endast för säkerhetsmallar för Interna konton, PIN-kod, och Lösenord.

Information

Om utgåvan

December 2020

Följande stycke gäller inte i de länder där sådana föreskrifter står i strid med gällande lag. LEXMARK INTERNATIONAL, INC., LEVERERAR DENNA SKRIFT I BEFINTLIGT SKICK, UTAN NÅGON SOM HELST GARANTI, VARE SIG UTTRYCKLIG ELLER UNDERFÖRSTÅDD, INKLUSIVE, MEN EJ BEGRÄNSAT TILL, UNDERFÖRSTÅDDA GARANTIER GÄLLANDE SÄLJBARHET ELLER LÄMPLIGHET FÖR ETT VISST SYFTE. Vissa stater tillåter inte friskrivningar från explicita eller implicita garantier vid vissa transaktioner, och därför är det möjligt att uttalandet ovan inte gäller just dig.

Denna skrift kan innehålla tekniska felaktigheter eller tryckfel. Innehållet är föremål för periodiska ändringar, sådana förändringar införlivas i senare utgåvor. Förbättringar eller förändringar av de produkter eller programvaror som beskrivs kan när som helst ske.

Hänvisningar till produkter, program och tjänster i det här dokumentet innebär inte att tillverkaren avser att göra dessa tillgängliga i alla länder. Hänvisningar till olika produkter, program eller tjänster innebär inte att endast dessa produkter, program eller tjänster kan användas. Andra produkter, program eller tjänster med likvärdiga funktioner där ingen konflikt föreligger vad gäller upphovsrätt kan användas istället. Det är upp till användaren att utvärdera och kontrollera funktionen i samverkan med produkter, program eller tjänster andra än de som uttryckligen anges av tillverkaren.

Teknisk support från Lexmark finns på **http://support.lexmark.com**.

Om du vill ha information om Lexmarks sekretesspolicy som reglerar användning av denna produkt, gå till **www.lexmark.com/privacy**.

Mer information om förbrukningsmaterial och nedladdningar finns på **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.

Varumärken

Lexmark och Lexmarks logotyp är varumärken eller registrerade varumärken som tillhör Lexmark International, Inc. i USA och/eller andra länder.

Alla andra varumärken tillhör sina respektive ägare.

Index

R

S

T

V

W

Å

Ö