EPSON
EXCEED YOUR VISION

DS-790WN

Administratörshandbok

NPD6726-00 SV

Upphovsrätt

Varumärken

- ❏ EPSON, EPSON EXCEED YOUR VISION, EXCEED YOUR VISION och deras logotyper är registrerade varumärken eller varumärken tillhörande Seiko Epson.
- ❏ Microsoft®, Windows®, and Windows Server® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- ❏ Chrome is a trademark of Google LLC.
- ❏ The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- ❏ Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- ❏ FeliCa och PaSoRi är registrerae varumärken som tillhör Sony Corporation.
- ❏ MIFARE är ett registrerat varumärke som tillhör NXP Semiconductor Corporation.
- ❏ Allmänt: andra produktnamn som förekommer i detta dokument används endast i identifieringssyfte och kan vara varumärken som tillhör respektive ägare. Epson frånsäger sig all rätt till dessa varumärken.

Innehållsförteckning

Upphovsrätt

Varumärken

Introduktion

Rekommenderade inställningar som passar för ditt ändamål

Nätverksinställningar

Mjukvara för att konfigurera skannern

Inställningar som krävs för skanning

Anpassa kontrollpanelens skärm

Grundläggande säkerhetsinställningar

Avancerade säkerhetsinställningar

Autentiseringsinställningar

Underhåll

Introduktion

Innehållet i detta dokument

Detta dokument erbjuder följande information för skanneradministratörer.

❏ Nätverksinställningar

❏ Förbereda skanningfunktionen

❏ Aktivera och hantera säkerhetsinställningar

❏ Aktivera och hantera Autentiseringsinställningar

❏ Utföra dagligt underhåll

För standardmetoder vid användning av skanner, se *Användarhandbok*.

Anmärkning:
Detta dokument förklarar Autentiseringsinställningar som erbjuder fristående autentisering utan att behöva använda autentiseringsservern. Utöver Autentiseringsinställningar som introducerats i denna bruksanvisning kan du även skapa ett autentiseringssystem med en autentiseringsserver. För att skapa ett system, använd Document Capture Pro Server Authentication Edition (det förkortade namnet är Document Capture Pro Server AE).

Kontakta ditt lokala Epson-kontor för mer information.

Använda denna handbok

Märken och symboler

> ***Obs!***
> *Instruktioner som måste följas noggrant för att undvika kroppsskada.*

> ***Viktigt:***
> *Instruktioner som måste följas för att undvika skada på utrustningen.*

Anmärkning:
Erbjuder kompletterande information och referensinformation.

Relaterad information

➡ Länkar till relaterade avsnitt.

Beskrivningar som används i denna användarhandbok

❏ Skärmbilderna för programmen är från Windows 10 eller macOS High Sierra. Innehållet som visas på skärmarna varierar beroende på modell och situation.

❏ Illustrationerna som används i denna användarhandbok är endast för referens. Även om de kan skilja sig något från den faktiska produkten är användningsmetoderna likadana.

Operativsystemsreferenser

Windows

I den här användarhandboken syftar termer som ”Windows 10”, ”Windows 8.1”, ”Windows 8”, ”Windows 7”, ”Windows Server 2019”, ”Windows Server 2016”, ”Windows Server 2012 R2”, ”Windows Server 2012”, och ”Windows Server 2008 R2” på följande operativsystem. Dessutom används ”Windows” för att hänvisa till alla versioner och ”Windows Server” används för att hänvisa till ”Windows Server 2019”, ”Windows Server 2016”, ”Windows Server 2012 R2”, ”Windows Server 2012”, och ”Windows Server 2008 R2”.

- ❏ Microsoft® Windows® 10 operativsystem
- ❏ Microsoft® Windows® 8.1 operativsystem
- ❏ Microsoft® Windows® 8 operativsystem
- ❏ Microsoft® Windows® 7 operativsystem
- ❏ Microsoft® Windows Server® 2019 operativsystem
- ❏ Microsoft® Windows Server® 2016 operativsystem
- ❏ Microsoft® Windows Server® 2012 R2 operativsystem
- ❏ Microsoft® Windows Server® 2012 operativsystem
- ❏ Microsoft® Windows Server® 2008 R2 operativsystem

Mac OS

I den här bruksanvisningen används ”Mac OS” för att hänvisa till macOS Big Sur, macOS Catalina, macOS Mojave, macOS High Sierra, macOS Sierra, OS X El Capitan, och OS X Yosemite.

Rekommenderade inställningar som passar för ditt ändamål

Rekommenderade inställningar som passar för ditt ändamål

Se nedan för att skapa nödvändiga inställningar som passar dina syften.

Ansluta skannern till nätverket

Syfte	Obligatoriska inställningar
Jag vill ansluta skannern till nätverket.	Ställ in din skanner för nätverksskanning. "Ansluta skannern till nätverket" på sidan 13
Jag vill ansluta skannern till en ny dator.	Konfigurera nätverksinnställningar för din skanner på den nya datorn. "Lägga till eller ersätta datorn eller enheter" på sidan 19

Inställningar för skanning

Syfte	Obligatoriska inställningar
Jag vill skicka skannade bilder via e-post. (Skanna till e-post)	1. Konfigurera e-spotservern jag vill länka till. "Konfigurera en e-postserver" på sidan 40 2. Registrera mottagarens e-postadress i **Kontakter** (valfritt). Genom att registrera e-postadressen behöver du inte öppna den varje gång du vill skicka något, utan du kan välja den från dina Kontakter. "Göra kontakter tillgängliga" på sidan 59
Jag vill spara bilder till en mapp i nätverket. (Skanna till nätverksmapp/FTP)	1. Skapa en mapp i nätverket är du vill spara bilderna. "Ställ in en delad nätverksmapp" på sidan 43 2. Registrera sökvägen till mappen i **Kontakter** (tillval). Genom att registrera mappsökvägen behöver du inte öppna den varje gång du vill skicka något, utan du kan välja den från dina Kontakter. "Göra kontakter tillgängliga" på sidan 59
Jag vill spara skannade bilder till en molntjänst. (Skanna till moln)	Konfigurera Epson Connect. Se Epson Connect-portalens webbplats för information om konfiguration. Vid konfiguration behöver du ett användarkonto för online-lagringstjänsten du vill länka till. https://www.epsonconnect.com/ http://www.epsonconnect.eu (Endast Europa)

Anpassa kontrollpanelens skärm

Syfte	Obligatoriska inställningar
Jag vill ändra objekten som visas på skannerns kontrollpanel.	Ställ in **Förinställ.** eller **Redigera Hem**. Du kan registrera dina favoritskanninginställningar för kontrollpanelen och redigera visade objekt. "Anpassa kontrollpanelens skärm" på sidan 72

Konfigurera grundläggande säkerhetsfunktioner

Syfte	Obligatoriska inställningar
Jag vill förhindra att administratören ändrar skannerinställningarna.	Konfigurera ett administratörslösenord för skannern. "Administratörsinställningar" på sidan 81
Jag vill inaktivera användning av skannrar med USB-anslutningar.	Inaktivera externt gränssnitt. "Inaktivera externt gränssnitt" på sidan 87

Konfigurera avancerade säkerhetsfunktioner

Syfte	Obligatoriska inställningar
Jag vill kontrollera vilka protokoll som ska användas.	Aktivera eller inaktivera protokollen. "Kontrollera med protokoll" på sidan 92
Jag vill kryptera kommunikationssökvägen.	1. Konfigurera ditt digitala certifikat. "Använda ett digitalt certifikat" på sidan 95 2. Konfigurera SSL/TLS-kommunikation. "SSL-/TLS-kommunikation med skannern" på sidan 100
Jag vill använda kypterad kommunikation (IPsec). Jag vill kunna använda programvaran endast från en specifik dator (IP-filtrering).	Konfigurera policier för trafikfiltrering. "Krypterad kommunikation med IPsec/IP-filtrering" på sidan 102
Jag vill använda en skanner i ett IEEE802.1X nätverk.	Installera IEEE802.1X för skannern. "Ansluta skannern till ett IEEE802.1X-nätverk" på sidan 112

Ställa in funktioner som ska autentiseras av skannern

Syfte	Obligatoriska inställningar
Jag vill aktivera Autentiseringsinställningar.	Se följande för mer information om tillgängliga Autentiseringsinställningar och Autentiseringsmetod. "Om Autentiseringsinställningar" på sidan 122 "Om Autentiseringsmetod" på sidan 123

Använda en servers autentiseringssystem

Med Document Capture Pro Server Authentication Edition (förkortad till Document Capture Pro Server AE), kan du skapa ett autentiseringssystem som använder en server för autentsering.

Kontakta ditt lokala Epson-kontor för mer information.

Nätverksinställningar

Ansluta skannern till nätverket

I detta avsnitt förklaras hur du ansluter skannern till nätverket med hjälp av skannerns kontrollpanel.

Anmärkning:
Om din skanner och dator är i samma segment kan du även ansluta med installationsprogrammet.

❏ *Installera från webbplatsen*

Öppna följande webbplats och ange sedan produktnamnet. Gå till ***Inställning*** *och starta konfigurationen.*

http://epson.sn

❏ *Konfigurera med mjukvaruskivan (endast för modeller som levereras med en mjukvaruskiva och användare med Windows-datorer med skivenheter).*

Mata in programskivan i datorn och följ instruktionerna på skärmen.

Innan du skapar en nätverksanslutning

För att ansluta till nätverket ska du kontrollera anslutningsmetoden och inställningsinformationen för anslutningen först.

Samla information i anslutningsinställningarna

Förbered nödvändig inställningsinformation för anslutning. Kontrollera följande information i förväg.

Avdelningar	Alternativ	Anmärkning
Enhetsanslutningsmetod	❏ Ethernet ❏ Wi-Fi	Bestäm hur du ansluter skannern till nätverket. För kabelförsett nätverk ansluter du till brytaren för det lokala nätverket. För Wi-Fi ansluter du till nätverket (SSID) för åtkomstpunkten.
LAN-anslutningsinformation	❏ IP-adress ❏ Nätmask ❏ Standard-gateway	Fastställ IP-adressen för att tilldela den till skannern. När du tilldelar IP-adressen statiskt krävs alla värden. När du tilldelar IP-adressen dynamiskt med DHCP-funktionen krävs inte den här informationen, eftersom den konfigureras automatiskt.
Wi-Fi-anslutningsinformation	❏ SSID ❏ Lösenord	Det finns SSID (nätverksnamn) och lösenord för åtkomstpunkten som skannern ansluter till. Om MAC-adressfiltrering har konfigurerats registrerar du MAC-adressen för skannern i förväg för att registrera skannern. Se följande för de standarder som stöds. "Nätverksspecifikationer" på sidan 26
DNS-serverinformation	❏ IP-adress för primär DNS ❏ IP-adress för sekundär DNS	Dessa krävs när du anger DNS-servrar. Sekundär DNS konfigureras när systemet har en redundant konfiguration och det finns en sekundär DNS-server. Om du är i en liten organisation och inte konfigurerar DNS-servern ska du konfigurera IP-adressen för routern.

Avdelningar	Alternativ	Anmärkning
Proxy-serverinformation	❏ Proxy-servernamn	Konfigurera detta när din nätverksmiljö använder proxyservern för åtkomst till Internet från intranätet och använd funktionen som skannern direkt kommer åt på Internet. För följande funktioner ansluter skannern direkt till Internet. ❏ Epson Connect-tjänster ❏ Molntjänster för andra företag ❏ Firmware-uppdatering ❏ Skicka skannade bilder till SharePoint (WebDAV)
Portnummerinformation	❏ Portnummer för aktivering	Kontrollera portnumret som används av skannern och datorn och aktivera porten som är blockerad av en brandvägg om det behövs. Se följande för vilket portnummer skannern använder. "Använda port för skannern" på sidan 29

IP-adresstilldelning

Följande typer av IP-adresstilldelning finns.

Statisk IP-adress:

Tilldela förutbestämd IP-adress (värd) för skannern manuellt.

Informationen för anslutning till nätverket (nätmask, standardgateway, DNS-server etc.) behöver konfigureras manuellt.

IP-adressen ändras inte även om enheten stängs av, vilket är praktiskt när du vill hantera enheter i en miljö där du inte kan ändra IP-adressen eller du vill hantera enheter med IP-adressen. Vi rekommenderar inställningar för skanner, server etc. som många datorer kan få åtkomst till. Vid användning av säkerhetsfunktioner, såsom IPsec-/IP-filtrering, tilldelar du en fast IP-adress så att IP-adressen inte ändras.

Automatisk tilldelning genom användning av DHCP-funktionen (dynamisk IP-adress):

Tilldela IP-adressen automatiskt till skannern (värden) genom att använda DHCP-funktionen på DHCP-servern eller routern.

Informationen för anslutning till nätverket (nätmask, standardgateway, DNS-server etc.) konfigureras automatiskt, så att du enkelt kan ansluta enheten till nätverket.

Om enheten eller routern stängs av, eller beroende på DHCP-serverinställningar, kan IP-adressen ändras vid återanslutning.

Vi rekommenderar hantering av andra enheter än IP-adressen och kommunikation med protokoll som kan följa IP-adressen.

Anmärkning:
När du använder IP-adressreservationsfunktionen för DHCP, kan du tilldela samma IP-adress till enheterna när som helst.

DNS-server och Proxy-server

DNS-servern har ett värdnamn, domännamn för e-postadress etc. kombinerat med IP-adressinformationen.

Kommunikation är omöjlig om den andra parten beskrivs med värdnamn, domännamn etc. när datorn eller skannern utför IP-kommunikationen.

Söker DNS-servern avseende informationen och hämtar IP-adressen till den andra parten. Den här processen kallas namnupplösning.

Därför kan enheter, såsom datorer och skannrar, kommunicera med IP-adressen.

Namnupplösningen är nödvändig för att skannern ska kommunicera med e-postfunktion eller Internet-anslutningsfunktion.

När du använder dessa funktioner ska du skapa DNS-serverinställningar.

När du tilldelar skannerns IP-adress genom att använda DHCP-funktionen på DHCP-servern eller routern konfigureras den automatiskt.

Proxyservern placeras i gatewayen mellan nätverket och Internet och kommunicerar med datorn, skannern och Internet (motsatt server) för var och en av dem. Motsatt server kommunicerar endast med proxyservern. Därför kan skannerinformation, såsom IP-adress och portnummer inte läsas och en ökad säkerhet förväntas.

När du ansluter till Internet via en proxyserver, konfigurerar du proxyservern på skannern.

Ansluta till nätverket via kontrollpanelen

Anslut skanner till nätverket via skannerns kontrollpanel.

Tilldela IP-adress

Konfigurera de grundläggande objekten som värdadress, Subnetmask, Standardgateway.

I det här avsnittet beskrivs proceduren för konfiguration av en statisk IP-adress.

1. Starta skannern.

2. Välj **Inst.** på startskärmen på skannerns kontrollpanel.

3. Välj **Nätverksinställningar** > **Avancerat** > **TCP/IP**.

4. Välj **Manuell** för **Erhåll IP-adress**.

   När du konfigurerar IP-adressen automatiskt genom att använda DHCP-funktionen för routern, väljer du **Auto**. I så fall ställs **IP-adress**, **Subnetmask** och **Standardgateway** i steg 5 till 6 in automatiskt, så gå vidare till steg 7.

5. Ange IP-adressen.

   Fokus flyttar till nästkommande segment eller bakomvarande segment separerat av en punkt om du väljer ◀ och ▶.

   Kontrollera värdet som visas på föregående skärm.

6. Konfigurera **Subnetmask** och **Standardgateway**.

   Kontrollera värdet som visas på föregående skärm.

> ***Viktigt:***
>
> *Om kombinationen av IP-adress, Subnetmask och Standardgateway är felaktiga, är **Börja konfiguration** inaktiv och kan inte fortsätta med inställningarna. Kontrollera att det inte finns något fel i inmatningen.*

7. Ange DNS-serverns IP-adress.

   Kontrollera värdet som visas på föregående skärm.

   Anmärkning:
   *När du väljer **Auto** för IP-adresstilldelningsinställningar kan du välja DNS-serverinställningar från **Manuell** eller **Auto**. Om du inte kan erhålla DNS-serveradressen automatiskt ska du välja **Manuell** och ange DNS-serveradressen. Ange sedan den sekundära DNS-serveradressen direkt. Om du väljer **Auto** går du till steg 9.*

8. Ange IP-adressen för den sekundära DNS-servern.

   Kontrollera värdet som visas på föregående skärm.

9. Tryck på **Börja konfiguration**.

Inställning av proxyserver

Konfigurera proxyservern om båda följande alternativen stämmer.

❏ Proxyservern är integrerad för Internet-anslutning.

❏ Vid användning av en funktion där skannern ansluter direkt till Internet, såsom Epson Connect-tjänst eller ett annat företags molntjänster.

1. Välj **Inst.** på startskärmen.

   Gör nödvändiga inställningar efter IP-adresskonfiguration så visas skärmen **Avancerat**. Gå till steg 3.

2. Välj **Nätverksinställningar** > **Avancerat**.

3. Välj **Proxy-server**.

4. Välj **Anvnd.** för **Proxy-serverinst.**.

5. Ange adressen för proxy-servern i IPv4- eller FQDN-format.

   Kontrollera värdet som visas på föregående skärm.

6. Ange portnumret för proxy-servern.

   Kontrollera värdet som visas på föregående skärm.

7. Tryck på **Börja konfiguration**.

Ansluta till Ethernet

Anslut skannern till nätverket med LAN-kabeln och kontrollera anslutningen.

1. Anslut skannern och hubben (LAN-brytare) med LAN-kabeln.

2. Välj  på startskärmen.

3. Välj **Router**.

4. Se till att inställningarna för Anslutning och IP-adress är korrekta.

5. Tryck på **Stäng**.

Ansluta till trådlöst nätverk

Du kan ansluta skannern till trådlöst LAN (Wi-Fi) på flera sätt. Välj den anslutningsmetod som matchar miljön och villkoren som du har.

Om du känner till informationen för den trådlösa routern, såsom SSID och lösenord, kan du göra inställningarna manuellt.

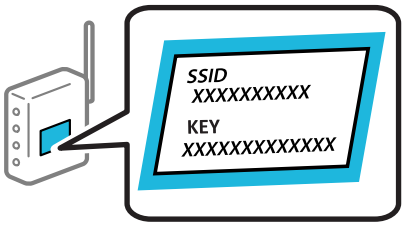
Om den trådlösa routern stöder WPS kan du göra inställningarna genom att använda tryckknappskonfigurationen.

Efter att du anslutit skannern till nätverket ansluter du till skannern från enheten som du vill använda (dator, smartenhet, surfplatta och så vidare.)

Konfigurera Wi-Fi genom att ange SSID och lösenord

Du kan konfigurera ett Wi-Fi-nätverk genom att ange den information som behövs för att ansluta till en trådlös router från skannerns kontrollpanel. För att kunna konfigurera på det här sättet behöver du SSID och lösenordet till den trådlösa routern.

Anmärkning:
Om du använder en trådlös router med standardinställningarna anges SSID och lösenord på dess dekal. Kontakta personen som konfigurerade den trådlösa routern eller läs dokumentationen som medföljde den trådlösa routern om du inte vet SSID eller lösenordet.



1. Tryck på  på startskärmen.

2. Välj **Router**.

3. Tryck på **Gör inställningar**.

   Om nätverksanslutnignen redan konfigurerats visas anslutningsdetaljerna. Tryck på **Ändra till Wi-Fi-anslutning.** eller **Ändra inställningar** för att ändra inställningarna.

4. Välj **Wi-Fi guide till inställningar**.

5. Följ instruktionerna på skärmen för att välja SSID, ange lösenordet för den trådlösa routern och starta installationen.

   Om du vill kontrollera statusen på skannerns nätverksanslutning efter att installationen är klar, se den relaterade informationslänken nedan för mer information.

Anmärkning:

❏ *Om du inte känner till SSID kan du se efter om det anges på den trådlösa routerns dekal. Om du använder den trådlösa routern med standardinställningarna ska du använda det SSID som anges på dekalen. Om du inte hittar någon information kan du granska dokumentationen som medföljde den trådlösa routern.*

❏ *Lösenordet är skiftlägeskänsligt.*

❏ *Om du inte känner till lösenordet kan du se efter om det anges på den trådlösa routerns dekal. Lösenordet kan anges som "Network Key", "Wireless Password" o.s.v. på dekalen. Om du använder den trådlösa routern med standardinställningarna ska du använda det lösenordet som anges på dekalen.*

Relaterad information

➡ "Kontrollera nätverksanslutningens status" på sidan 25

Göra Wi-Fi-inställningarna genom tryckknappskonfiguration (WPS)

Du kan automatiskt ställa in ett Wi-Fi-nätverk genom att trycka på en knapp på den trådlösa routern. Om följande villkor uppfylls kan du konfigurera genom att använda den här metoden.

❏ Den trådlösa routern är kompatibel med WPS (Wi-Fi Protected Setup).

❏ Den befintliga Wi-Fi-anslutningen upprättades med en knapptryckning på den trådlösa routern.

Anmärkning:
Se dokumentationen som medföljde den trådlösa routern om du inte kan hitta knappen eller om du vill konfigurera den.

1. Tryck på  på startskärmen.

2. Välj **Router**.

3. Tryck på **Gör inställningar**.

   Om nätverksanslutnignen redan konfigurerats visas anslutningsdetaljerna. Tryck på **Ändra till Wi-Fi-anslutning.** eller **Ändra inställningar** för att ändra inställningarna.

4. Välj **Tryckknappsinst(WPS)**.

5. Följ instruktionerna på skärmen.

   Om du vill kontrollera statusen på skannerns nätverksanslutning efter att installationen är klar, se den relaterade informationslänken nedan för mer information.

   Anmärkning:
   Om det inte går att ansluta, startar du om den trådlösa routern, flyttar den närmare skannern och försöker igen.

Relaterad information

➡ "Kontrollera nätverksanslutningens status" på sidan 25

Göra Wi-Fi-inställningarna genom PIN-kodskonfiguration (WPS)

Du kan ansluta automatiskt till en trådlös router med en PIN-kod. Du kan använda den här inställningsmetoden när den trådlösa routern har stöd för WPS (Wi-Fi Protected Setup). Ange en PIN-kod på den trådlösa routern via en dator.

1. Tryck på  på startskärmen.
2. Välj **Router**.
3. Tryck på **Gör inställningar**.

   Om nätverksanslutnignen redan konfigurerats visas anslutningsdetaljerna. Tryck på **Ändra till Wi-Fi-anslutning.** eller **Ändra inställningar** för att ändra inställningarna.
4. Välj **Övriga** > **PIN-kodsinst. (WPS)**
5. Följ instruktionerna på skärmen.

   Om du vill kontrollera statusen på skannerns nätverksanslutning efter att installationen är klar, se den relaterade informationslänken nedan för mer information.

   Anmärkning:
   Mer information om hur du anger en PIN-kod finns i dokumentationen som medföljde den trådlösa routern.

Relaterad information

➡ ”Kontrollera nätverksanslutningens status” på sidan 25

Lägga till eller ersätta datorn eller enheter

Ansluta till en skanner som har anslutits till nätverket

När skannern redan är ansluten till nätverken kan du ansluta en dator eller en smartenhet till skannern via nätverket.

Använda en nätverksskanner från en andra en dator

Vi rekommenderar att du använder installationsverktyget för att ansluta skannern till en dator. Du kan köra installationsprogrammet på ett av följande sätt.

❏ Installera från webbplatsen

Öppna följande webbplats och ange sedan produktnamnet. Gå till **Inställning** och starta konfigurationen.

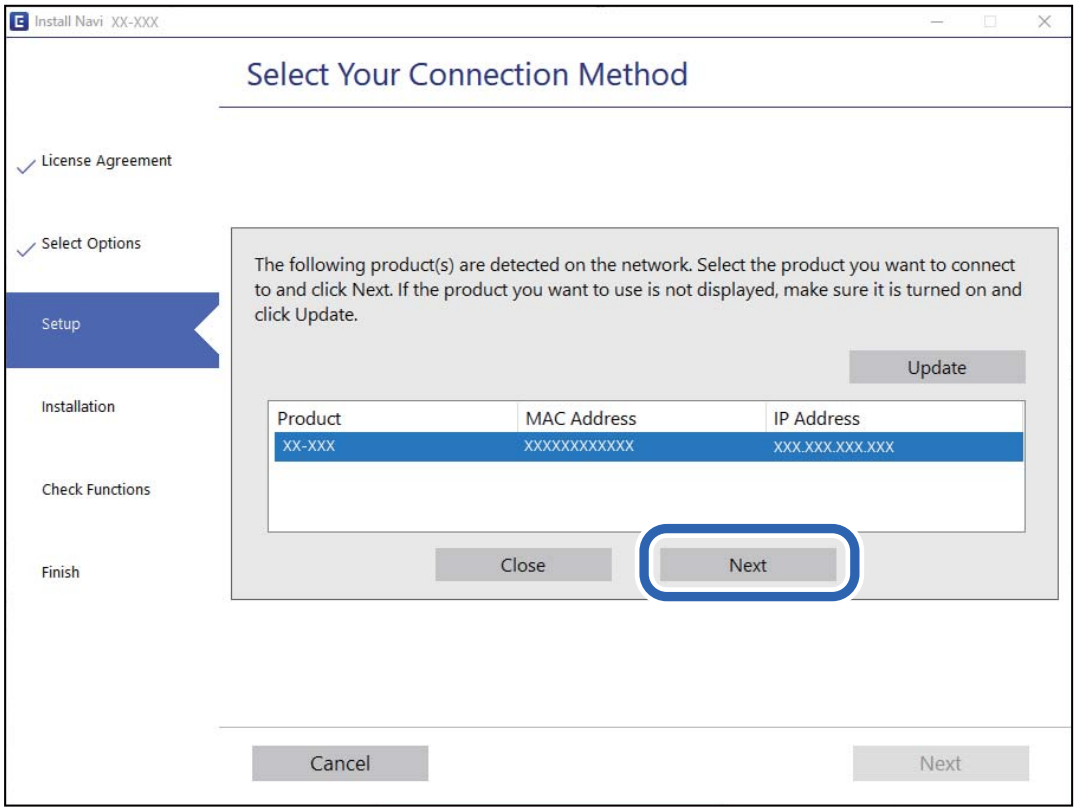
http://epson.sn

❏ Konfigurera med mjukvaruskivan (endast för modeller som levereras med en mjukvaruskiva och användare med Windows-datorer med skivenheter).

Mata in programskivan i datorn och följ instruktionerna på skärmen.

Val av skanner

Följ instruktionerna på skärmen tills följande skärm visas, välj namnet på den skanner som du vill ansluta till och klicka sedan på **Nästa**.



Följ instruktionerna på skärmen.

Använda en nätverksskanner från en smartenhet

Du kan ansluta en smartenhet till skannern med en av metoderna nedan.

Ansluta via en trådlös router

Anslut smartenheten till samma Wi-Fi-nätverk (SSID) som skannern.

Se följande för mer information.

”Göra inställningar för anslutning till smartenheten” på sidan 24

Ansluta med Wi-Fi Direct

Anslut smartenheten direkt till skannern utan en trådlös router.

Se följande för mer information.

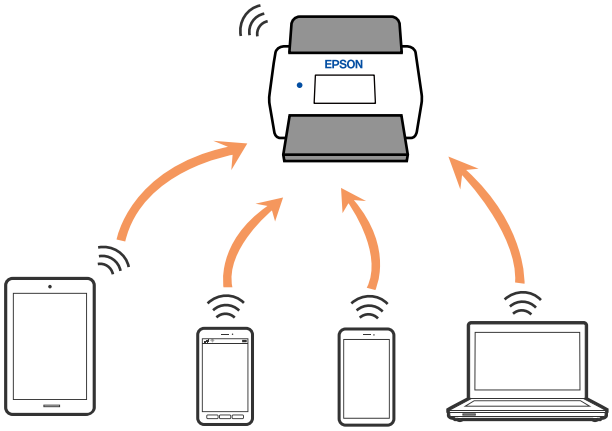
”Ansluta en smartenhet och skanner direkt (Wi-Fi Direct)” på sidan 21

Ansluta en smartenhet och skanner direkt (Wi-Fi Direct)

Wi-Fi Direct (enkel AP) låter dig ansluta en smartenhet direkt till skannern utan en trådlös router och skanna från den smarta enheten.

Om Wi-Fi Direct

Använd den här anslutningsmetoden när du inte använder Wi-Fi i hemmet, på kontoret eller när du vill ansluta skannern och datorn eller den smarta enheten direkt. I det här läget fungerar skannern som en trådlös router och du kan ansluta enheterna till skannern utan att behöva använda en standard trådlös router. Enheterna som ansluts dock korrekt till skannern kan dock inte kommunicera med varandra genom skannern.



Skannern kan anslutas med Wi-Fi eller Ethernet och Wi-Fi Direct (enkel AP)-anslutning samtidigt. Om du däremot startar en nätverksanslutning i Wi-Fi Direct (enkel AP)-anslutning när skannern är ansluten med Wi-Fi blir Wi-Fi tillfälligt frånkopplad.

Ansluta till en smartenhet med Wi-Fi Direct

Denna metod låter dig ansluta skannern direkt till smarta enheter utan en trådlös router.

1. Välj  på startskärmen.
2. Välj **Wi-Fi Direct**.
3. Välj **Gör inställningar**.
4. Starta Epson Smart Panel på din smartenhet.
5. Följ anvisningarna på Epson Smart Panel för att ansluta till din skanner.

   När din smarta enhet är ansluten till skannern går du till nästa steg.
6. Välj **Slutförd** på skannerns kontrollpanel.

Koppla bort Wi-Fi Direct-anslutning (enkel AP)

Det finns två metoder för att inaktivera en Wi-Fi Direct (enkel AP)-anslutning. Du kan inaktivera alla anslutningar från skannerns kontrollpanel, eller inaktivera alla anslutningar från datorn eller smarta enheten.

När du vill inaktivera alla anslutningar väljer du  > **Wi-Fi Direct** > **Gör inställningar** > **Ändra** > **Avaktivera Wi-Fi Direct**.

> ***Viktigt:***
> *Om Wi-Fi Direct (enkel AP)-anslutning är inaktiverad, är alla datorer och smartenheter som är anslutna till skannern med Wi-Fi Direct (enkel AP)-anslutning frånkopplade.*

Anmärkning:
Om du vill koppla bort en viss enhet ska du koppla bort från den enheten i stället för från skannern. Använd en av de följande metoderna för att inaktivera Wi-Fi Direct (enkel AP)-anslutningen från enheten.

❏ *Inaktivera Wi-Fi-anslutningen till skannerns nätverksnamn (SSID).*

❏ *Anslut till ett annat nätverksnamn (SSID).*

Ändra Wi-Fi Direct (enkel AP) inställningar såsom SSID

Om Wi-Fi Direct (enkel AP)-anslutningen är aktiverad, kan du ändra dessa inställningar via  > **Wi-Fi Direct** > **Gör inställningar** > **Ändra**, och följa sedan de alternativ som visas.

Ändra nätverksnamn

Ändra Wi-Fi Direct (enkel AP)-nätverksnamn (SSID) som används för att ansluta skannern till ditt godtyckliga namn. Du kan ange nätverksnamnet (SSID) med ASCII-tecken som visas på tangentbordet på kontrollpanelen. Du kan ange upp till 22 tecken.

När du ändrar nätverksnamnet (SSID) kopplas alla anslutna enheter bort. Använd det nya nätverksnamnet (SSID) om du vi ansluta till enheten igen.

Ändra lösenord

Ändra Wi-Fi Direct (enkel AP)-lösenord för att ansluta till skannern med ditt godtyckliga värde. Du kan konfigurera lösenordet i de ASCII-tecken som visas på mjukvarutangentbordet på kontrollpanelen. Du kan ange från 8 till 22 tecken.

När du ändrar lösenordet kopplas alla anslutna enheter bort. Använd det nya lösenordet om du vill återansluta enheten.

Ändra frekvensintervall

Ändra frekvensintervallet på Wi-Fi Direct som användas för att ansluta skannern. Du kan välja 2,4 GHz eller 5 GHz.

När du ändrar frekvensintervallet kopplas alla anslutna enheter bort. Anslut enheten igen.

Observera att du inte kan ansluta igen från enheter som inte stöder frekvensintervallet 5 GHz när du ändrar till 5 GHz.

Det kan hända att den här inställningen inte visas beroende på region.

Avaktivera Wi-Fi Direct

Inaktivera skannerns Wi-Fi Direct (enkel AP)-inställningar. När du inaktiverar dem kopplas alla enheter som är anslutna till skannern med Wi-Fi Direct (enkel AP)-anslutning bort.

Återställ inställningarna

Återställ alla Wi-Fi Direct (enkel AP)-inställningar till fabriksinställningar.

Smartenhetens Wi-Fi Direct (enkel AP)-anslutningsinformation som finns sparad på skannern tas bort.

Anmärkning:
*Du kan också konfigurera följande inställningar via fliken **Nätverk** > **Wi-Fi Direct** i Web Config.*

- ❏ *Aktivera eller inaktivera Wi-Fi Direct (enkel AP)*
- ❏ *Ändra nätverksnamn (SSID)*
- ❏ *Ändra lösenord*
- ❏ *Ändra frekvensintervallet*

  Det kan hända att den här inställningen inte visas beroende på region.
- ❏ *Återställa Wi-Fi Direct (enkel AP)-inställningar*

Återställa nätverksanslutningen

I detta avsnitt förklaras hur du gör nätverkningsinställningar och ändrar anslutningssättet när du byter ut den trådlösa routern eller datorn.

När du byter ut den trådlösa routern

Utför anslutningsinställningar för anslutning mellan datorn eller smartenheten och skannern när du byter ut den trådlösa routern.

Du måste göra dessa inställningar om du ändrar internetleverantören och så vidare.

Göra inställningar för anslutning till datorn

Vi rekommenderar att du använder installationsverktyget för att ansluta skannern till en dator. Du kan köra installationsprogrammet på ett av följande sätt.

- ❏ Installera från webbplatsen

  Öppna följande webbplats och ange sedan produktnamnet. Gå till **Inställning** och starta konfigurationen.

  http://epson.sn
- ❏ Konfigurera med mjukvaruskivan (endast för modeller som levereras med en mjukvaruskiva och användare med Windows-datorer med skivenheter).

  Mata in programskivan i datorn och följ instruktionerna på skärmen.

Välja anslutningssätt

Följ instruktionerna på skärmen. På skärmen **Välj åtgärd** väljer du **Konfigurera Skrivare-anslutning (för nya nätverksroutrar eller ändra USB till nätverk, etc.)**, och klickar sedan på **Nästa**.

Följ instruktionerna på skärmen för att slutföra installationen.

Om du inte kan ansluta ska du läsa det följande för att försöka lösa problemet.

”Kan inte ansluta till ett nätverk” på sidan 30

Göra inställningar för anslutning till smartenheten

Du kan använda skannern från en smartenhet, om du ansluter skannern till samma Wi-Fi-nätverk (SSID) som smartenheten. För att använda skannern från en smart enhet öppnar du följande webbplats och anger sedan produktnamnet. Gå till **Inställning** och starta konfigurationen.

http://epson.sn

Åtkomst till webbplatsen från smartenheten som du vill ansluta till skannern.

När du ändrar datorn

Utför anslutningsinställningarna mellan datorn och skannern när du ändrar datorn.

Göra inställningar för anslutning till datorn

Vi rekommenderar att du använder installationsverktyget för att ansluta skannern till en dator. Du kan köra installationsprogrammet med följande metod.

❏ Installera från webbplatsen

Öppna följande webbplats och ange sedan produktnamnet. Gå till **Inställning** och starta konfigurationen.

http://epson.sn

❏ Konfigurera med mjukvaruskivan (endast för modeller som levereras med en mjukvaruskiva och användare med Windows-datorer med skivenheter).

Mata in programskivan i datorn och följ instruktionerna på skärmen.

Följ instruktionerna på skärmen.

Ändra anslutningssätt till datorn

I detta avsnitt förklaras hur du ändrar anslutningssättet när datorn och skannern har anslutits.

Ändra nätverksanslutningen från Ethernet till Wi-Fi

Ändra Ethernet-anslutningen till Wi-Fi-anslutning via skannerns kontrollpanel. Sättet hur du ändrar typ av anslutning är i grund densamma som inställning för Wi-Fi-anslutning.

Relaterad information

➡ ”Ansluta till trådlöst nätverk” på sidan 17

Ändra nätverksanslutningen från Wi-Fi till Ethernet

Följ stegen nedan för att ändra från en Wi-Fi-anslutning till en Ethernet-anslutning.

1. Välj **Inst.** på startskärmen.
2. Välj **Nätverksinställningar** > **Konfiguration av trådbundet LAN**.

3. Följ instruktionerna på skärmen.

Ändra från USB-anslutning till en nätverksanslutning

Du kan använda installationsverktyget och installera om med en annan anslutningsmetod.

❏ Installera från webbplatsen

Öppna följande webbplats och ange sedan produktnamnet. Gå till **Inställning** och starta konfigurationen.

http://epson.sn

❏ Konfigurera med mjukvaruskivan (endast för modeller som levereras med en mjukvaruskiva och användare med Windows-datorer med skivenheter).

Mata in programskivan i datorn och följ instruktionerna på skärmen.

Välja att ändra anslutningssätt

Följ instruktionerna på skärmen. På skärmen **Välj åtgärd** väljer du **Konfigurera Skrivare-anslutning (för nya nätverksroutrar eller ändra USB till nätverk, etc.)**, och klickar sedan på **Nästa**.

Välj den nätverksanslutning som du vill använda, **Anslut via trådlöst nätverk (Wi-Fi)** eller **Anslut via trådbundet LAN (Ethernet)**, och klicka sedan på **Nästa**.

Följ instruktionerna på skärmen för att slutföra installationen.

Kontrollera nätverksanslutningens status

Du kan kontrollera nätverksanslutningsstatus på följande sätt.

Kontrollera nätverksanslutningens status från kontrollpanelen

Du kan kontrollera nätverksanslutningens status via nätverksikonen eller nätverksinformationen på skannerns kontrollpanel.

Kontrollera nätverksanslutningens status med nätverksikonen

Du kan kontrollera nätverksanslutningens status och styrka via nätverksikonen på skannerns startskärm.

	Visar nätverksanslutningsstatus. Välj ikonen för att kontrollera och ändra de aktuella inställningarna. Detta är en genväg till följande meny. **Inst.** > **Nätverksinställningar** > **Inställning av Wi-Fi**	
		Skannern är inte ansluten till ett trådlöst nätverk (Wi-Fi).
		Skannern söker efter SSID, ej konfigurerad IP-adress, eller har problem med ett trådlöst nätverk (Wi-Fi).
		Skannern är ansluten till ett trådlöst nätverk (Wi-Fi). Antalet streck anger signalstyrkan för anslutningen. Ju fler streck desto starkare anslutning.
		Skannern är inte ansluten till ett trådlöst nätverk (Wi-Fi) i Wi-Fi Direct-läge (enkel AP).
		Skannern är ansluten till ett trådlöst nätverk (Wi-Fi) i Wi-Fi Direct-läge (enkel AP).
		Skannern är inte ansluten till ett trådbundet nätverk (Ethernet) eller så har den inaktiverat det.
		Skannern är ansluten till ett kabelanslutet nätverk (Ethernet).

Visa detaljerad nätverksinformation på kontrollpanelen

Du kan även visa annan nätverksrelaterad information genom att välja nätverksmenyerna som du vill kontrollera när skannern är ansluten till nätverket.

1. Välj **Inst.** på startskärmen.
2. Välj **Nätverksinställningar** > **Nätverksstatus**.
3. Om du vill kontrollera annan information ska du välja menyerna du vill kontrollera.
   - ❏ Kabel-LAN/Wi-Fi-status

     Visar nätverksinformation (enhetsnamn, anslutning, signalstyrka och så vidare) för Ethernet- eller Wi-Fi-anslutningar.
   - ❏ Wi-Fi Direct Status

     Visar om Wi-Fi Direct är aktiverad eller inaktiverad och lösenordet för SSID, och så vidare för Wi-Fi Direct-anslutningar.
   - ❏ Status för e-postserver

     Visar nätverksinformation för e-postservern.

Nätverksspecifikationer

Wi-Fi-specifikationer

Se följande tabell för Wi-Fi-specifikationer.

Länder eller regioner med undantag för de som är listade nedan	Tabell A
Australien Nya Zeeland Taiwan Sydkorea	Tabell B

Tabell A

Standarder	IEEE 802.11b/g/n*1
Frekvensområde	2,4 GHz
Maximal radiofrekvenseffekt utsänd	2 400–2 483,5 MHz: 20 dBm (EIRP)
Kanaler	1/2/3/4/5/6/7/8/9/10/11/12/13
Anslutningslägen	Infrastruktur, Wi-Fi Direct (enkel AP)*2*3
Säkerhetsprotokoll*4	WEP (64/128bit), WPA2-PSK (AES)*5, WPA3-SAE (AES), WPA2/WPA3-Enterprise

*1 Finns endast för HT20.

*2 Stöds inte för IEEE 802.11b.

*3 Infrastruktur och lägen för Wi-Fi Direct eller en Ethernet-anslutning kan användas samtidigt.

*4 Wi-Fi Direct stöder endast WPA2-PSK (AES).

*5 Överensstämmer med WPA2-standarder för stöd för WPA/WPA2 Personal.

Tabell B

Standarder	IEEE 802.11a/b/g/n*1/ac		
Frekvensintervall	IEEE 802.11b/g/n: 2,4 GHz, IEEE 802.11a/n/ac: 5 GHz		
Kanaler	Wi-Fi	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12*2/13*2
		5 GHz*3	W52 (36/40/44/48), W53 (52/56/60/64), W56 (100/104/108/112/116/120/124/128/132/136/140/144), W58 (149/153/157/161/165)
	Wi-Fi Direct	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12*2/13*2
		5 GHz*3	W52 (36/40/44/48) W58 (149/153/157/161/165)
Anslutningslägen	Infrastruktur, Wi-Fi Direct (enkel AP)*4, *5		
Säkerhetsprotokoll*6	WEP (64/128bit), WPA2-PSK (AES)*7, WPA3-SAE (AES), WPA2/WPA3-Enterprise		

*1 Finns endast för HT20.

*2 Ej tillgänglig i Taiwan.

*3 Tillgängligheten till dessa kanaler och användning av produkten utomhus över dessa kanaler varierar beroende på plats. För mer information, se http://support.epson.net/wifi5ghz/

*4 Stöds inte för IEEE 802.11b.

*5 Infrastruktur och lägen för Wi-Fi Direct eller en Ethernet-anslutning kan användas samtidigt.

*6 Wi-Fi Direct stöder endast WPA2-PSK (AES).

*7 Överensstämmer med WPA2-standarder för stöd för WPA/WPA2 Personal.

Ethernetspecifikationer

Standarder	IEEE802.3i (10BASE-T)*1 IEEE802.3u (100BASE-TX)*1 IEEE802.3ab (1000BASE-T)*1 IEEE802.3az (Energy Efficient Ethernet)*2
Kommunikationsläge	Auto, 10 Mbps Full duplex, 10 Mbps Halv duplex, 100 Mbps Full duplex, 100 Mbps Halv duplex
Anslutningsenhet	RJ-45

*1 Använd en kategori 5e eller högre STP-kabel (Shielded twisted pair) för att förhindra risk för radiostörningar.

*2 Den anslutna enheten ska uppfylla kraven enligt normen IEEE802.3az.

Nätverksfunktioner och IPv4/IPv6

Funktioner	Stöds
Epson Scan 2	IPv4, IPv6
Document Capture Pro/Document Capture	IPv4
Document Capture Pro Server	IPv4, IPv6

Säkerhetsprotokoll

IEEE802.1X*	
IPsec/IP-filtrering	
SSL/TLS	HTTPS Server/Klient
SMTPS (STARTTLS, SSL/TLS)	
SNMPv3	

* Du behöver använda en anslutningsenhet som uppfyller kraven enligt IEEE802.1X.

Använda port för skannern

Skannern använder följande port. Dessa portar ska vid behov göras tillgängliga för nätverksadministratören.

När sändaren (klient) är skannern

Använd	Destination (server)	Protokoll	Portnummer
Skicka fil (När skanning till nätverksmapp används från skannern)	FTP-/FTPS-server	FTP/FTPS (TCP)	20
			21
	Filserver	SMB (TCP)	445
		NetBIOS (UDP)	137
			138
		NetBIOS (TCP)	139
	WebDAV-server	Protocol HTTP (TCP)	80
		Protocol HTTPS (TCP)	443
Skicka e-post (När skanning till e-post används från skannern)	SMTP-server	SMTP (TCP)	25
		SMTP SSL/TLS (TCP)	465
		SMTP STARTTLS (TCP)	587
POP före SMTP-anslutning (När skanning till e-post används från skannern)	POP-server	POP3 (TCP)	110
Om Epson Connect används	Epson Connect-server	HTTPS	443
		XMPP	5222
Samla in användarinformation (Använd kontakterna från skannern)	LDAP-server	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389
Användarautentisering när du samlar in användarinformation (När du använder kontakterna från skannern) Användarautentisering när du använder skanningen till nätverksmappen (SMB) från skannern	KDC-server	Kerberos	88
Kontroll-WSD	Kundens dator	WSD (TCP)	5357
Sök efter datorn vid push-skanning från en applikation	Kundens dator	Network Push Scan Discovery	2968

När sändaren (klient) är klientdatorn

Använd	Destination (server)	Protokoll	Portnummer
Upptäck skannern från en applikation, såsom EpsonNet Config och skannerdrivrutin.	Skanner	ENPC (UDP)	3289
Samla in och konfigurera MIB-information från en applikation, såsom EpsonNet Config och skannerdrivrutin.	Skanner	SNMP (UDP)	161
Söker WSD-skanner	Skanner	WS-Discovery (UDP)	3702
Vidarebefordra skannade data från ett program	Skanner	Nätverksskanning (TCP)	1865
Samlar jobbinformation vid push-skanning från en applikation	Skanner	Push-skanning av nätverk	2968
Web Config	Skanner	HTTP (TCP)	80
		HTTPS (TCP)	443

Lösa problem

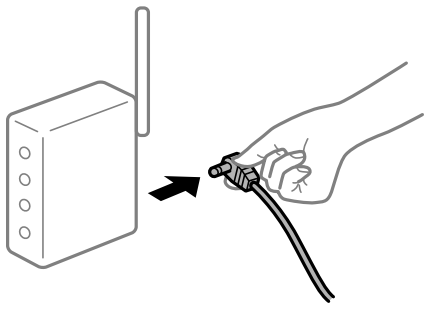
Kan inte ansluta till ett nätverk

Problemet kan bero på ett av de följande orsaken.

Det är något fel med nätverksenheterna för Wi-Fi-anslutning.

Lösningar

Stäng av enheterna du vill ansluta till nätverket. Vänta i cirka 10 sekunder och sätt sedan på enheterna i följande ordning; trådlös router, dator eller smartenhet och sedan skannern. Flytta skannern och datorn eller smarta enheten närmare den trådlösa routern för att förbättra radiovågskommunikationen och försök sedan att utföra nätverksinställningarna igen.



Enheter kan inte ta emot signaler från den trådlösa routern eftersom de är för långt bort.

Lösningar

Efter att du flyttar datorn eller smartenheten och skannern närmare till den trådlösa routern ska du stänga av den trådlösa routern och sedan starta den igen.

När du ändrar den trådlösa routern matchar inställningarna inte till den nya routern.

Lösningar

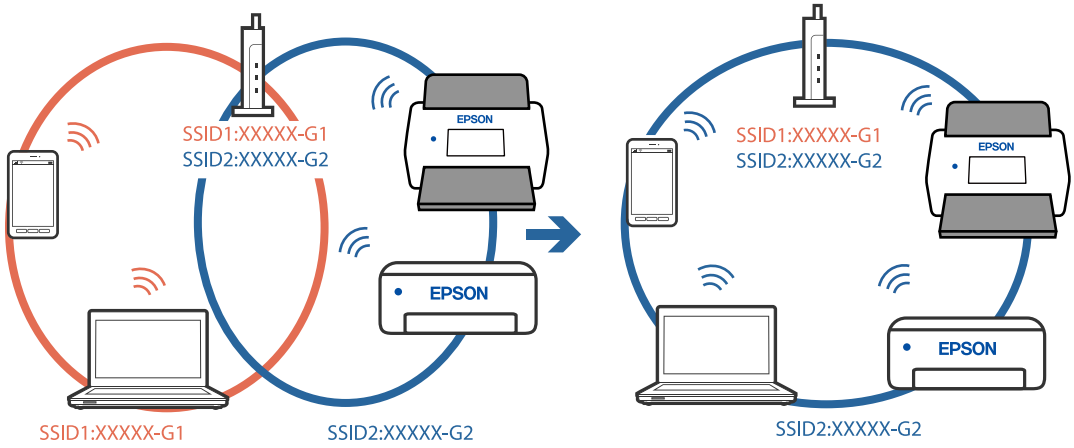
Utför anslutningsinställningarna igen så att de matchar till den nya trådlösa routern.

SSID:er som är ansluta från datorn eller smartenheten och datorn skiljer sig åt.

Lösningar

När du använder flera trådlösa routrar samtidigt eller om den trådlösa routerna har flera SSID:er och enheter som är anslutna till olika SSID:er kan du inte ansluta den trådlösa routern.

Anslut datorn eller smartenheten till samma SSID som skannern.



En sekretessseparatorfunktion finns tillgänglig på den trådlösa routern.

Lösningar

De flesta trådlösa routrar har en sekretesseparatorfunktion som hindrar kommunikationen mellan de anslutna enheterna. Om du inte kan kommunicera mellan skannern och datorn eller smartenheten även om de är anslutna till samma nätverk ska du inaktivera sekretesseparatorn på den trådlösa routern. Mer information finns i dokumentationen som medföljde den trådlösa routern.

IP-adressen är inte tilldelad korrekt.

Lösningar

Om IP-adressen som tilldelats till skannern är 169.254.XXX.XXX, och nätmasken är 255.255.0.0, kanske IP-adressen inte tilldelas korrekt.

Välj **Inst.** > **Nätverksinställningar** > **Avancerat** > **TCP/IP-inställning** på skannerns kontrollpanel och kontrollera sedan IP-adressen och nätmasken som är tilldelade till skannern.

Starta om den trådlösa routern eller återställ nätverksinställningarna för skannern.

Det finns ett problem med datorns nätverksinställningar.

Lösningar

Försök att komma åt webbplatsen från datorn för att kontrollera att datorns nätverksinställningar är korrekt. Om du inte kan komma åt någon webbplats, ligger problemet i datorn.

Kontrollera datorns nätverksanslutning. Mer information finns i dokumentationen som medföljde datorn.

Skannern är ansluten via Ethernet med hjälp av enheter som stöder IEEE 802.3az (energieffektiv Ethernet).

Lösningar

När du ansluter skannern via Ethernet med enheter som stöder IEEE 802.3az (energieffektiv Ethernet) kan följande problem uppstå beroende på vilken hubb eller router du använder.

- ❏ Anslutningen blir instabil, skannern ansluts och kopplas bort gång på gång.
- ❏ Kan inte ansluta till skannern.
- ❏ Kommunikationshastigheten är långsam.

Följ stegen nedan för att inaktivera IEEE 802.3az för skannern och sedan ansluta.

1. Dra ur Ethernetkabeln som är ansluten till datorn och skannern.
2. När IEEE 802.3az på datorn är aktiverat, stäng av det.
   Mer information finns i dokumentationen som medföljde datorn.
3. Anslut datorn direkt till skannern med en ethernetkabel.
4. Kontrollera nätverksinställningarna på skannern.
   Välj **Inst.** > **Nätverksinställningar** > **Nätverksstatus** > **Kabel-LAN/Wi-Fi-status**.
5. Kontrollera skannerns IP-adress.
6. Gå till Web Config på datorn.
   Öppna en webbläsare och ange skannerns IP-adress.
   ”Kör Web-Config i en webbläsare” på sidan 34
7. Välj fliken **Nätverk** > **Kabelanslutet LAN**.
8. Välj **Av** för **IEEE 802.3az**.
9. Klicka på **Nästa**.
10. Klicka på **OK**.
11. Dra ur Ethernetkabeln som är ansluten till datorn och skannern.
12. Om du stängt av IEEE 802.3az på datorn i steg 2, aktivera det.
13. Anslut Ethernetkabeln som du avlägsnade i steg 1 till datorn och skannern.

Om problemet kvarstår kan det vara andra enheter än skannern som orsakar problemet.

Skannern är avstängd.

Lösningar

Kontrollera att skannern är påslagen.

Vänta också tills statuslampan slutar blinka vilket innebär att skannern är klar för skanning.

Mjukvara för att konfigurera skannern

Web Config

Web Config är ett program som körs i en webbläsare, till exempel Internet Explorer eller Safari, på en dator. Du kan bekräfta skannerns status och ändra inställningar för nätverkstjänsten eller skannern. Eftersom skannrar öppnas och används direkt från nätverket är det lämpligt att konfigurera en skanner i taget. För att använda Web Config, ansluter du din dator till samma nätverk som skannern.

Det finns stöd för följande webbläsare.

Microsoft Edge, Windows Internet Explorer 8 eller senare, Firefox*, Chrome*, Safari*

* Använd den senaste versionen.

Kör Web-Config i en webbläsare

1. Kontrollera skannerns IP-adress.

   Välj **Inst.** > **Nätverksinställningar** > **Nätverksstatus** på skannerns kontrollpanel. Välj sedan status för aktiv anslutningsmetod (**Kabel-LAN/Wi-Fi-status** eller **Wi-Fi Direct Status**) för att bekräfta skannerns IP-adress.

2. Öppna en webbläsare på en dator eller smartenhet och ange sedan skannerns IP-adress.

   Format:

   IPv4: http://skannerns IP-adress/

   IPv6: http://[skannerns IP-adress]/

   Exempel:

   IPv4: http://192.168.100.201/

   IPv6: http://[2001:db8::1000:1]/

   Anmärkning:
   Eftersom skannern använder ett självsignerat certifikat vid åtkomst till HTTPS visas en varning i webbläsaren när du startar Web Config; detta tyder inte på ett problem och kan ignoreras.

3. Logga in som administratör för att ändra skannerinställningarna.

   Klicka på **Administratörsinloggning** uppe i högra hörnet av skärmen. Ange **Användarnamn** och **Nuvarande lösenord** och klicka sedan på **OK**.

   Anmärkning:
   ❏ *Följande ger de initiala värdena för Web Config-administratörsinformationen.*

   ·Användarnamn: inget (blank)

   ·Lösenord: skannerns serienummer

   För att hitta serienumret, kontrollera etiketten som sitter på baksidan av skannern.

   ❏ *Om **Logga ut administratör** visas längst upp till höger på skärmen är du redan inloggad som administratör.*

Köra Web Config på Windows

Vid anslutning av en dator till skannern via WSD, följ stegen nedan för att köra Web Config.

1. Öppna skannerlistan på datorn.

   ❏ Windows 10

   Klicka på startknappen och välj sedan **Windows-system** > **Kontrollpanelen** > **Visa enheter och skrivare** i **Maskinvara och ljud**.

   ❏ Windows 8.1/Windows 8

   Välj **Skrivbord** > **Inställningar** > **Kontrollpanelen** > **Visa enheter och skrivare** i **Maskinvara och ljud** (eller **Maskinvara**).

   ❏ Windows 7

   Klicka på startknappen och välj **Kontrollpanelen** > **Visa enheter och skrivare** i **Maskinvara och ljud**.

2. Högerklicka på skannern och välj **Egenskaper**.

3. Välj fliken **Webbtjänst** och klicka på URL-adressen.

   Eftersom skannern använder ett självsignerat certifikat vid åtkomst till HTTPS visas en varning i webbläsaren när du startar Web Config; detta tyder inte på ett problem och kan ignoreras.

   Anmärkning:

   ❏ *Följande ger de initiala värdena för Web Config-administratörsinformationen.*

   ·Användarnamn: inget (blank)

   ·Lösenord: skannerns serienummer

   För att hitta serienumret, kontrollera etiketten som sitter på baksidan av skannern.

   ❏ *Om **Logga ut administratör** visas längst upp till höger på skärmen är du redan inloggad som administratör.*

Epson Device Admin

Med multifunktionsprogrammet Epson Device Admin kan du hantera skrivarens inbyggda programvara.

Du kan använda konfigurationsmallar för att verkställa gemensamma inställningar till flera skannrar i ett nätverk, vilket gör den lämplig för installation och hantering av flera skannrar.

Du kan hämta Epson Device Admin från webbplatsen för Epson-support. För detaljer kring hur du använder detta program, se dokumentation eller hjälp för Epson Device Admin.

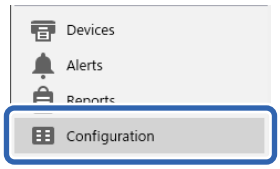
Konfigurationsmall

Skapa konfigurationsmallen

Skapa konfigurationsmallen.

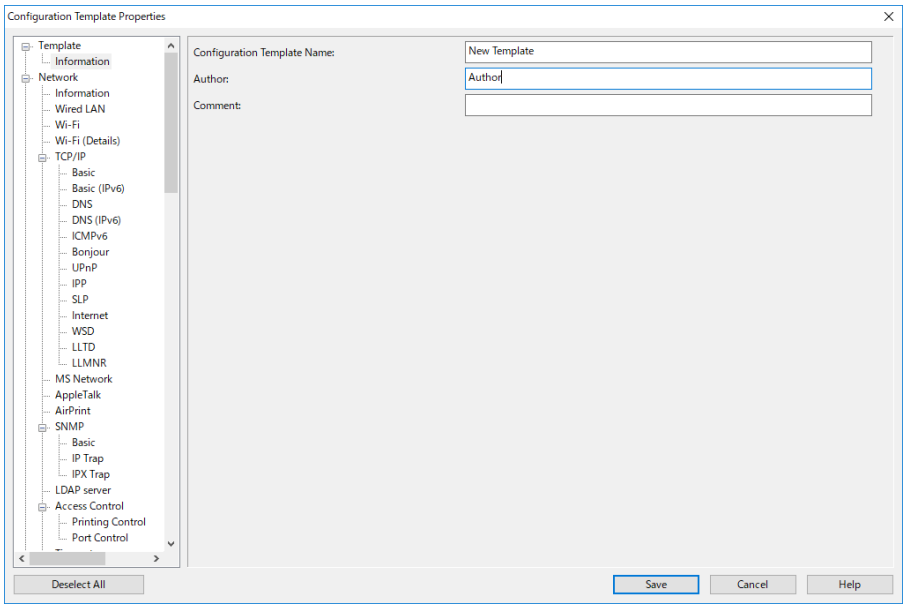
1. Starta Epson Device Admin.

2. Välj **Configuration** på siduppgiftsmenyn.



3. Välj **New** på färgbandsmenyn.

4. Ställ in varje objekt.



Alternativ	Förklaring
Configuration Template Name	Namn på konfigurationsmall. Ange högst 1024 tecken i Unicode (UTF-8).
Author	Information kring skapare av mallen. Ange högst 1024 tecken i Unicode (UTF-8).
Comment	Ange godtycklig information. Ange högst 1024 tecken i Unicode (UTF-8).

5. Välj de objekt som du vill konfigurera till vänster.

Anmärkning:
Klicka på menyobjekten till vänster för att växla till varje skärm. Det konfigurerade värdet spras om du växlar skärm, men inte om du avbryter skärmen. När du har slutfört alla inställningar klickar du på ***Save****.*

Verkställ konfigurationsmallen

Verkställ den sparade konfigurationsmallen för skannern. Objekten som valts i mallen verkställs. Om målskannern saknar tillämplig funktion verkställs den inte.

Anmärkning:
När ett administratörslösenord är konfigurerat för skannern ska du konfigurera lösenordet i förväg.

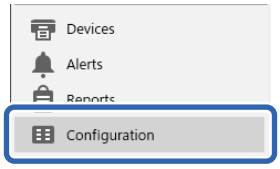
*1. I färgbandsmenyn för enhetslistskärmen väljer du **Options** > **Password manager**.*

*2. Välj **Enable automatic password management**, och klicka sedan på **Password manager**.*

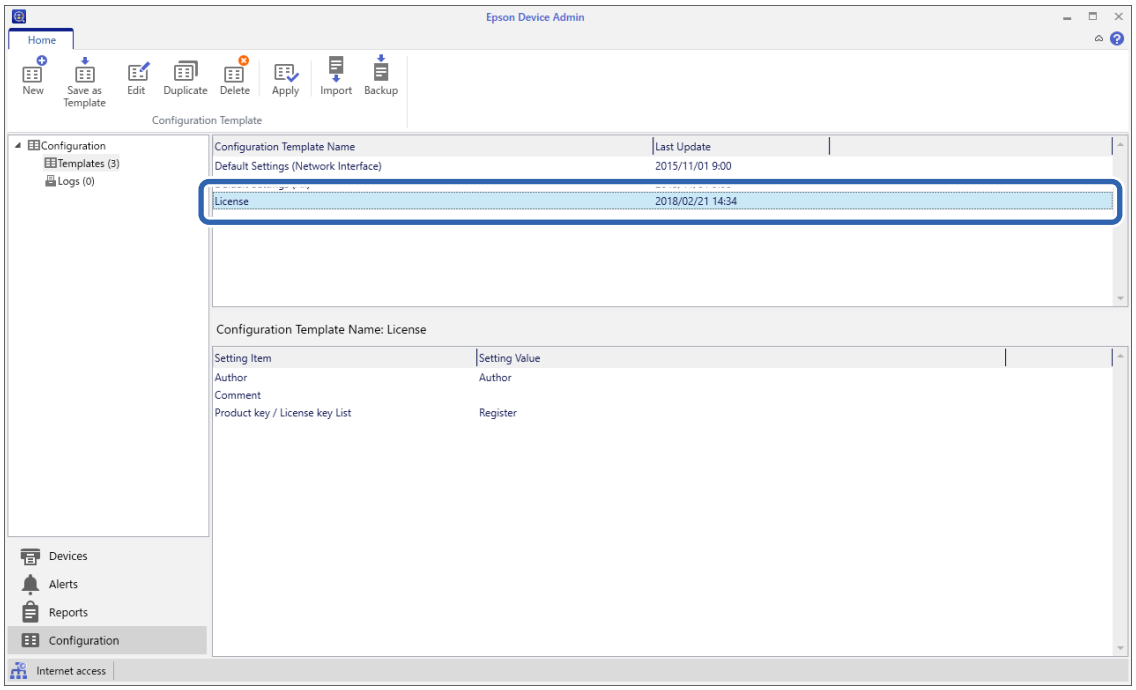
*3. Välj lämplig skanner och klicka sedan på **Edit**.*

*4. Konfigurera lösenordet och klicka sedan på **OK**.*

1. Välj **Configuration** på siduppgiftsmenyn.



2. Välj den konfigurationsmall du vill verkställa från **Configuration Template Name**.



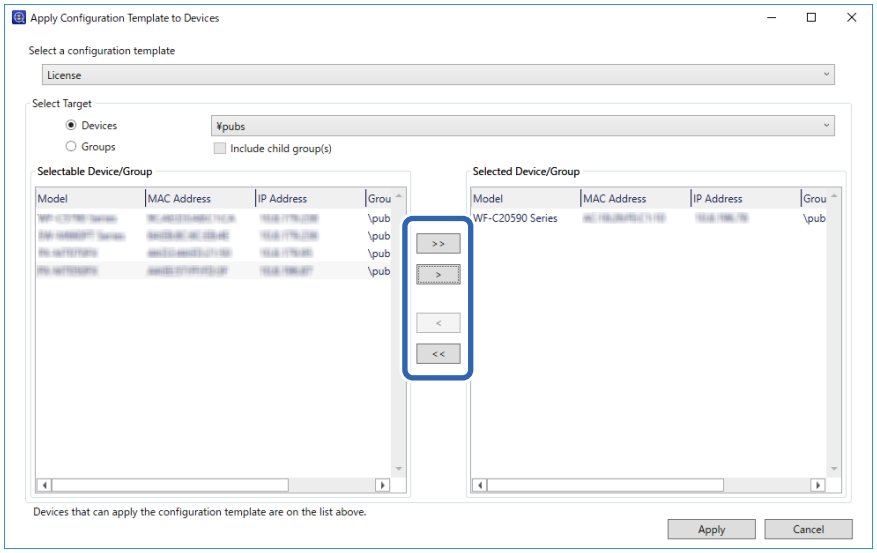
3. Klicka på **Apply** på färgbandsmenyn.

   Skärmen för enhetsval visas.

4. Välj den konfigurationsmall du vill verkställa.

   Anmärkning:
   - ❏ *När du väljer **Devices** och grupper med enheter från menyn visas varje enhet.*
   - ❏ *Grupper visas när du väljer **Groups**. Välj **Include child group(s)** för att automatiskt välja barngrupper inom den valda gruppen.*

5. Flytta skanner eller grupper som du vill verkställa mallen för **Selected Device/Group**.



6. Klicka på **Apply**.

   En bekräftelseskärm för konfigurationsmallen som ska verkställas visas.

7. Klicka på **OK** för att verkställa konfigurationsmallen.

8. När ett meddelande visas om att registreringen är slutförd så stäng webbläsaren **OK**.

9. Klicka på **Details** och kontrollera informationen.

   När visas för objekten du har verkställs slutförs applikationen.

10. Klicka på **Close**.

Inställningar som krävs för skanning

Konfigurera en e-postserver

Konfigurera e-postservern från Web Config.

När skannern kan skicka e-post genom att konfigurera e-postservern är följande möjligt.

❏ Överför skanningsresultat med e-post

❏ Tar emot e-postmeddelande från skannern

Kontrollera nedan innan du utför konfigurationen.

❏ Skannern ansluts till nätverket som kan få åtkomst till e-postservern.

❏ Informationen för e-postinställningarna för datorn som använder samma e-postserver som skannern.

Anmärkning:

❏ *När du använder e-postservern på Internet ska du kontrollera inställningsinformationen från leverantören eller webbplatsen.*

❏ *Du kan även konfigurera e-postservern från kontrollpanelen. Öppna enligt nedan.*

Inst. > ***Nätverksinställningar*** > ***Avancerat*** > ***E-postserver*** > ***Serverinställningar***

1. Öppna Web Config och välj fliken **Nätverk** > **E-postserver** > **Grundläggande**.
2. Ange ett värde för varje alternativ.
3. Välj **OK**.

   Inställningarna du har valt visas.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

Inställningsalternativ för e-postserver

Alternativ	Inställningar och förklaringar	
Autentiseringsmetod	Ange autentiseringsmetoden som skannern ska använda för åtkomst till e-postservern.	
	Av	Autentisering är inaktiverad vid kommunikation med meddelandeservern.
	SMTP AUT.	Kräver att en mejlserver stöder SMTP-autentisering.
	POP före SMTP	Konfigurera en POP3-server när du väljer den här metoden.
Autentiseringskonto	Om du väljer **SMTP AUT.** eller **POP före SMTP** som **Autentiseringsmetod**, ange autentiserat kontonamn mellan 0 och 255 tecken i ASCII (0x20–0x7E).	
Autentiserat lösenord	Om du väljer **SMTP AUT.** eller **POP före SMTP** som **Autentiseringsmetod**, ange autentiserat kontonamn mellan 0 och 20 tecken i ASCII (0x20–0x7E).	
Avsändarens e-postadress	Ange avsändarens e-postadress. Ange mellan 0 och 255 tecken i ASCII (0x20–0x7E) förutom : ( ) < > [ ] ; ¥. Det första tecknet kan inte vara en punkt ”.”.	
SMTP-serveradress	Ange mellan 0 och 255 tecken med A–Z a–z 0–9 . -. Du kan använda IPv4- eller FQDN-format.	

Alternativ	Inställningar och förklaringar	
SMTP-serverportnummer	Ange ett nummer mellan 1 och 65535.	
Säker anslutning	Ange säker anslutningsmetod för e-postservern.	
	Saknas	Om du väljer **POP före SMTP** i **Autentiseringsmetod**, är anslutningsmetoden inställd på **Saknas**.
	SSL/TLS	Detta är tillgängligt när **Autentiseringsmetod** är satt till **Av** eller **SMTP AUT.**.
	STARTTLS	Detta är tillgängligt när **Autentiseringsmetod** är satt till **Av** eller **SMTP AUT.**.
Certifikatverifiering	Certifikatet är validerat när detta är aktiverat. Vi rekommenderar att detta är satt till **Aktivera**.	
POP3-serveradress	Om du väljer **POP före SMTP** som **Autentiseringsmetod**, anger du POP3-serveradress med mellan 0 och 255 tecken med A–Z a–z 0–9 . -. Du kan använda IPv4- eller FQDN-format.	
POP3-serverportnummer	Om du väljer **POP före SMTP** för **Autentiseringsmetod**, ska du ange ett nummer mellan 1 och 65535.	

Kontrollera e-postserverns anslutning

Du kan kontrollera anslutningen till mejlservern genom att utföra anslutningskontrollen.

1. Öppna Web Config och välj fliken **Nätverk** > **E-postserver** > **Anslutningstest**.
2. Välj **Starta**.

   Anslutningstest för e-postservern startas. Efter testet, kontrollera rapporten som visas.

   Anmärkning:
   Du kan också kontrollera anslutningen till mailservern från kontrollpanelen. Öppna enligt nedan.

   Inst. > ***Nätverksinställningar*** > ***Avancerat*** > ***E-postserver*** > ***Kontrollera anslutning***

Referens för anslutningstest av e-postserver

Meddelanden	Orsak
Anslutningstest lyckades.	Detta meddelande visas när anslutningen till servern lyckades.
Kommunikationsfel för SMTP-server. Kontrollera följande. - Nätverksinställningar	Detta meddelande visas när ❏ Skannern är inte ansluten till ett nätverk ❏ SMTP-servern ligger nere ❏ Närverksanslutning är frånkopplad under kommunikationen ❏ Ofullständiga data mottagna

Meddelanden	Orsak
Kommunikationsfel för POP3-server. Kontrollera följande. - Nätverksinställningar	Detta meddelande visas när ❏ Skannern är inte ansluten till ett nätverk ❏ POP3-servern ligger nere ❏ Närverksanslutning är frånkopplad under kommunikationen ❏ Ofullständiga data mottagna
Ett fel inträffade vid anslutning till SMTP-server. Kontrollera de följande. - SMTP-serveradress - DNS-server	Detta meddelande visas när ❏ Anslutning till en DNS-server misslyckades ❏ Namnmatchning för en SMTP-server misslyckades
Ett fel inträffade vid anslutning till POP3-server. Kontrollera de följande. - POP3-serveradress - DNS-server	Detta meddelande visas när ❏ Anslutning till en DNS-server misslyckades ❏ Namnupplösning för en POP3-server misslyckades
Autentiseringsfel för SMTP-server. Kontrollera de följande. - Autentiseringsmetod - Autentiseringskonto - Autentiseringslösenord	Detta meddelande visas när SMTP-serverautentisering misslyckades.
Autentiseringsfel för POP3-server. Kontrollera de följande. - Autentiseringsmetod - Autentiseringskonto - Autentiseringslösenord	Detta meddelande visas när POP3-serverautentisering misslyckades.
Kommunikationsmetoden saknar stöd. Kontrollera följande. - SMTP-serveradress - Portnummer för SMTP-server	Detta meddelande visas när du försöker kommunicera med protokoll som inte stöds.
Anslutning till SMTP-server misslyckades. Ändra Säker anslutning till Saknas.	Detta meddelade visas när det uppstår en SMTP-felmatchning mellan en server och en klient, eller när servern inte stödjer SMTP-säker anslutning (SSL-anslutning).
Anslutning till SMTP-server misslyckades. Ändra Säker anslutning till SSL/TLS.	Detta meddelande visas när det uppstår en SMTP-felmatchning mellan en server och en klient, eller när servers frågar om att använda en SSL/TLS-anslutning för en SMTP säker anslutning.
Anslutning till SMTP--server misslyckades. Ändra Säker anslutning till STARTTLS.	Detta meddelande visas när det uppstår en SMTP-felmatchning mellan en server och en klient, eller när servern frågar om att använda en STARTTLS-anslutning för en SMTP säker anslutning.
Anslutningen är inte betrodd. Kontrollera följande. - Datum och tid	Detta meddelande visas när skanners inställningar för datum och tid är fel eller när certifikatet har gått ut.
Anslutningen är inte betrodd. Kontrollera följande. - CA-certifikat	Detta meddelande visas när skannern inte har ett rotcertifikat som motsvarar servern eller när ett CA-certifikat inte har importerats.
Anslutningen är inte säker.	Detta meddelande visas när det förvärvda certifikatet är skadat.
Autentisering av SMTP-server misslyckades. Ändra Autentiseringsmetod till SMTP-AUTH.	Detta meddelande visas när det uppstod en felmatchning i autentiseringsmetoden mellan en server och en klient. Servern stödjer SMTP AUT..

Meddelanden	Orsak
Autentisering av SMTP-server misslyckades. Ändra Autentiseringsmetod till POP före SMTP.	Detta meddelande visas när det uppstod en felmatchning i autentiseringsmetoden mellan en server och en klient. Servern stödjer inte SMTP AUT..
Avsändarens e-postadress är felaktig. Ändra till e-postadressen för din e-posttjänst.	Detta meddelande visas när sändarens specificerade e-postadress är fel.
Det går inte att komma åt produkten förrän bearbetningen är klar.	Detta meddelande visas när skannern är upptagen.

Ställ in en delad nätverksmapp

Ställ in en delad nätverksmapp för att spara den skannade bilden.

När du sparar en fil i mappen loggar skannern in som användaren av datorn som mappen skapades på.

Skapa delad mapp

Relaterad information

➡ ”Innan du skapar den delade mappen” på sidan 43

➡ ”Kontrollera nätverksprofilen” på sidan 43

➡ ”Plats där den delade mappen skapas och ett exempel på säkerhet” på sidan 44

➡ ”Lägga till grupp eller användare med behörighetsåtkomst” på sidan 55

Innan du skapar den delade mappen

Innan du skapar den delade mappen ska du kontrollera följande.

❏ Skannern är ansluten till nätverket där den kan få åtkomst till datorn där den delade mappen skapas.

❏ Ett multibyte-tecken är inte inkluderat i namnet på datorn där den delade mappen skapas.

Viktigt:

När ett multibyte-tecken är inkluderat i datornamnet kanske det inte går att spara den delade mappen.

I så fall ändrar du till datorn som inte inkluderar multibyte-tecken i namnet eller ändrar datornamn.

Vid byte av datornamn ska du se till att kontrollera med administratören i förväg, eftersom det kan påverka vissa inställningar, såsom datorhantering, resursåtkomst etc.

Kontrollera nätverksprofilen

På datorn där den delade mappen skapas ska du kontrollera om mappdelning finns tillgänglig.

1. Logga in på datorn där den delade mappen skapas av användarkontot med administratörsbehörighet.

2. Välj **Kontrollpanelen** > **Nätverk och Internet** > **Nätverk och delningscenter**.

3. Klicka på **Ändra avancerade delningsinställningar**, och klicka sedan på för profilen med **(aktuell profil)** i de nätverksprofiler som visas.

4. Kontrollera om **Aktivera fil- och skrivardelning** väljs i **Fil- och skrivardelning**.

   Om det redan har valts, klicka på **Avbryt** och stäng fönstret.

   När du ändrar inställningar klickar du på **Spara ändringar** och stänger fönstret.

Plats där den delade mappen skapas och ett exempel på säkerhet

Beroende på platsen där den delade mappen skapas kan säkerheten och bekvämligheten variera.

För att använda den delade mappen från skannern eller andra datorer krävs följande läs- och ändringsbehörigheter för mappen.

❏ Fliken **Delning** > **Avancerad delning** > **Behörighet**

Den kontrollerar nätverksåtkomstbehörigheten för den delade mappen.

❏ Åtkomstbehörighet för fliken **Säkerhet**

Den kontrollerar nätverksåtkomstbehörigheten och lokal åtkomst för den delade mappen.

När du konfigurerar **Alla** för den delade mappen som skapas på skrivbordet, som ett exempel på hur du skapar en delad mapp får alla användare som kan få åtkomst till datorn behörig åtkomst.

Användaren som inte har behörighet kan få åtkomst på grund av att skrivbordet (mappen) styrs av användarmappen och sedan säkerhetsinställningarna för mappen som hanteras nedåt i den. Användaren som är behörig att få åtkomst på fliken **Säkerhet** (användaren loggar in och administratören i det här fallet) kan använda mappen.

Se nedan för hur du skapar korrekt plats.

Det här exemplet är till när du skapar mappen ”scan_folder”.

Relaterad information

➡ ”Exempel på konfiguration för filservrar” på sidan 44

➡ ”Exempel på konfiguration för en dator” på sidan 50

Exempel på konfiguration för filservrar

Den här förklaringen är ett exempel på hur du skapar den delade mappen i roten för enheten på den delade datorn, såsom filservern under följande förhållanden.

Åtkomstkontrollerbara användare, såsom någon som har samma domän för en dator för att skapa en delad mapp, kan få åtkomst till den delade mappen.

Ange konfigurationen när du godkänner att en användare ska läsa och skriva till den delade mappen på datorn, såsom filservern och den delade datorn.

❏ Plats för att skapa delad mapp: Rotenhet

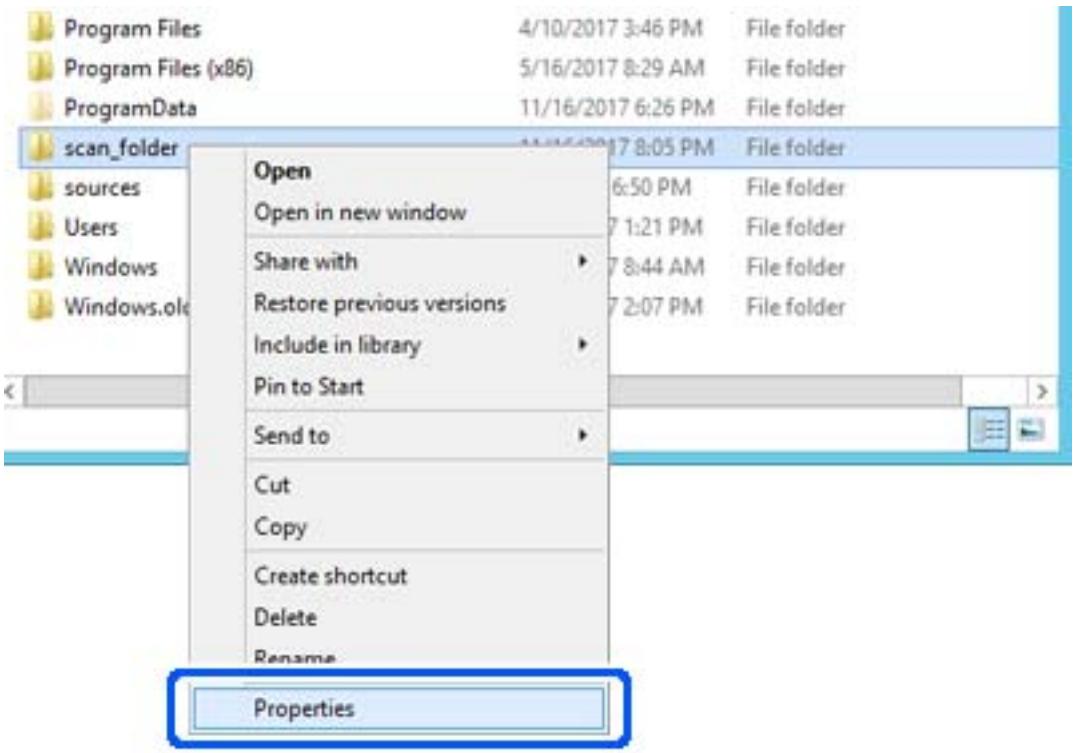
❏ Mappsökväg: C:\scan_folder

❏ Åtkomstbehörighet via nätverk (delningsbehörighet): Alla

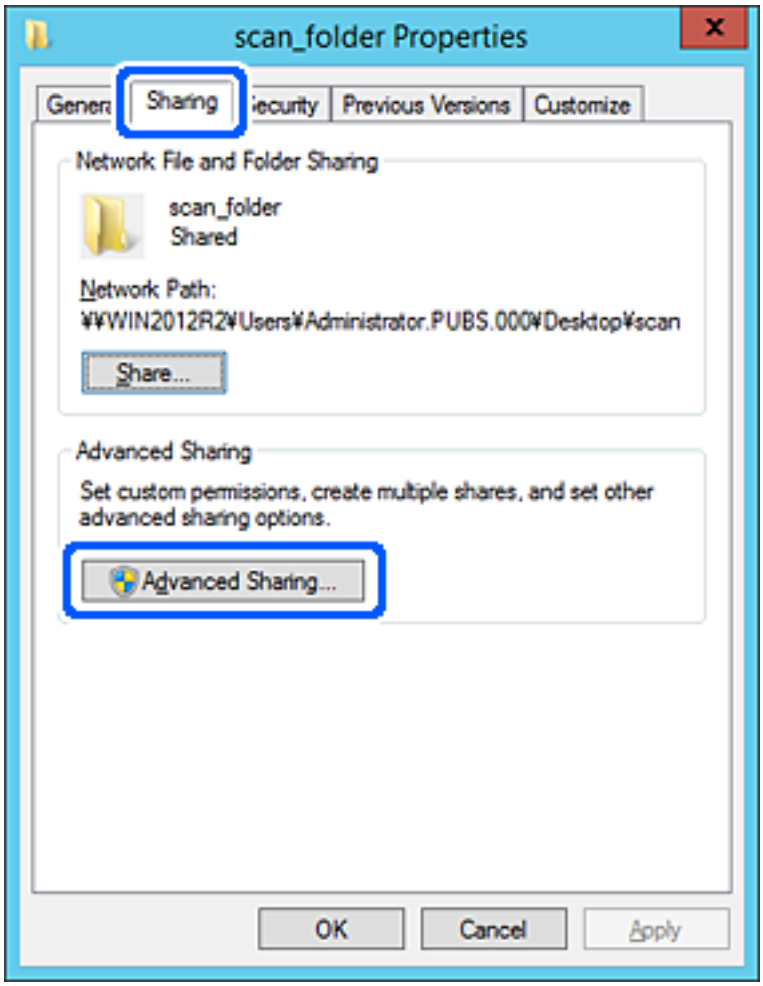
❏ Åtkomstbehörighet i filsystem (Security): Autentiserade användare

1. Logga in på datorn där den delade mappen skapas av användarkontot med administratörsbehörighet.
2. Starta utforskaren.
3. Skapa mappen i rotenheten och ge den namnet ”scan_folder”.

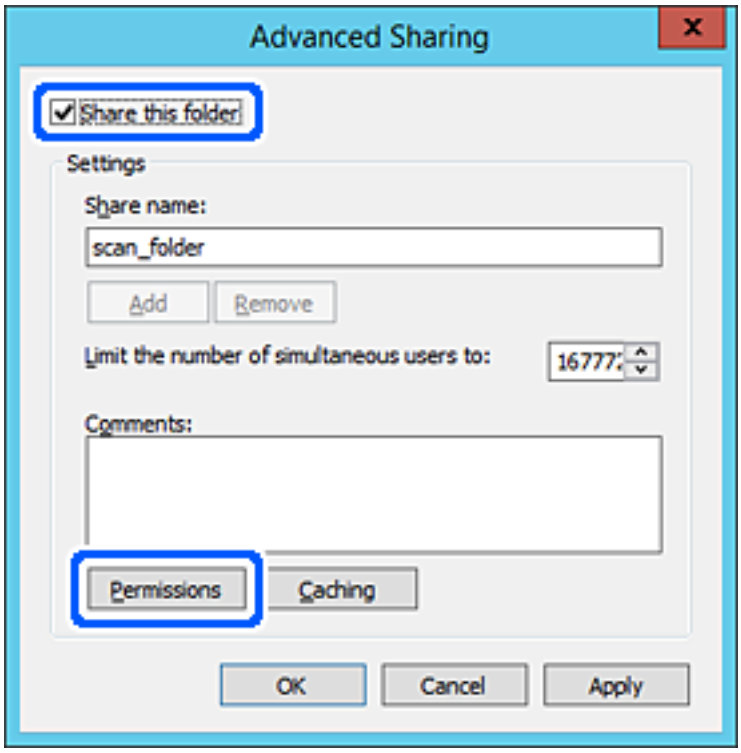
   För mappnamnet anger du mellan 1 och 12 alfanumeriska tecken. Om teckengränsen för mappnamnet är överskriden kan du inte komma åt den på normalt sätt genom varierad miljö.
4. Högerklicka på mappen och välj sedan **Egenskaper**.



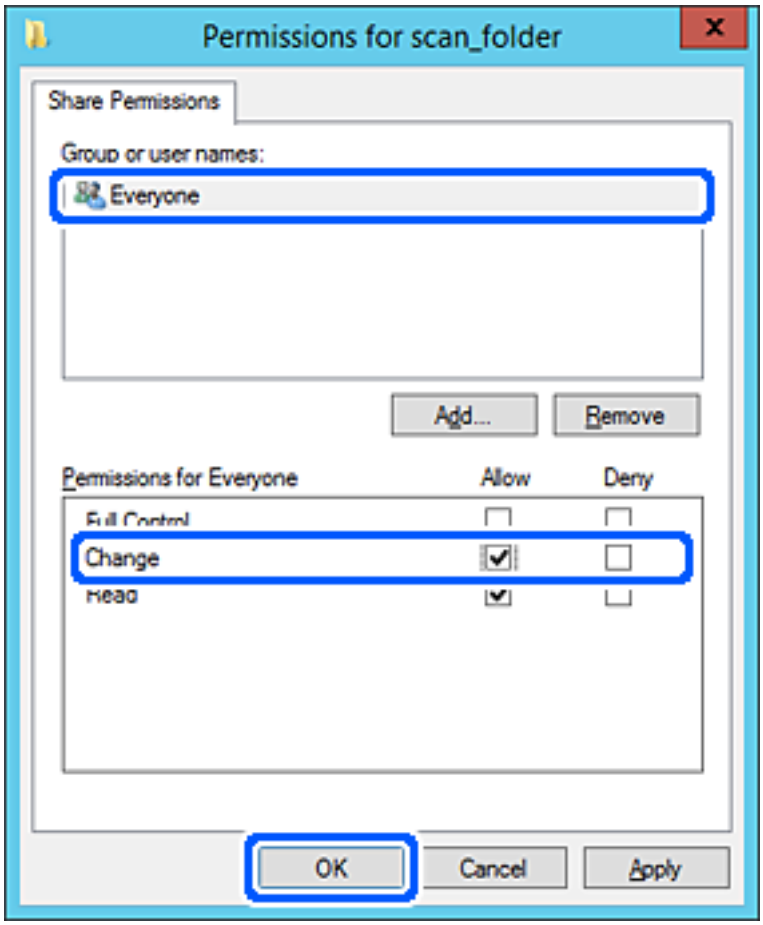
5. Klicka på **Avancerad delning** i fliken **Delning**.



6. Välj **Dela den här mappen**, och klicka på **Behörighet**.

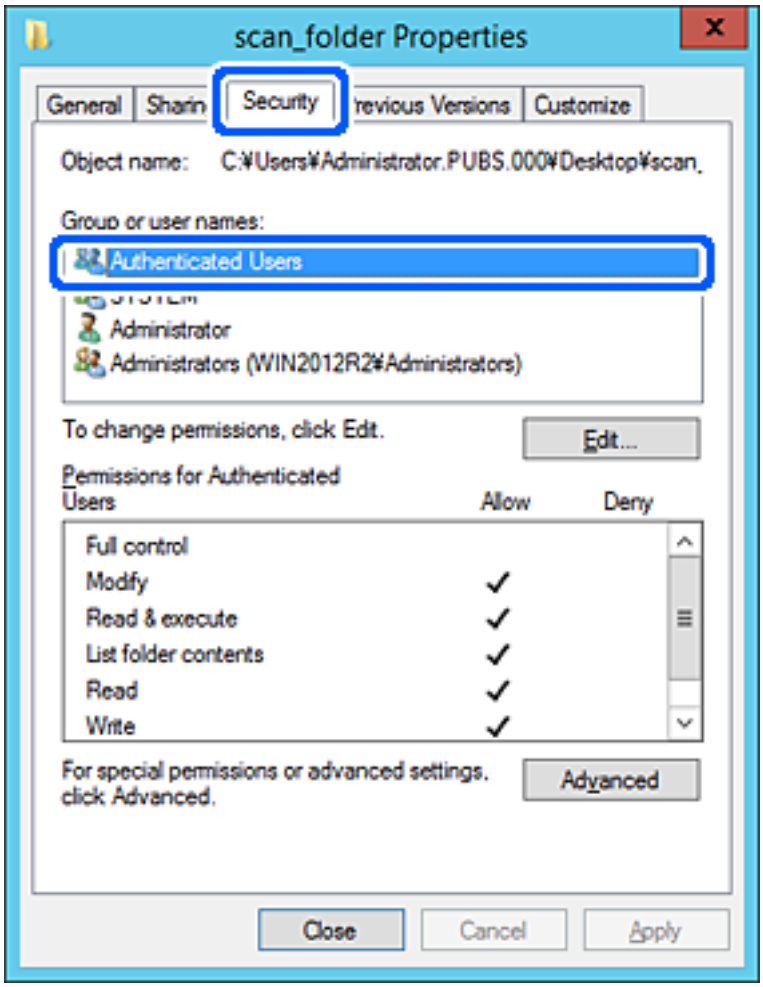


7. Välj gruppen **Alla** i **Grupp- eller användarnamn**, välj **Tillåt** i **Ändra** och klicka sedan på **OK**.



8. Klicka på **OK**.

9. Välj **Säkerhet** och välj sedan **Autentiserade användare** i **Grupp eller användarnamn**.

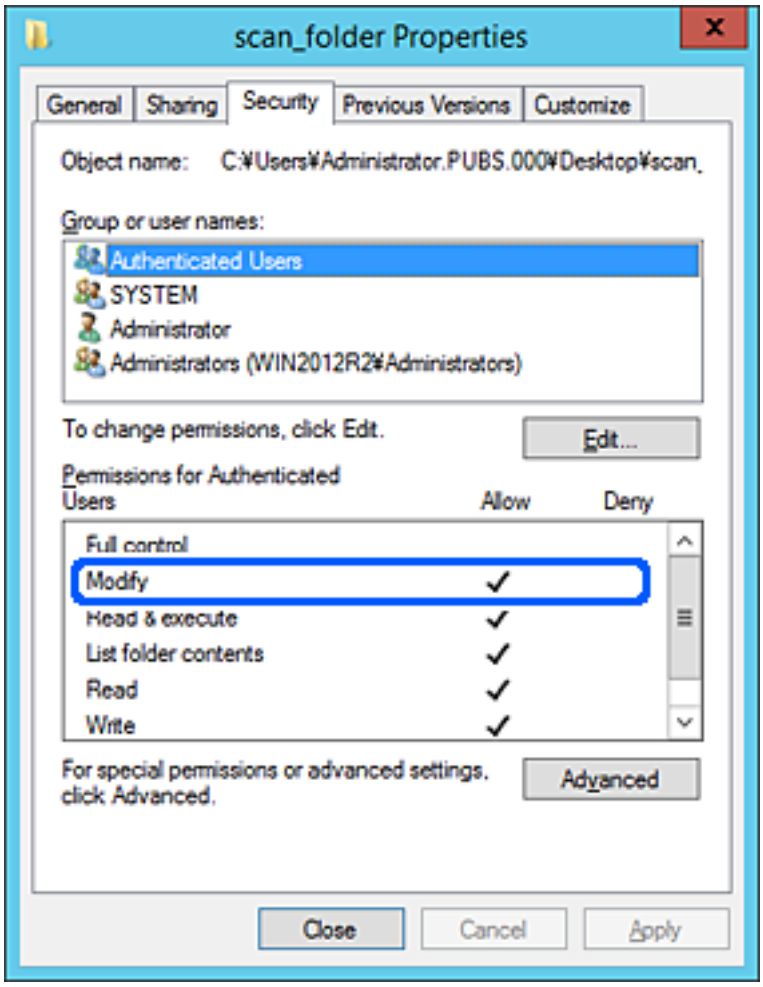


”Autentiserade användare” är specialgruppen som inkluderar alla användare som kan logga in på domänen eller datorn. Den här gruppen visas bara när mappen skapas under rotmappen.

Du kan lägga till genom att klicka på **Redigera** om den inte visas. För mer information, se Relaterad information.

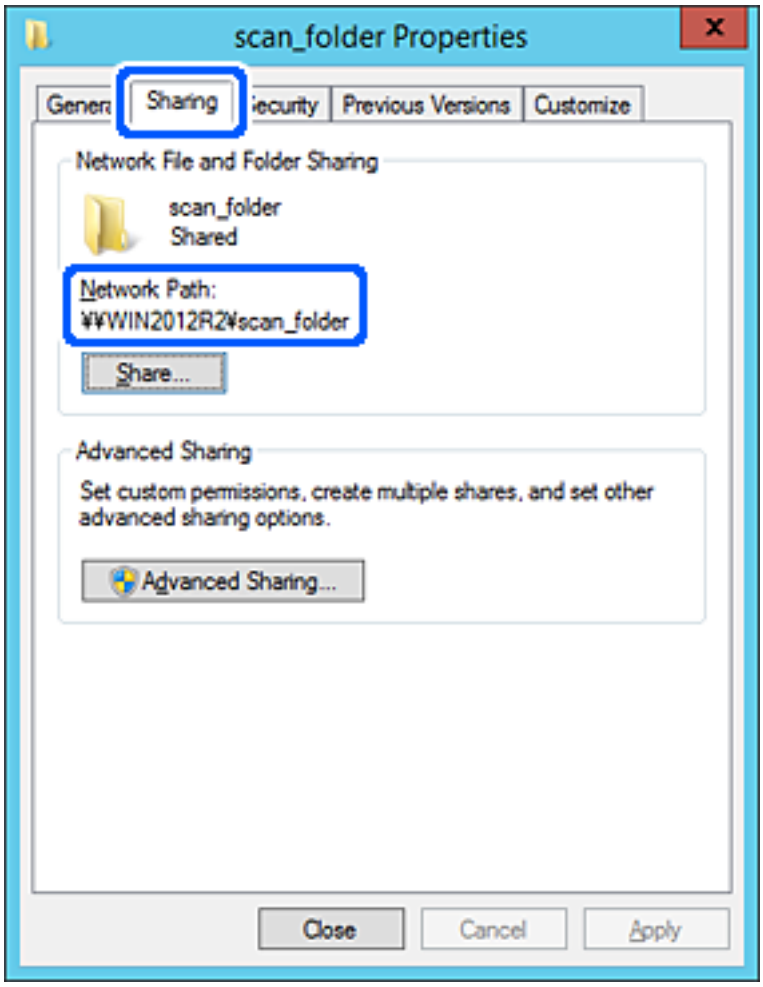
10. Kontrollera att **Tillåt** på **Modifiera** väljs i **Behöriheter för autentiserade användare**.

    Om alternativet inte väljs väljer du **Autentiserade användare**, klickar på **Redigera**, väljer **Tillåt** på **Modifiera** i **Behörigehter för autentiserade användare**, och klickar sedan på **OK**.



11. Välj fliken **Delning**.

    Den delade mappens nätverksväg visas. Det här används vid registrering i skannerns kontaktlista. Skriv ned den.



12. Klicka på **OK** eller **Stäng** för att stänga skärmen.

    Kontrollera om filen kan skrivas över eller läsas i den delade mappen från datorer i samma domän.

Relaterad information

➡ ”Lägga till grupp eller användare med behörighetsåtkomst” på sidan 55
➡ ”Registrera en destination i kontakter med Web Config” på sidan 60

Exempel på konfiguration för en dator

Den här förklaringen är ett exempel på hur du skapar den delade mappen på skrivbordet för användaren som är inloggad på datorn.

Användaren som loggar in på datorn och har administratörsbehörighet kan få åtkomst till skrivbordsmappen och dokumentmappen som ligger under användarmappen.

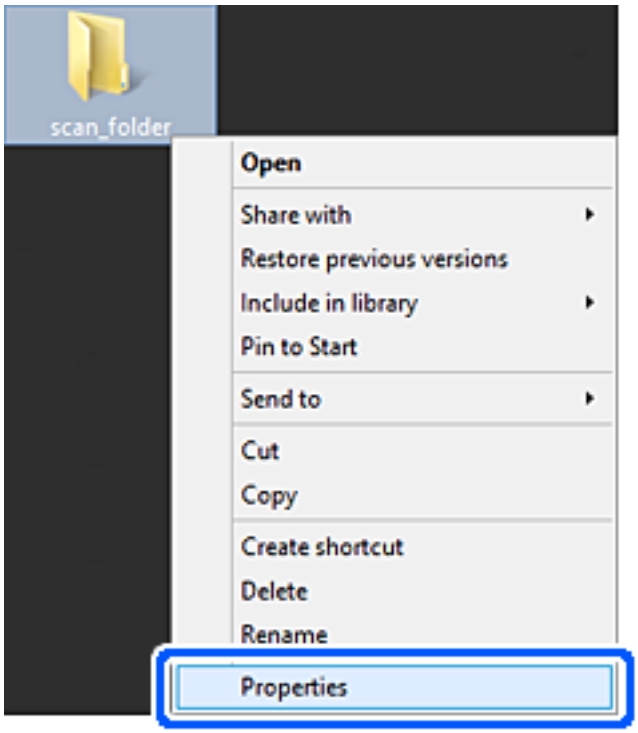
Ställ in den här konfigurationen när DU INTE tillåter läsning och skrivning till en annan användare till den delade mappen på en persondator.

❏ Plats för att skapa delad mapp: Skrivbord

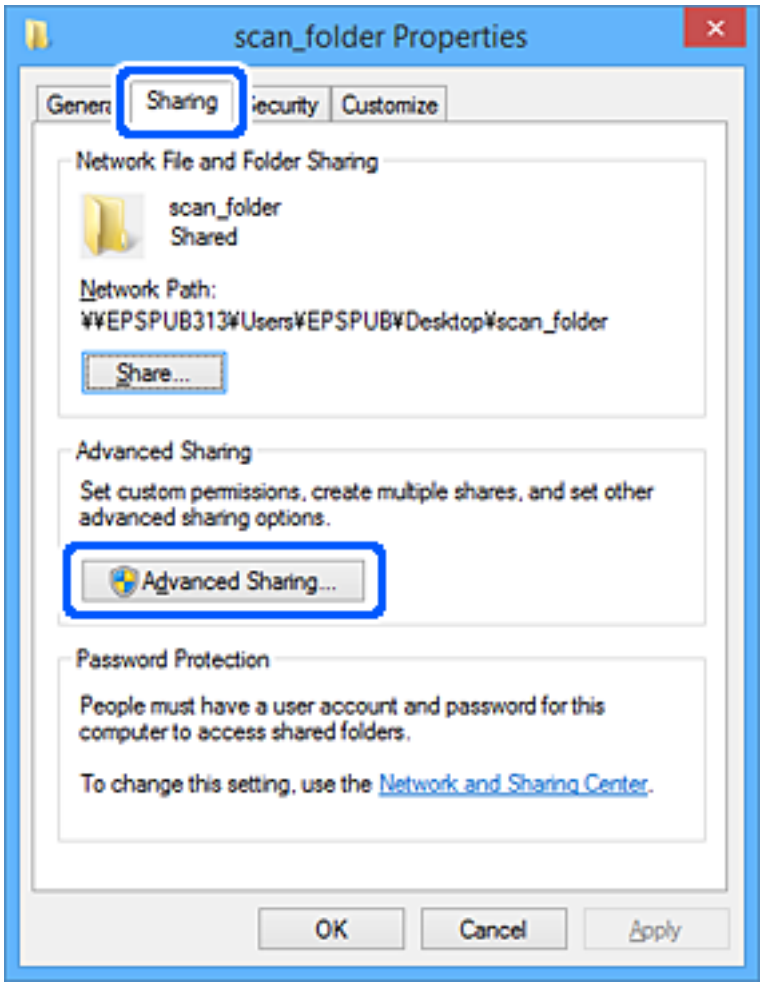
- ❏ Mappsökväg: C:\Users\xxxx\Desktop\scan_folder
- ❏ Åtkomstbehörighet via nätverk (delningsbehörighet): Alla
- ❏ Åtkomstbehörighet i filstystem (Säkerhet): lägg inte till, eller lägg till Användare/Gruppnamn för att tillåta åtkomst

1. Logga in på datorn där den delade mappen skapas av användarkontot med administratörsbehörighet.
2. Starta utforskaren.
3. Skapa mappen på skrivbordet och ge den namnet ”scan_folder”.

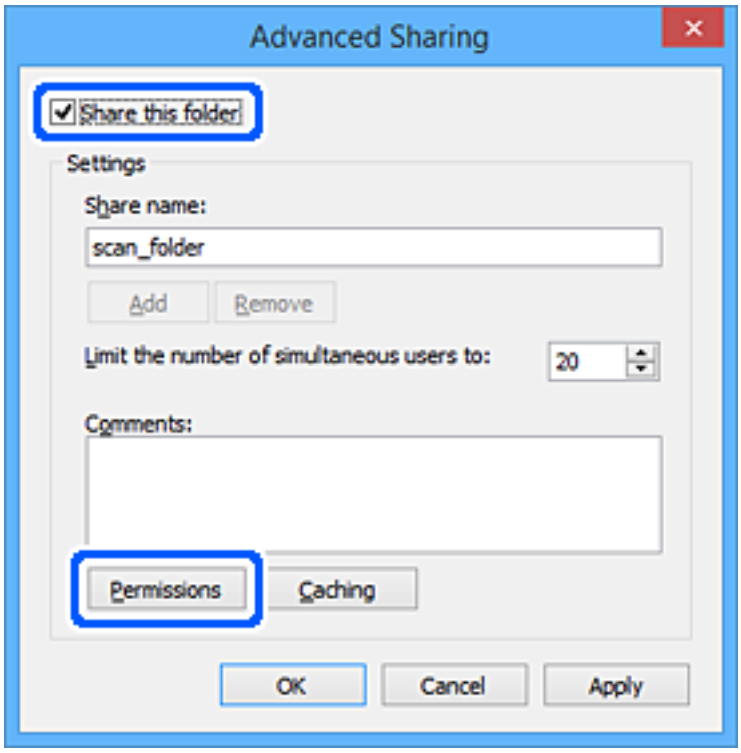
   För mappnamnet anger du mellan 1 och 12 alfanumeriska tecken. Om teckengränsen för mappnamnet är överskriden kan du inte komma åt den på normalt sätt genom varierad miljö.
4. Högerklicka på mappen och välj sedan **Egenskaper**.



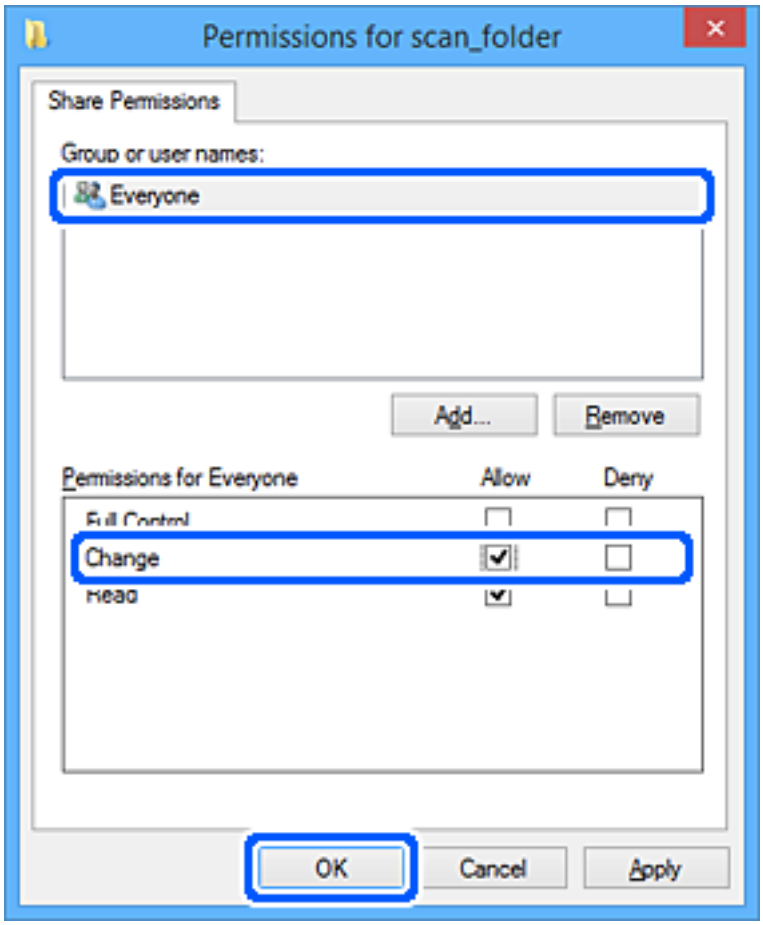
5. Klicka på **Avancerad delning** i fliken **Delning**.



6. Välj **Dela den här mappen**, och klicka på **Behörighet**.



7. Välj gruppen **Alla** i **Grupp- eller användarnamn**, välj **Tillåt** i **Ändra** och klicka sedan på **OK**.



8. Klicka på **OK**.

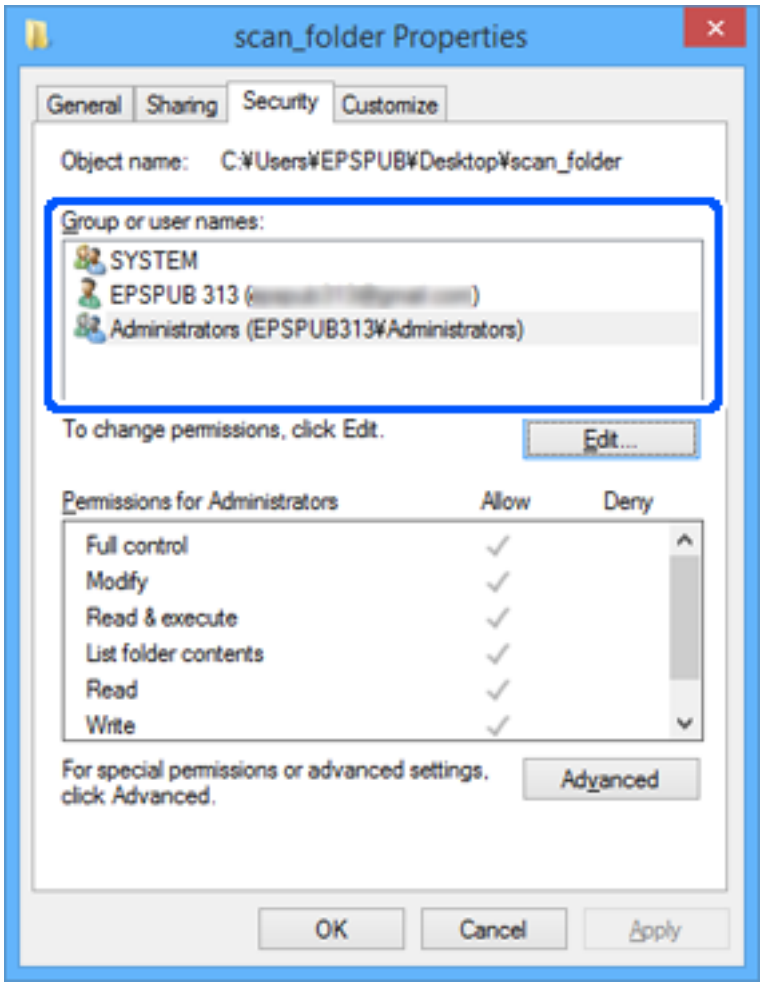
9. Välj fliken **Säkerhet**.

10. Kontrollera gruppen eller användaren i **Grupp- eller användarnamn**.

    Gruppen eller användaren som visas här kan få åtkomst till den delade mappen.

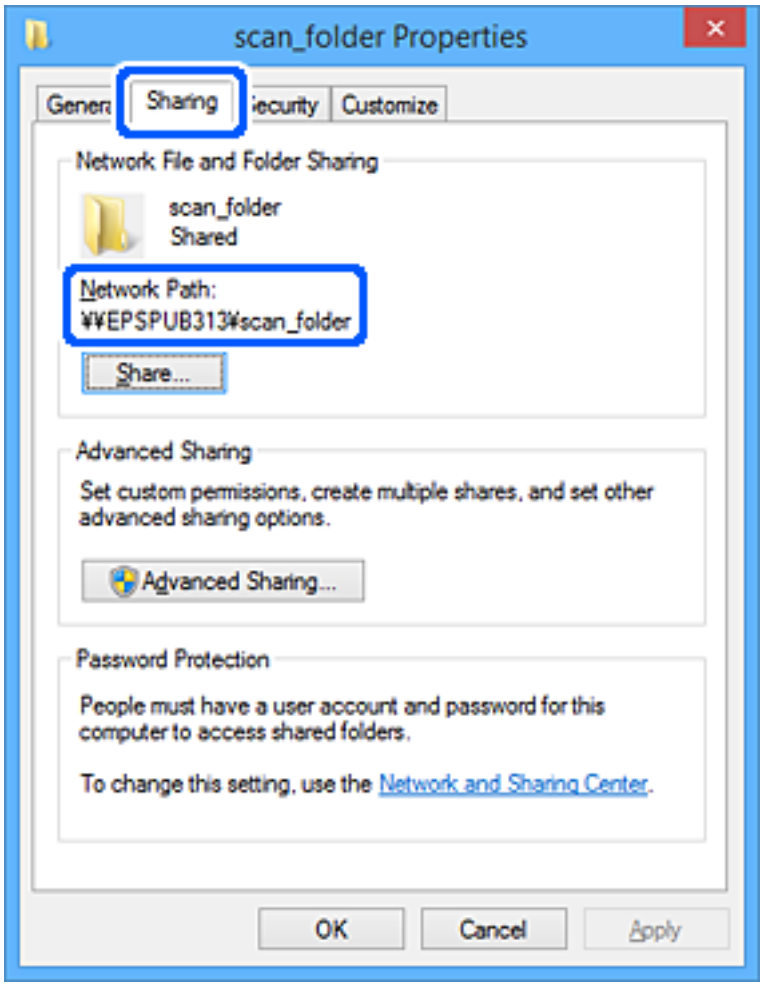
    I det här fallet kan användaren som loggar in på den här datorn och administraötren få åtkomst till den delade mappen.

    Lägg till åtkomstbehörigheten vid behov. Du kan lägga till genom att klicka på **Redigera**. För mer information, se Relaterad information.



11. Välj fliken **Delning**.

    Den delade mappens nätverksväg visas. Det här används vid registrering i skannerns kontaktlista. Skriv ned den.



12. Klicka på **OK** eller **Stäng** för att stänga skärmen.

    Kontrollera om filen kan skrivas över eller läsas i den delade mappen från datorer eller användare eller grupper med åtkomstbehörighet.

Relaterad information

➡ ”Lägga till grupp eller användare med behörighetsåtkomst” på sidan 55
➡ ”Registrera en destination i kontakter med Web Config” på sidan 60

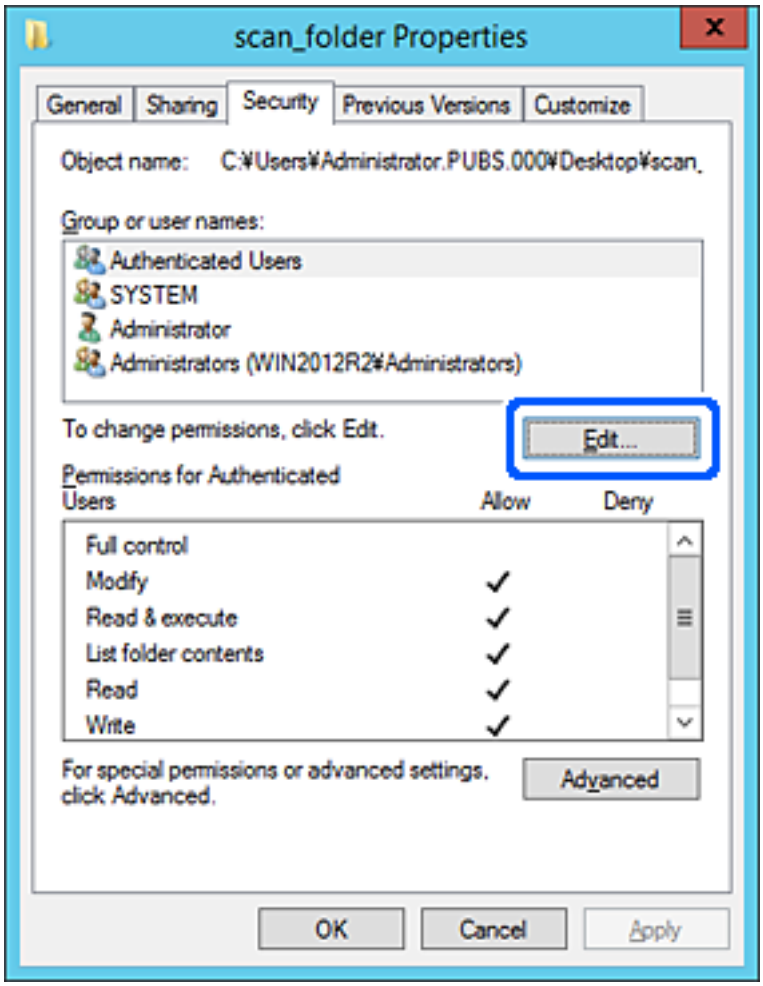
Lägga till grupp eller användare med behörighetsåtkomst

Du kan lägga till gruppen eller användaren med behörighetsåtkomst.

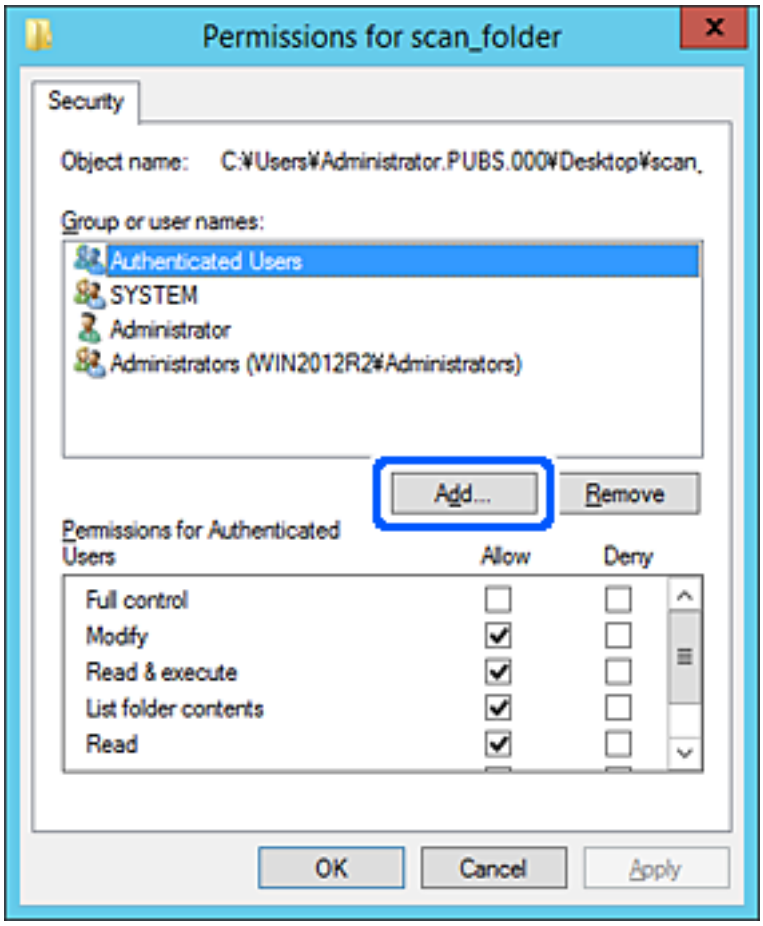
1. Högerklicka på mappen och välj sedan **Egenskaper**.

2. Välj fliken **Säkerhet**.

3. Klicka på **Redigera**.



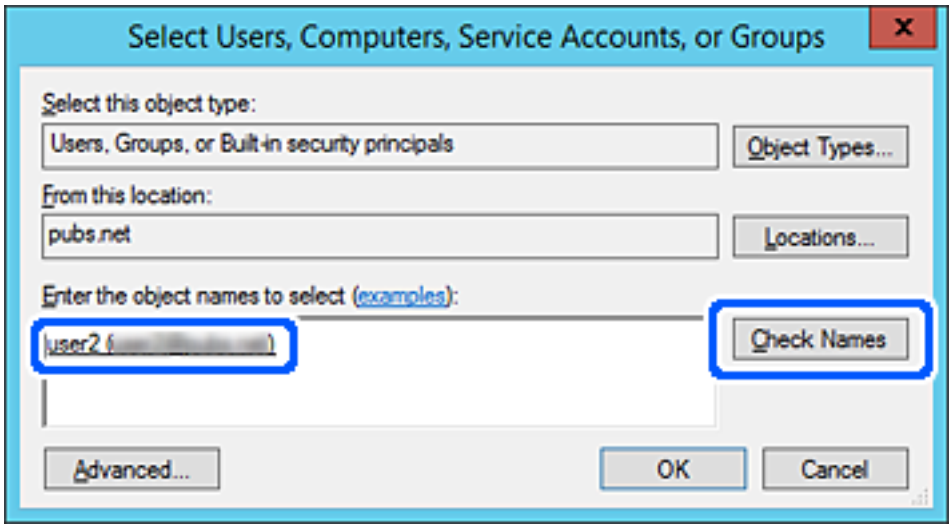
4. Klicka på **Lägg till** under **Gruppnamn eller användarnamn**.



5. Ange grupp- eller användarnamnet som du vill erbjuda åtkomst för, och klicka sedan på **Kontrollera namn**.
   Ett understreck läggs till namnet.

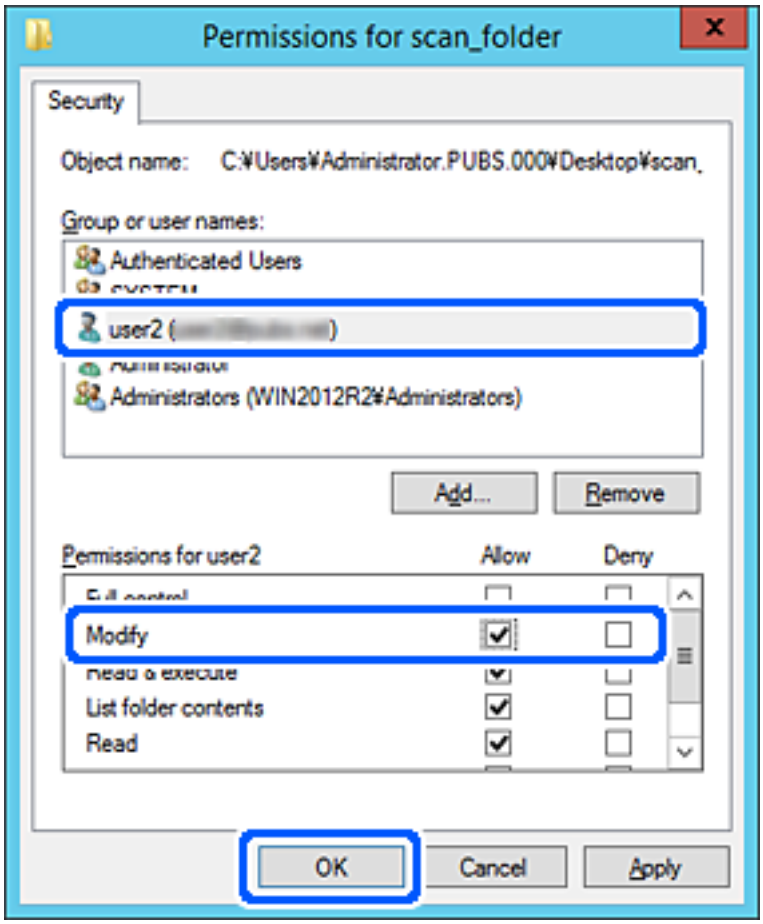
Anmärkning:
Om du inte känner till hela namnet på gruppen eller användaren, ange del av namnet och klicka sedan på ***Kontrollera namn****. Gruppnamn eller användarnamn som matchar delen av namnet som är listat och sedan kan du välja hela namnet från listan.*

Om bara ett namn överensstämmer visas hela namnet med understreck i ***Ange objektnamn att välja****.*



6. Klicka på **OK**.

7. På skärmen Behörighet väljer du användarnamnet som har angetts i **Gruppnamn eller användarnamn**, väljer åtkomstkontrollen i **Ändra**, och klickar sedan på **OK**.



8. Klicka på **OK** eller **Stäng** för att stänga skärmen.

   Kontrollera om filen kan skrivas över eller läsas i den delade mappen från datorer eller användare eller grupper med åtkomstbehörighet.

Göra kontakter tillgängliga

Om du registrerar destinationer i skannerns kontaktlista kan du enkelt ange destinationen när du skannar.

Du kan registrera följande typer av destinationer i kontaktlistan. Du kan registrera upp till 300 poster totalt.

Anmärkning:
Du kan också använda LDAP-servern (LDAP-sökning) för att ange destinationen.

E-post	Destination för e-post. Du måste konfigurera inställningar för e-postservern i förväg.
Nätverksmapp	Destination för skanningsdata. Du måste förbereda nätverksmappen i förväg.

Relaterad information

➡ ”Samarbete mellan LDAP-servrar och användare” på sidan 66

Jämförelse av konfiguration av kontakter

Du kan använda tre verktyg när du konfigurerar skannerns kontakter: Web Config, Epson Device Admin och skannerns kontrollpanel. Skillnaderna mellan de tre verktygen anges i tabellen nedan.

Funktion	Web Config*	Epson Device Admin	Skannerns kontrollpanel
Registrera en destination	✓	✓	✓
Redigera en destination	✓	✓	✓
Lägga till en grupp	✓	✓	✓
Redigera en grupp	✓	✓	✓
Radera en destination eller grupp	✓	✓	✓
Radera alla destinationer	✓	✓	–
Importera en fil	✓	✓	–
Exportera till en fil	✓	✓	–

* Logga in som administratör för att göra inställningar.

Registrera en destination i kontakter med Web Config

Anmärkning:
Du kan också registrera kontakter via skannerns kontrollpanel.

1. Öppna Web Config och välj fliken **Skanna** > **Kontakter**.
2. Välj numret som du vill registrera och klicka sedan på **Redigera**.
3. Ange **Namn** och **Indexord**.
4. Välj destinationsplatsen som **Typ** alternativ.

   Anmärkning:
   *Du kan inte ändra alternativet **Typ** efter att registreringen är klar. Om du vill ändra typen, ta bort destinationen och registrera sedan igen.*
5. Ange värdet för varje alternativ och klicka sedan på **Tillämpa**.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

Alternativ för destinationsinställning

Alternativ	Inställningar och förklaringar
Vanliga inställningar	
Namn	Ange ett namn i kontakterna med 30 tecken eller mindre i Unicode (UTF-8). Om du inte specificerar detta, lämna det tomt.
Indexord	Ange ett namn med högst 30 tecken i Unicode (UTF-8) för att söka i kontakterna på skannerns kontrollpanel. Om du inte specificerar detta, lämna det tomt.
Typ	Välj adresstypen som du vill registrera.
Tilldela till ofta använd	Välj för att ställa in den registrerade adressen som en ofta använd adress. När du ställer in den som en ofta använd adress, visas den överst på skärmen för skanning och du kan specificera destinationen utan att visa kontakterna.
E-post	
E-postadress	Ange mellan 1 och 255 tecken med A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.
Nätverksmapp (SMB)	
Spara till	\\"Mappsökväg" Ange platsen där målmappen är lokaliserad med mellan 1 och 253 tekcen i Unicode (UTF-8), utan "\\". Ange nätverksvägen som visas på mappens egenskapsskärm. Se följande för information om att ställa in nätverksvägen. "Exempel på konfiguration för en dator" på sidan 50
Användarnamn	Ange användarnamn för åtkomst till en nätverksmapp med 30 tecken eller mindre i Unicode (UTF-8). Men undvik att använda styrtecken (0x00 till 0x1F, 0x7F).
Lösenord	Ange lösenord för åtkomst till en nätverksmapp med 20 tecken eller mindre i Unicode (UTF-8). Men undvik att använda styrtecken (0x00 till 0x1F, 0x7F).
FTP	
Säker anslutning	Välj FTP eller FTPS i enlighet med filöverföringsprotokollet som FTP-servern stöder. Välj **FTPS** för att låta skannern kommunicera med säkerhetsåtgärder.
Spara till	Ange servernamnet med mellan 1 och 253 tecken i ASCII (0x20–0x7E), utelämna "ftp://" eller "ftps://".
Användarnamn	Ange användarnamn för åtkomst till en FTP-server med 30 tecken eller mindre i Unicode (UTF-8). Men undvik att använda styrtecken (0x00 till 0x1F, 0x7F). Om servern tillåter anonyma anslutningar, ange ett användarnamn som anonymt och FTP. Om du inte specificerar detta, lämna det tomt.
Lösenord	Ange lösenord för åtkomst till en FTP-server med 20 tecken eller mindre i Unicode (UTF-8). Men undvik att använda styrtecken (0x00 till 0x1F, 0x7F). Om du inte specificerar detta, lämna det tomt.
Anslutningsläge	Välj anslutningsläget från menyn. Om en brandvägg är inställd mellan skannern och FTP-servern ska du välja **Passivt läge**.
Portnummer	Ange FTP-serverportnummer mellan 1 och 65535.

Alternativ	Inställningar och förklaringar
Certifikatverifiering	FTP-serverns certifikat är validerat när detta är aktiverat. Detta är tillgängligt när **FTPS** är valt för **Säker anslutning**. För att konfigurera behöver du importera CA-certifikat till skannern.
SharePoint(WebDAV)	
Säker anslutning	Välj HTTP eller HTTPS i enlighet med filöverföringsprotokollet som-servern stöder. Välj **HTTPS** för att låta skannern kommunicera med säkerhetsåtgärder.
Spara till	Ange servernamnet med mellan 1 och 253 tecken i ASCII (0x20–0x7E), utelämna "http://" eller "https://".
Användarnamn	Ange användarnamn för åtkomst till en server med 30 tecken eller mindre i Unicode (UTF-8). Men undvik att använda styrtecken (0x00 till 0x1F, 0x7F). Om du inte specificerar detta, lämna det tomt.
Lösenord	Ange lösenord för åtkomst till en server med 20 tecken eller mindre i Unicode (UTF-8). Men undvik att använda styrtecken (0x00 till 0x1F, 0x7F). Om du inte specificerar detta, lämna det tomt.
Certifikatverifiering	Serverns certifikat är validerat när detta är aktiverat. Detta är tillgängligt när **HTTPS** är valt för **Säker anslutning**. För att konfigurera behöver du importera CA-certifikat till skannern.
Proxyserver	Välj om en proxyserver ska användas eller inte.

Registrera destinationer som en grupp med Web Config

Om destinationstypen är inställd på **E-post**, kan du registrera destinationerna som en grupp.

1. Öppna Web Config och välj fliken **Skanna** > **Kontakter**.
2. Välj numret som du vill registrera och klicka sedan på **Redigera**.
3. Välj en grupp från **Typ**.
4. Klicka på **Välj** för **Kontakt(er) för Grupp**.
   De tillgängliga destinationerna visas.
5. Välj destinationen som du vill registrera till gruppen och klicka sedan på **Välj**.
6. Ange ett **Namn** och **Indexord**.
7. Välj om du vill tilldela den registrerade gruppen till den ofta använda gruppen eller inte.
   Anmärkning:
   Destinationer kan registreras för flera grupper.
8. Klicka på **Tillämpa**.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

Säkerhetskopiera och importera kontakter

Genom att använda Web Config eller andra verktyg kan du säkerhetskopiera och importera kontakter.

För Web Config kan du säkerhetskopiera kontakter genom att exportera skannerinställningarna som innehåller kontakter. Den exporterade filen kan inte redigeras, eftersom den exporteras som en binär fil.

Vid import av skannerinställningarna till skannern skrivs kontakter över.

För Epson Device Admin kan endast kontakter exporteras från enhetens egenskapsskärm. Om du inte exporterar de säkerhetsrelaterade objekten kan du redigera exporterade kontakter och importera dem, eftersom denna kan sparas som en SYLK-fil eller CSV-fil.

Importera kontakter med Web Config

Om du har en skanner som tillåter dig att säkerhetskopiera kontakter och är kompatibel med denna skanner, kan du registrera kontakter enkelt genom att importera filen med säkerhetskopian.

Anmärkning:
Anvisningar om hur du säkerhetskopierar skannerns kontakter finns i handboken som medföljde skannern.

Följ stegen nedan för att importera kontakter till skannern.

1. Öppna Web Config, välj fliken **Enhetshantering** > **Inställningsvärde för export och import** > **Importera**.
2. Välj filen med säkerhetskopian du skapade i **Fil**, ange lösenordet och klicka sedan på **Nästa**.
3. Markera kryssrutan **Kontakter** och klicka sedan på **Nästa**.

Säkerhetskopiera kontakter med Web Config

Kontaktdata kan förloras på grund av ett skannerfel. Vi rekommenderar att du gör en säkerhetskopia varje gång du uppdaterar data. Epson kan inte hållas ansvarigt för dataförluster, för säkerhetskopior eller återställning av data och/eller inställningar även om garantiperioden fortfarande gäller.

Med Web Config kan du säkerhetskopiera kontaktuppgifter som finns lagrade i skannern till datorn.

1. Öppna Web Config och välj sedan fliken **Enhetshantering** > **Inställningsvärde för export och import** > **Exportera**.
2. Välj **Kontakter**-kryssrutan under kategorin **Skanna**.
3. Ange ett lösenord för att koda den exporterade filen.

   Du behöver ett lösenord för att importera filen. Lämna detta tomt, om du inte vill koda filen.
4. Klicka på **Exportera**.

Export och bulkregistrering av kontakter med verktyget

Om du använder Epson Device Admin, kan du säkerhetskopiera kontakter och redigerade exporterade filer och sedan registrera alla samtidigt.

Detta är praktiskt om du vill säkerhetskopiera kontakter eller när du byter skannern och vill överföra kontakter från den gamla till den nya.

Exportera kontakter

Spara kontaktinformationen i filen.

Du kan redigera filer som sparats i SYLK- eller CSV-format genom att använda kalkylarksapplikationen eller textredigeraren. Du kan registrera alla på en gång efter att du har raderat eller lagt till informationen.

Information som inkluderar säkerhetsalternativ, såsom lösenord och personlig information kan sparas i binärt format med ett lösenord. Du kan inte redigera filen. Denna kan användas som säkerhetskopieringsfil för information som inkluderar säkerhetsobjekt.

1. Starta Epson Device Admin.
2. Välj **Devices** på siduppgiftsmenyn.
3. Välj enheten du vill konfigurera från enhetslistan.
4. Klicka på **Device Configuration** på fliken **Home** i menyn.

   När administratörslösenordet har konfigurerats anger du lösenordet och klickar på **OK**.
5. Klicka på **Common** > **Contacts**.
6. Välj exportformat från **Export** > **Export items**.
   - ❏ All Items

     Exportera den krypterade binära filen. Välj när du vill inkludera säkerhetsalternativ, såsom lösenord och personlig information. Du kan inte redigera filen. Om du väljer den måste du konfigurera lösenordet. Klicka på **Configuration** och konfigurera ett lösenord med mellan 8 och 63 tecken i ASCII. Det här lösenordet krävs vid import av den binära filen.
   - ❏ Items except Security Information

     Exportera filer i SYLK- eller CSV-format. Välj när du vill redigera informationen i den exporterade filen.
7. Klicka på **Export**.
8. Specificera platsen där du vill spara filen, välj filtyp och klicka sedan på **Save**.

   Ett meddelande om slutförande visas.
9. Klicka på **OK**.

   Kontrollera att filen sparats på den angivna platsen.

Importera kontakter

Importera kontaktinformationen från filen.

Du kan importera de filer som sparats i SYLK- eller csv-format eller den säkerhetskopierade binära filen som inkluderar säkerhetsobjekten.

1. Starta Epson Device Admin.
2. Välj **Devices** på siduppgiftsmenyn.
3. Välj enheten du vill konfigurera från enhetslistan.
4. Klicka på **Device Configuration** på fliken **Home** i menyn.

   När administratörslösenordet har konfigurerats anger du lösenordet och klickar på **OK**.
5. Klicka på **Common** > **Contacts**.
6. Klicka på **Browse** på **Import**.
7. Välj de filen som du vill importera och klicka på **Open**.

   När du väljer den binära filen i **Password** anger du lösenordet du konfigurerar vid export av filen.
8. Klicka på **Import**.

   Bekräftelseskärmen visas.
9. Klicka på **OK**.

   Valideringsresultatet visas.

   ❏ Edit the information read

   Klicka när du vill redigera informationen individuellt.

   ❏ Read more file

   Klicka när du vill importera flera filer.
10. Klicka på **Import**, och sedan på **OK** på importslutförandeskärmen.

    Återgå till enhetens egenskapsskärm.
11. Klicka på **Transmit**.
12. Klicka på **OK** i bekräftelsemeddelandet.

    Inställningarna skickas till skannern.
13. På skärmen för slutförande av sändning klickar du på **OK**.

    Skannerns information uppdateras.

    Öppna kontakter från Web Config eller på skannerns kontrollpanel och kontrollera sedan att kontakten uppdateras.

Samarbete mellan LDAP-servrar och användare

Vid samarbete med LDAP-servern, kan du använda adressinformationen som registrerats på LDAP-servern som mål för en e-postadress.

Konfigurera en LDAP-server

För att använda LDAP-serverinformation, registrerar du den på skannern.

1. Öppna Web Config och välj fliken **Nätverk** > **LDAP-server** > **Grundläggande**.
2. Ange ett värde för varje alternativ.
3. Välj **OK**.

   Inställningarna du har valt visas.

Inställningsalternativ för LDAP-server

Alternativ	Inställningar och förklaringar
Använd LDAP-server	Välj **Använd** eller **Använd inte**.
LDAP-serveradress	Ange LDAP-servers adress. Ange mellan 1 och 255 tecken med IPv4-, IPv6- eller FQDN-format. Med formatet FQDN kan du använda alfanumeriska tecken i ASCII (0x20–0x7E) och "-" utom i början och slutet av adressen.
Portnummer för LDAP-server	Ange LDAP-servers portnummer mellan 1 och 65535.
Säker anslutning	Ange autentiseringsmetoden när skannern öppnar LDAP-servern.
Certifikatverifiering	När det här alternativet är aktiverat valideras certifikatet för LDAP-servern. Vi rekommenderar att detta är satt till **Aktivera**. För att utföra konfigurationen behöver **CA-certifikat** importeras till skannern.
Söktimeout (sek)	Ställ in tidslängden för sökning mellan 5 och 300 innan det kommer till timeout.
Autentiseringsmetod	Välj en av metoderna. Om du väljer **Kerberos-autentisering**, välj **Kerberosinställningar** för att göra inställningar för Kerberos. För att utföra Kerberos-autentisering, krävs följande miljö. ❏ Skannern och DNS-servern kan kommunicera. ❏ Tiden för skannern, KDC-servern och servern som krävs för autentisering (LDAP-server, SMTP-server, filserver) synkroniseras. ❏ När tjänsteservern tilldelas som IP-adress registreras FQDN för tjänsteservern på den omvända sökzonen för DNS-servern.
Kerberos-resurs som ska användas	Om du väljer **Kerberos-autentisering** för **Autentiseringsmetod**, välj den Kerberos-sfär som du vill använda.
Administratörs-DN / Användarnamn	Ange användarnamnet för LDAP-servern med 128 tecken eller mindre i Unicode (UTF-8). Du kan inte använda kontrolltecken som 0x00–0x1F och 0x7F. Denna inställning används inte när **Anonym autentisering** är vald som **Autentiseringsmetod**. Om du inte specificerar detta, lämna det tomt.

Alternativ	Inställningar och förklaringar
Lösenord	Ange lösenorden för LDAP-serverautentisering med 128 tecken eller mindre i Unicode (UTF-8). Du kan inte använda kontrolltecken som 0x00–0x1F och 0x7F. Denna inställning används inte när **Anonym autentisering** är vald som **Autentiseringsmetod**. Om du inte specificerar detta, lämna det tomt.

Inställningar för Kerberos

Om du väljer **Kerberos-autentisering** för **Autentiseringsmetod** för **LDAP-server** > **Grundläggande**, ska du göra följande Kerberos-inställningar från fliken **Nätverk** > **Kerberosinställningar**. Du kan registrera upp till 10 inställningar för Kerberos.

Alternativ	Inställningar och förklaringar
Resurs (domän)	Ange sfären för Kerberos-autentisering med max 255 tecken i ASCII (0x20–0x7E). Om du inte registrerar detta, lämna det tomt.
KDC-adress	Ange adressen på Kerberos-autentiseringsservern. Ange 255 tecker eller mindre antingen i IPv4-, IPv6- eller FQDN-format. Om du inte registrerar detta, lämna det tomt.
Portnummer (Kerberos)	Ange Kerberos-servers portnummer mellan 1 och 65535.

Konfigurera sökinställningar för en LDAP-server

När du konfigurerar sökinställningarna kan du använda e-postadressen som registrerats på LDAP-servern.

1. Öppna Web Config och välj fliken **Nätverk** > **LDAP-server** > **Sökinställningar**.
2. Ange ett värde för varje alternativ.
3. Klicka på **OK** för att visa inställningsresultat.

   Inställningarna du har valt visas.

Inställningsalternativ för LDAP-serversökning

Alternativ	Inställningar och förklaringar
Sökbas (unikt namn)	Om du vill söka en godtycklig domän ska du ange LDAP-serverns domännamn. Ange mellan 0 och 128 tecken i Unicode (UTF-8). Om du inte söker för egenmäktig attribut, lämna detta tomt. Exempel på den lokala serverkatalogen: dc=server,dc=local
Antal sökposter	Specificera antalet sökposter mellan 5 och 500. Det specificerade antalet sökposter har sparats och visas temporärt. Även om antalet sökposter överskrider det specificerade antalet och ett felmeddelande visas, kan sökningen slutföras.
Användarattribut	Specificera attributnamnet som skall visas när du söker efter användarnamn. Ange mellan 1 och 255 tecken i Unicode (UTF-8). Det första tecknet skall vara a–z eller A–Z. Exempel: cn, uid

Alternativ	Inställningar och förklaringar
Visning av användarattribut	Specificera attributnamnet som skall visas som användarnamn. Ange mellan 0 och 255 tecken i Unicode (UTF-8). Det första tecknet skall vara a–z eller A–Z. Exempel: cn, sn
E-postadressattribut	Specificera attributnamnet som skall visas när du söker efter e-postadresser. Ange en kombination mellan 1 och 255 tecken med A–Z, a–z, 0–9 och -. Det första tecknet skall vara a–z eller A–Z. Exempel: mail
Godtyckligt attribut 1 - Godtyckligt attribut 4	Du kan specificera andra egenmäktiga attribut att söka efter. Ange mellan 0 och 255 tecken i Unicode (UTF-8). Det första tecknet bör vara a–z eller A–Z. Lämna det tomt om du inte vill söka efter godtyckliga attribut. Exempel: o, ou

Kontrollera LDAP-serverns anslutning

Utför anslutningstestet till LDAP-servern genom att använda parameteruppsättningen på **LDAP-server** > **Sökinställningar**.

1. Öppna Web Config och välj fliken **Nätverk** > **LDAP-server** > **Anslutningstest**.
2. Välj **Starta**.

   Anslutningstestet startades. Efter testet, kontrollera rapporten som visas.

Referens för anslutningstest av LDAP-server

Meddelanden	Förklaring
Anslutningstest lyckades.	Detta meddelande visas när anslutningen till servern lyckades.
Anslutningstest misslyckades. Kontrollera inställningarna.	Detta meddelande visas av följande orsaker: ❏ LDAP-serverns adress eller portnummer är fel. ❏ Det kom till en timeout. ❏ **Använd inte** är vald som **Använd LDAP-server**. ❏ Om **Kerberos-autentisering** är vald som **Autentiseringsmetod** är inställningar som **Resurs (domän)**, **KDC-adress** och **Portnummer (Kerberos)** fel.
Anslutningstest misslyckades. Kontrollera Datum och tid på din produkt eller server.	Detta meddelande visas när anslutningen misslyckas eftersom tidsinställningarna för skannern och LDAP-servern inte matchar varandra.
Autentisering misslyckades. Kontrollera inställningarna.	Detta meddelande visas av följande orsaker: ❏ **Användarnamn** och/eller **Lösenord** är fel. ❏ Om **Kerberos-autentisering** är vald som **Autentiseringsmetod**, tiden/datumen kan inte konfigureras.
Det går inte att komma åt produkten förrän bearbetningen är klar.	Detta meddelande visas när skannern är upptagen.

Att använda Document Capture Pro Server

Genom att använda Document Capture Pro Server, kan du hantera sorteringsmetoden, sparandeformat och vidarebefordringsmål för ett skanningresultat som körs från skannerns kontrollpanel. Du kan ringa och köra ett jobb som tidigare registrerats på servern via skannerns kontrollpanel.

Installera den på datorn som är ansluten till servern.

Kontakta din lokala Epson-återförsäljare för mer information om Document Capture Pro Server.

Konfigurera serverläge

För att använda Document Capture Pro Server, utför du installationen enligt följande.

1. Öppna Web Config och välj fliken **Skanna** > **Document Capture Pro**.
2. Välj **Serverläge** för **Läge**.
3. Skriv in serveradressen med Document Capture Pro Server installerat på den för **Serveradress**.

   Ange mellan 2 och 255 tecken med IPv4-, IPv6-, värdnamns- eller FQDN-format. Med formatet FQDN kan du använda alfanumeriska tecken i ASCII (0x20–0x7E) och ”-” utom i början och slutet av adressen.
4. Klicka på **OK**.

   Nätverket kopplas upp på nytt och inställningarna aktiveras.

Konfiguration av AirPrint

Öppna fliken Web Config, välj **Nätverk** och välj sedan **AirPrint-inställning**.

Alternativ	Förklaring
Tjänstenamn f. Bonjour	Ange ett Bonjour-tjänstenamn, med ASCII-text (0x20–0x7E) och upp till 41 tecken.
Plats för Bonjour	Ange en beskrivning av skannerns placering, med Unicode (UTF-8) text och upp till 127 byte.
Wide-Area Bonjour	Ange om du vill använda Wide-Area Bonjour eller inte. Om du använder skannern måste skrivare registreras på DNS-servern för att kunna söka skrivaren över segmentet.
Aktivera AirPrint	Bonjour och AirPrint (Skanningtjänst) är aktiverade.

Problem vid förberedelse av nätverksskanning

Tips för att lösa problem

❏ Kontrollera felmeddelandet

När ett fel har uppstått ska du först kontrollera om det finns några meddelanden på skannern kontrollpanel eller drivrutinsskärmen. Om du har e-postinställningar för meddelanden när händelsen inträffar kan du snabbt få information om statusen.

❏ Kontrollera kommunikationens status

Kontrollera kommunikationsstatus för serverdatorn eller klientdatorn genom att använda kommando såsom ping och ipconfig.

❏ Anslutningstest

Kontrollera anslutningen mellan skannern och mejlservern genom att använda anslutningstestet på skannern. Kontrollera även anslutningen från klientdatorn till servern för att se kommunikationsstatus.

❏ Initiera inställningarna

Om inställningar och kommunikationsstatus inte uppvisar några problem kan problemen lösas genom att inaktivera eller återställa nätverksinställningarna för skannern och sedan konfigurera på nytt.

Kan inte komma åt Web Config

IP-adressen har inte tilldelats till skannern.

Lösningar

En giltig IP-adress kanske inte tilldelas till skannern. Konfigurera IP-adressen med skannerns kontrollpanel. Du kan kontrollera de aktuella inställningarna via skannerns kontrollpanel.

Webbläsaren stöder inte kodningsstyrkan för SSL/TLS.

Lösningar

SSL/TLS har Krypteringsstyrka. Du kan öppna Web Config via en webbläsare som stöder bulkkodningar enligt nedan. Kontrollera att du användaren den webbläsare som stöds.

❏ 80 bitar: AES256/AES128/3DES

❏ 112 bitar: AES256/AES128/3DES

❏ 128 bitar: AES256/AES128

❏ 192 bitar: AES256

❏ 256 bitar: AES256

CA-signerat Certifikat har gått ut.

Lösningar

Om det finns ett problem med certifikatets utgångsdatum visas meddelandet ”Certifikatet har gått ut” vid anslutning till Web Config med SSL/TLS-kommunikation (https). Om meddelandet visas före utgångsdatumet ska du kontrollera att skannerns datum har ställts in korrekt.

Det gemensamma namnet för certifikatet och skannern överensstämmer inte.

Lösningar

Om det gemensamma namnet för certifikatet och skannern inte överensstämmer visas meddelandet ”Namnet på säkerhetscertifikatet överensstämmer inte …” vid åtkomst till Web Config med SSL/TLS-kommunikation (https). Detta händer på grund av att följande IP-adresser inte överensstämmer.

❏ Skannerns IP-adress anges som gemensamt namn för att skapa en Självsignerat certifikat eller CSR

❏ IP-adressen som anges för webbläsaren vid körning av Web Config

För Självsignerat certifikat ska du uppdatera certifikatet.

För CA-signerat Certifikat tar du certifikatet igen för skannern.

Inställningen för proxy-server för den lokala adressen är inte inställd till webbläsaren.

Lösningar

Om skannern är inställd till att använda en proxy-server ska du konfigurera webbläsaren så att den inte ansluter till den lokala adressen via proxy-servern.

❏ Windows:

Välj **Kontrollpanel** > **Nätverk och internet** > **Internetalternativ** > **Anslutningar** > **LAN-inställningar** > **Proxy-server**, och konfigurera sedan proxy-servern för LAN (lokala adresser).

❏ Mac OS:

Välj **Systeminställningar** > **Nätverk** > **Avancerad** > **Proxy-servrar** och registrera sedan den lokala adressen för **Förbigå proxy -inställningar för dessa värdar och domäner**.

Exempel:

192.168.1.*: Lokal adress 192.168.1.XXX, nätmask 255.255.255.0

192.168.*.*: Lokal adress 192.168.XXX.XXX, nätmask 255.255.0.0

DHCP är inaktiverat i datorns inställningar.

Lösningar

Om DHCP för att få en IP-adress automatiskt är inaktiverad på datorn kan du inte komma åt Web Config. Aktivera DHCP.

Exempel för Windows 10:

Öppna Kontrollpanelen och klicka sedan > **Nätverk och Internet** > **Nätverks- och delningscenter** > **Ändra adapterinställningar** Öppna skärmen Egenskaper för anslutningen du använder och öppna sedan skärmen egenskaper för **internetprotokoll version 4 (TCP/IPv4)** eller **internetprotokoll version 6 (TCP/IPv6)**. Kontrollera att **Obtain an IP address automatically** är vald på den skärmen som visas.

Anpassa kontrollpanelens skärm

Registrering av Förinställ.

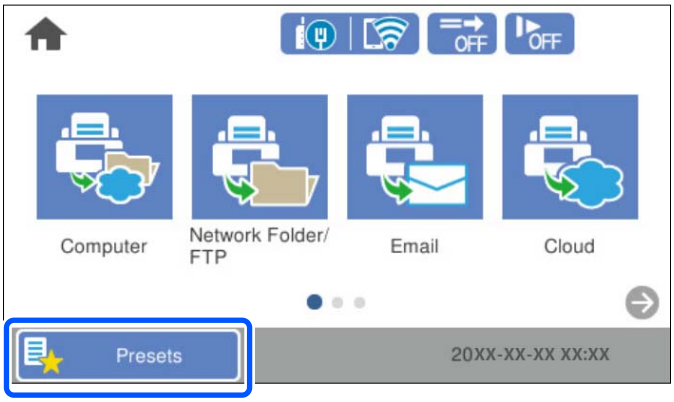
Du kan registrera ofta använda skanningsinställningar som **Förinställ.**. Du kan registrera upp till 48 förinställningar.

Anmärkning:

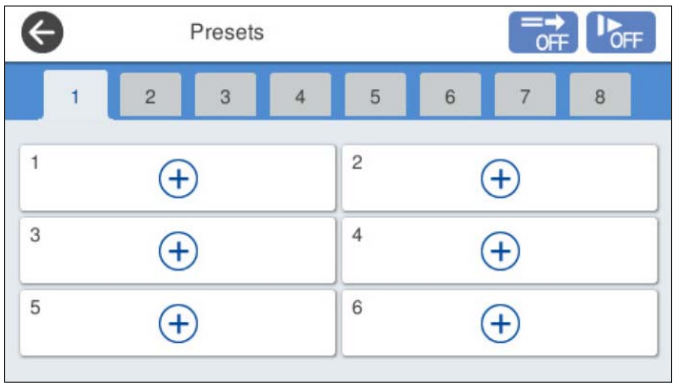
- *Du kan registrera de aktuella inställningarna genom att välja* ☆ *skärmen för att börja skanna.*
- *Du kan också registrera* ***Förinställningar*** *i Web Config.*

  Välj fliken ***Skanna*** *>* ***Förinställningar****.*
- *Om du väljer* ***Skanna till dator*** *vid registrering kan du registrera jobbet skapat i Document Capture Pro som* ***Förinställningar****. Detta är endast tillgängligt för datorer som är anslutna via ett nätverk. Registrera jobbet i Document Capture Pro i förväg.*
- *Om autentiseringsfunktionen är aktiverad kan bara administratören registrera* ***Förinställningar****.*

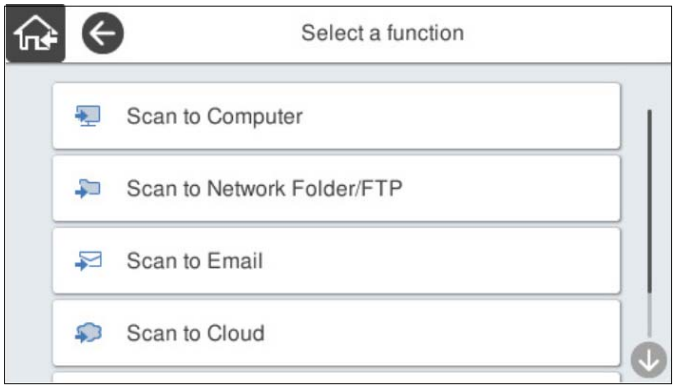
1. Välj **Förinställ.** på startskärmen på skannerns kontrollpanel.



2. Välj ⊕.



3. Välj menyn du vill använda för att registrera en förinställning.



4. Ställ in varje objekt och välj sedan på ☆+.

Anmärkning:
*När du väljer **Skanna till dator**, välj den dator på vilken Document Capture Pro är installerat och välj sedan ett registrerat jobb. Detta är endast tillgängligt för datorer som är anslutna via ett nätverk.*

5. Gör förinställningarna.

- ❏ **Namn**: Ställ in namnet.
- ❏ **Ställ in Ikon**: Ställ in bilden och färgen på ikonen som ska visas.
- ❏ **Snabbskanninginst.**: Börjar omedelbart skanna utan bekräftelse när förinställningen är vald.

  När du använder Document Capture Pro Server, även om du ställer in programvaran för att bekräfta innehållet i jobbet innan du skannar tar **Snabbskanninginst.** på skannerns förinställningar företräde framför programvaran.
- ❏ **Innehåll**: Kontrollera skannerinställningarna.

6. Välj **OK**.

Menyalternativ för Förinställ.

Du kan ändra inställningarna för en förinställning genom att välja > i varje förinställning.

Ändra Namn:

Ändrar det förinställda namnet.

Ändra Ikon:

Ändrar ikonbilden och färgen på förinställningen.

Snabbskanninginst.:

Börjar omedelbart skanna utan bekräftelse när förinställningen är vald.

Ändra plats:

Ändrar visningsordningen för förinställningarna.

Radera:

Raderar förinställningen.

Lägg till eller ta bort Ikon på Hem:

Lägger till eller tar bort den förinställda ikonen från startskärmen.

Bekräfta Information:

Visa inställningar för en förinställning. Du kan läsa in förinställningen genom att välja **Använd den här inställningen**.

Redigera startskärmen för kontrollpanelen

Du kan anpassa startskärmen genom att välja **Inst.** > **Redigera Hem** på skanners kontrollpanel.

- ❏ Layout: Ändrar visningsmetod för menyikonerna.
  ”Ändrar Layout på startskärmen” på sidan 75
- ❏ Lägg till ikon: Lägger till ikoner till de **Förinställ.** du har ställt in eller återställer ikoner som du tidigare har tagit bort från skärmen.
  ”Lägg till ikon” på sidan 76
- ❏ Ta bort ikon: Tar bort ikonen från startskärmen.
  ”Ta bort ikon” på sidan 77
- ❏ Flytta ikon: Ändrar visningsordningen för ikonerna.
  ”Flytta ikon” på sidan 78
- ❏ Återställ ikonernas standardvisning: Återställer standardvisningsinställningarna för startskärmen.
- ❏ Bakgrund: ändra bakgrundsfärg på startskärmen.

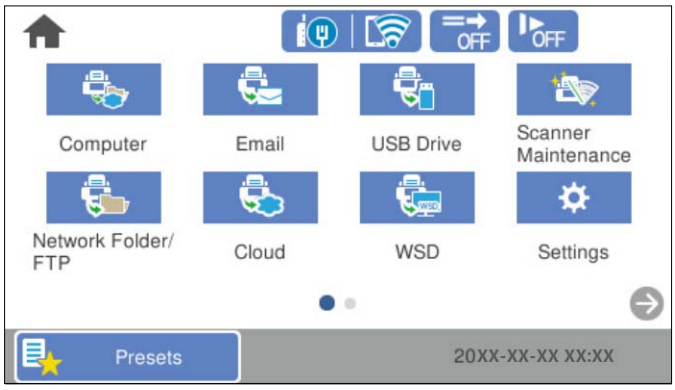
Ändrar Layout på startskärmen

1. Välj **Inst.** > **Redigera Hem** > **Layout** på skannerns kontrollpanel.

2. Välj **Rad** eller **Matris**.

   Rad:

   Matris:



3. Välj för att återgå och kontrollera startskärmen.

Lägg till ikon

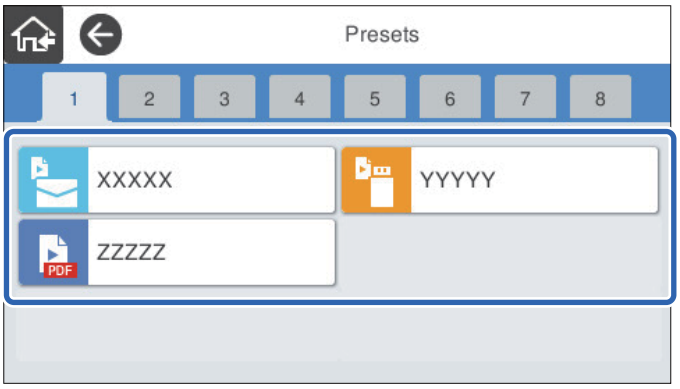
1. Välj **Inst.** > **Redigera Hem** > **Lägg till ikon** på skannerns kontrollpanel.

2. Välj **Funktion** eller **Förinställ.**.

   ❏ Funktion: Visar standardvisningsinställningarna för startskärmen.

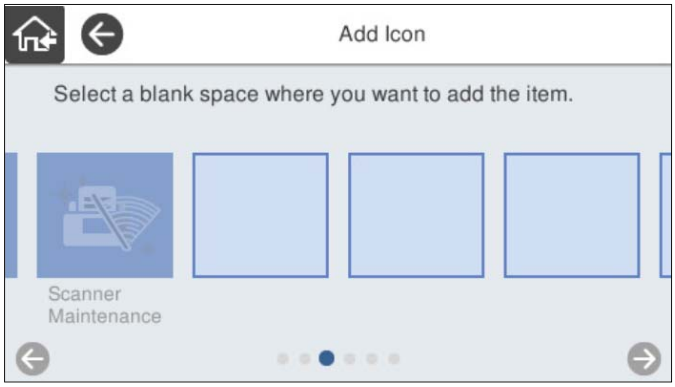
❏ Förinställ.: Visar registrerade förinställningar.

3. Markera det objekt som du vill lägga till på startskärmen.



4. Välj det tomma utrymmet där du vill lägga till objektet.

   Upprepa procedur 3 till 4 om du vill lägga till flera ikoner.

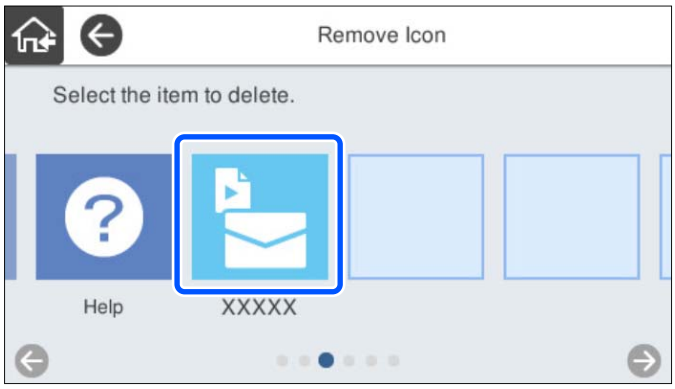


5. Välj för att återgå och kontrollera startskärmen.

Ta bort ikon

1. Välj **Inst.** > **Redigera Hem** > **Ta bort ikon** på skannerns kontrollpanel.

2. Välj ikonen du vill ta bort.



3. Välj **Ja** för att slutföra.

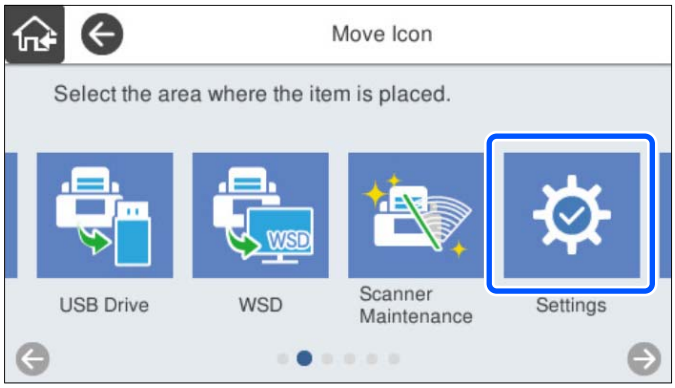
   Upprepa procedur 2 till 3 om du vill ta bort flera ikoner.

4. Välj för att återgå och kontrollera startskärmen.

Flytta ikon

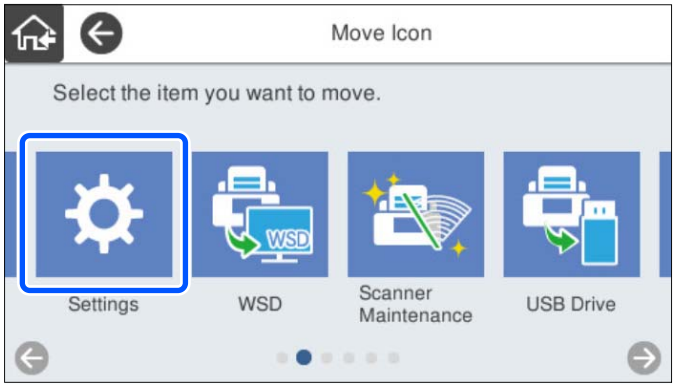
1. Välj **Inst.** > **Redigera Hem** > **Flytta ikon** på skannerns kontrollpanel.

2. Välj ikonen du vill ta flytta.



3. Välj destinationsram.

   Ikonerna ersätts om en annan ikon redan är inställd i destinationsramen.



4. Välj  för att återgå och kontrollera startskärmen.

Grundläggande säkerhetsinställningar

Introduktion till produktens säkerhetsfunktioner

Detta avsnitt ger en introduktion till säkerhetsfunktioner som används i enheter från Epson.

Funktionens namn	Typ av funktion	Att konfigurera	Att förebygga
Konfigurera administratörslösenordet	Låser systeminställningar, såsom anslutningskonfiguration för nätverk eller USB.	Administratören konfigurerar enhetens lösenord. Du kan ställa in och ändra från både Web Config och från skannerns kontrollpanel.	Förhindra olaglig läsning och ändring av information som finns lagrad i enheten, såsom ID, lösenord, nätverksinställningar och så vidare. Minska även många säkerhetsrisker såsom informationsläckor om nätverksmiljön eller säkerhetspolicyn.
Konfigurera extern gränssnitt	Kontrollerar gränssnittet som ansluts till enheten.	Aktivera eller inaktivera USB-anslutning till datorn.	USB-anslutning till dator: Förhindrar obehörig användning av enheten genom att förbjuda skanning utan att gå genom nätverket.

Relaterad information

➡ ”Konfigurera administratörslösenord” på sidan 81
➡ ”Inaktivera externt gränssnitt” på sidan 87

Administratörsinställningar

Konfigurera administratörslösenord

När du konfigurerar administratörslösenordet kan du förhindra användare från att ändra i systemhanteringsinställningarna. Standardvärden är konfigurerade vid tiden för köpet. Ändra dem efter behov.

Anmärkning:
Följande ger standardvärden för administratörsinformationen.

❏ *Användarnamn (används för Web Config): ingen (blank)*

❏ *Lösenord: skannerns serienummer*

För att hitta serienumret, kontrollera etiketten som sitter på baksidan av skannern.

Du kan ställa in och ändra administratörslösenordet med antingen Web Config, skannerns kontrollpanel eller Epson Device Admin. När du använder Epson Device Admin, se Epson Device Admin guide eller hjälp.

Ändra administratörslösenord med Web Config

Ändra administratörslösenordet i Web Config.

1. Öppna Web Config och välj fliken **Produktsäkerhet** > **Ändra Administratörslösenord**.

2. Ange nödvändig information i **Nuvarande lösenord**, **Användarnamn**, **Nytt Lösenord**, och **Bekräfta nytt Lösenord**.

   Ange minst ett tecken för det nya lösenordet.

   Anmärkning:
   Följande ger standardvärden för administratörsinformationen.

   ❏ *Användarnamn: inget (blank)*

   ❏ *Lösenord: skannerns serienummer*

   För att hitta serienumret, kontrollera etiketten som sitter på baksidan av skannern.

   > ***Viktigt:***
   > *Se till att komma ihåg administratörens lösenord som du konfigurerat. Om du glömmer ditt lösenord kan du inte återställa det och du behöver begräa hjälp från servicepersonalen.*

3. Välj **OK**.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

Konfigurera administratörslösenordet från kontrollpanelen

Du kan ändra administratörslösenordet från skannerns kontrollpanel.

1. Välj **Inst.** på skannerns kontrollpanel.
2. Välj **Systemadministration** > **Admin. inställningar**.
3. Välj **Administratörslösenord** > **Ändra**.
4. Ange ditt aktuella lösenord.

   Anmärkning:
   Konfigurationen vid tiden för köpet (standardvärde) för administratörslösenordet är skannerns serienummer.

   För att hitta serienumret, kontrollera etiketten som sitter på baksidan av skannern.

5. Ange det nya lösenordet.

   Ange minst ett tecken.

   > ***Viktigt:***
   > *Se till att komma ihåg administratörens lösenord som du konfigurerat. Om du glömmer ditt lösenord kan du inte återställa det och du behöver begräa hjälp från servicepersonalen.*

6. Ange det nya lösenordet igen som bekräftelse.

Ett meddelande om slutförande visas.

Använda Låsinställning för kontrollpanelen

Du kan använda Låsinställning för att låsa kontrollpanelen för att förhindra användare från att ändra objekt kopplade till systeminställningar.

Anmärkning:
Om du aktiverar Autentiseringsinställningar på skannern, Låsinställning aktiveras det också för kontrollpanelenl. Kontrollpanelen kan inte låsas upp när Autentiseringsinställningar är aktiverad.

Även om du inaktiverar Autentiseringsinställningar, förblir Låsinställning aktiverad. Om du vill inaktivera det kan du göra inställningar från kontrollpanelen eller Web Config.

Konfigurera Låsinställning från kontrollpanelen

1. Om du vill avbryta **Låsinställning** när den har aktiverats trycker du på  längst uppe i högra hörnet på startskärmen för att logga in som en administratör.

    visas inte när **Låsinställning** är aktiverat. Om du inte väljer att aktivera inställningen ska du gå till nästa steg.

2. Välj **Inst.**.

3. Välj **Systemadministration** > **Admin. inställningar**.

4. Välj **På** eller **Av** som **Låsinställning**.

Konfigurera Låsinställning från Web Config

1. Välj fliken **Enhetshantering** > **Kontrollpanel**.

2. Välj **På** eller **Av** för **Panellås**.

3. Klicka på **OK**.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

Låsinställning objekt på menyn Inst.

Detta är en lista över objekt som är låsta i menyn **Inst.** på kontrollpanelen med Låsinställning.

✓ = Som ska låsas.

- = Som inte ska låsas.

Menyn Inst.	Låsinställning
Grundl. inställn.	-

Menyn Inst.		**Låsinställning**
	LCD-ljusstyrka	-
	Ljud	-
	Sömntimer	✓
	Avstängningstimer	✓
	Datum-/tidsinställningar	✓
	Språk/Language	✓/-*
	Tangentbord (Den här funktionen är kanske inte tillgänglig beroende på din region.)	-
	Åtgärden avbröts	✓
	PC Anslutning via USB	✓
	Snabbstart	✓
Skannerinställningar		-
	Långsam	-
	Stannatiming vid dubbelmatning	✓
	DFDS-funktion	-
	Pappersskydd	✓
	Dammskydd av glas	✓
	Ultraljudsidentifiering av dubbelmatn.	✓
	Automatiskt matningsläge överskred tidsgränsen	✓
	Bekräfta mottagare	✓
Redigera Hem		✓
	Layout	✓
	Lägg till ikon	✓
	Ta bort ikon	✓
	Flytta ikon	✓
	Återställ ikonernas standardvisning	✓
	Bakgrund	✓
Användarinställningar		✓
	Nätverksmapp/FTP	✓
	E-post	✓
	Moln	✓
	USB-enhet	✓

Menyn Inst.		**Låsinställning**
Nätverksinställningar		✓
	Inställning av Wi-Fi	✓
	Konfiguration av trådbundet LAN	✓
	Nätverksstatus	✓
	Avancerat	✓
Inställningar för webbtjänst		✓
	Epson Connect-tjänster	✓
Document Capture Pro		-
	Ändra inställningar	✓
Kontakter-hanterare		-
	Registrera/Radera	✓/-*
	Ofta	-
	Visa alternativ	-
	Sökalternativ	-
Systemadministration		✓
	Kontakter-hanterare	✓
	Admin. inställningar	✓
	Begränsningar	✓
	Lösenordskryptering	✓
	Kundundersökning	✓
	WSD-inställningar	✓
	Återställ inställningarna	✓
	Uppdatering av fast programvara	✓
Enhetsinformation		-

Menyn Inst.			**Låsinställning**
	Serienummer		-
	Nuvarande version		-
	Totalt antal skanningar		-
	Antal 1-sidiga skanningar		-
	Antal 2-sidiga skanningar		-
	Antal skanningar av Bärarark		-
	Antalet skan. efter byte av underhållsvals		-
	Antalet skan. efter Regelbunden rengöring		-
	Återställ antal skanningar		✓
Underhåll av skanner			-
	Rengöring av rulle		-
	Byte av underhållsvals		-
		Återställ antal skanningar	✓
		Byta ut	-
	Regelbunden rengöring		-
		Återställ antal skanningar	✓
		Rengöring	-
	Glas-rengöring		-
Inställning för larm om byte av vals			✓
	Inställ. för antal larm		✓
Larminställningar för regelbunden rengöring			✓
	Inställningar för varningslarm		✓
	Inställ. för antal larm		✓

* Du kan ange om du vill tillåta utskrift från **Systemadministration** > **Begränsningar**.

Logga in som en administratör från kontrollpanelen

Du kan använda följande metoder för att logga in som administratör från skannerns kontrollpanel.

1. Tryck på  uppe till höger på skärmen.
   - ❏ När Autentiseringsinställningar är aktiverad visas ikonen på skärmen **Välkommen** (autentiseringsstandby-skärm).
   - ❏ När Autentiseringsinställningar inaktiveras visas ikonen på hemskärmen.

2. Tryck på **Ja** när bekräftelseskärmen visas.

3. Ange administratörslösenordet.

   Ett komplett inloggningsmeddelande visas och sedan visas hemskärmen på kontrollpanelen.

Tryck på  uppe till höger på hemskärmen för att logga ut.

Inaktivera externt gränssnitt

Du kan inaktivera gränssnittet som används till att ansluta enheten till skannern. Ställ in begränsningen för att begränsa andra skanningsjobb än de som görs via nätverket.

Anmärkning:
Du kan också utföra inställningar för begränsning via skannerns kontrollpanel.

PC Anslutning via USB: ***Inst.*** *>* ***Grundl. inställn.*** *>* ***PC Anslutning via USB***

1. Öppna Web Config och välj fliken **Produktsäkerhet** > **Externt gränssnitt**.

2. Välj **Inaktivera** för de funktioner som du vill ställa in.

   Välj **Aktivera** om du inte längre vill kontrollera.

   PC Anslutning via USB

   Du kan hindra användning av USB-anslutningen från datorn. Om du vill hindra den väljer du **Inaktivera**.

3. Klicka på **OK**.

4. Kontrollera att den inaktiverade porten inte kan användas.

   PC Anslutning via USB

   Om drivrutinen har installerats på datorn

   Anslut skannern till datorn med en USB-kabel och bekräfta sedan att skannern inte skannrar.

   Om drivrutinen inte har installerats på datorn

   Windows:

   Öppna enhetshanteraren och behåll den, anslut skannern till datorn med en USB-kabel och bekräfta sedan att enhetshanterarens displayinnehåll förblir oförändrat.

   Mac OS:

   Anslut skannern till datorn med en USB-kabel och bekräfta sedan att du inte kan lägga till skannern **Skrivare och skannrar**.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

Övervaka en fjärrskanner

Kontrollerar information för en fjärrskanner

Du kan kontrollera följande information om skannern som används från **Status** med hjälp av Web Config.

❏ Produktstatus

Kontrollera status, molntjänst, produktnummer, MAC-adress etc.

❏ Nätverksstatus

Kontrollera informationen för nätverksanslutningsstatus, IP-adress, DNS server, etc.

❏ Användningsstatus

Kontrollera den första dagen för skanning, antal skanningsjobb etc.

❏ Hårdvarustatus

Kontrollera statusen för varje funktion på skannern.

❏ Panel stillbild

Visar en stillbild av skärmen som visas på skannerns kontrollpanel.

Ta emot e-postmeddelanden när händelser inträffar

Om e-postaviseringar

Det här är en aviseringsfunktion som, när händelser, såsom skanningstopp och skannerfel uppstår, skickar e-post till den specificerade adressen.

Du kan registrera upp till fem mål och konfigurera meddelandeinställningar för varje mål.

För att använda den här funktionen behöver du konfigurera mejlservern innan du konfigurerar meddelanden.

Relaterad information

➡ ”Konfigurera en e-postserver” på sidan 40

Konfigurera e-postavisering

Konfigurera e-postmeddelande genom att använda Web Config.

1. Öppna Web Config och välj fliken **Enhetshantering** > **E-postavisering**.
2. Konfigurera ämne för e-postbekräftelsen.

   Markera innehåll som visas för ämnet på de båda menyerna.

   ❏ Det valda innehållet visas intill **Ämne**.

   ❏ Samma innehåll kan inte konfigureras på vänster och höger sida.

   ❏ När antalet tecken i **Plats** överskrider 32 byte, nonchaleras tecken som överskrider 32 byte.

3. Ange e-postadress för sändning av e-postavisering.

   Använd A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @, och uppge mellan 1 och 255 tecken.

4. Välj språk för e-postaviseringar.

5. Markera kryssrutan för händelsen du vill få en avisering för.

   Numret för **Aviseringsinställningar** länkas till målnumret för **Inställningar för e-postadress**.

   Exempel:

   Om du vill ha en avisering skickad till e-postadressen du har konfigurerat för nummer 1 i **Inställningar för e-postadress** när administratörslösenordet har ändrats, markerar du kryssrutan i kolumn **1** på rad **Administratörslösenord ändrat**.

6. Klicka på **OK**.

   Kontrollera att en e-postbekräftelse skickas genom att orsaka en händelse.

   Exempel: Administratörslösenordet har ändrats.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

Alternativ för e-postaviseringar

Alternativ	Inställningar och förklaringar
Administratörslösenord ändrat	Avisera när administratörslösenordet har ändrats.
Skannerfel	Avisera om det uppstår ett skannerfel.
Wi-Fi-fel	Meddelande när felet i det trådlösa nätverksgränssnittet har uppstått.

Lösa problem

Har du glömt ditt administratörslösenord

Du behöver hjälp av servicepersonal. Kontakta din lokala återförsäljare.

Anmärkning:
Följande ger de initiala värdena för Web Config-administratören.

❏ *Användarnamn: inget (blank)*

❏ *Lösenord: skannerns serienummer*

För att hitta serienumret, kontrollera etiketten som sitter på baksidan av skannern. Om du återställer standardinställningarna för administratörslösenordet återställs det till de ursprungliga värdena.

Avancerade säkerhetsinställningar

Säkerhetsinställningar och förebyggande av fara

När en skanner är ansluten till ett nätverk kan du öppna den från en fjärrstyrd plats. Dessutom kan många människor dela skannern, vilket är praktiskt vid förbättring av operationell effektivitet och bekvämlighet. Risker, såsom olaglig åtkomst, olaglig användning och modifiering av data ökar. Om du använder skannern i en miljö där du kan få åtkomst till Internet är riskerna ännu högre.

För skannrar som inte har åtkomstskydd utifrån går det att läsa kontakter som lagras i skannern från Internet.

För att undvika den här risken har Epson-skannrar en rad olika säkerhetstekniker.

Konfigurera skannern efter behov enligt miljövillkoren som har byggts in i kundens miljöinformation.

Namn	Typ av funktion	Att konfigurera	Att förebygga
Kontroll av protokoll	Kontrollerar protokollen och tjänsterna som ska användas för kommunikation mellan skannrar och datorer, och aktiverar och inaktiverar funktioner.	Ett protokoll eller en tjänst som verkställs för funktioner tillåts eller förbjuds separat.	Genom att minska säkerhetsrisker som kan uppstå vid oavsiktlig användning där användare förhindras från att använda onödiga funktioner.
SSL/TLS-kommunikation	Kommunikationsinnehållet krypteras med SSL/TLS-kommunikationer vid åtkomst till Epson-servern på Internet från skannern, såsom kommunikation med datorn via webbläsaren, med Epson Connect, och firmware-uppdatering.	Få ett CA-signerat certifikat och importera det sedan till skannern.	Genom att rensa en identifiering av skannern med CA-signerad certifiering förhindras impersonifiering och obehörig åtkomst. Dessutom skyddas kommunikationsinnehållet i SSL/TLS och innehållsläckage förhindras för skanningdata och konfigurationsinformation.
IPsec-/IP-filtrering	Du kan göra inställningar för att tillåta beskärning och urklipp av data som kommer från en viss klient eller är av en viss typ. Eftersom IPsec skyddar data via IP-paketenhet (kryptering och autentisering), kan du säkert kommunicera osäkra protokoll.	Skapa en grundläggande policy och individuell policy för att konfigurera klienten eller typen av data som kan få åtkomst till skannern.	Skydda från obehörig åtkomst och klåfingerskydd och störning av kommunikationsdata till skannern.
IEEE 802.1X	Låter endast autentiserade användare att ansluta till nätverket. Tillåter bara en behörig användare att använda skannern.	Autentiseringsinställningar för RADIUS-servern (autentiseringsserver).	Skyddar från obehörig åtkomst och användning av skannern.

Relaterad information

➡ ”Kontrollera med protokoll” på sidan 92

➡ ”SSL-/TLS-kommunikation med skannern” på sidan 100

➡ ”Krypterad kommunikation med IPsec/IP-filtrering” på sidan 102

➡ ”Ansluta skannern till ett IEEE802.1X-nätverk” på sidan 112

Säkerhetsfunktionsinställningar

När du ställer in IPsec-/IP-filtrering eller IEEE 802.1X, rekommenderas det att du öppnar Web Config med SSL/TLS för att kommunicera inställningsinformation för att minska säkerhetsrisker som manipulation eller avlyssning.

Se till att du konfigurerar administratörslösenordet innan du ställer in IPsec-/IP-filtrering eller IEEE 802.1X.

Kontrollera med protokoll

Du kan skanna med hjälp av ett antal olika vägar och protokoll. Du kan också använda nätverksskanning från ett ospecificerat antal nätverksdatorer.

Du kan sänka oönskade säkerhetsrisker genom att begränsa skanning från särskilda vägar eller genom att kontrollera de tillgängliga funktionerna.

Kontrollera protokoll

Konfigurera protokollinställningarna som stöds av skannern.

1. Öppna Web Config och välj sedan fliken **Nätverkssäkerhet** tab > **Protokoll**.
2. Konfigurera varje punkt.
3. Klicka på **Nästa**.
4. Klicka på **OK**.

   Inställningarna aktiveras på skannern.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

Protokoll som du kan aktivera eller avaktivera

Protokoll	Beskrivning
Bonjour-inställningar	Du kan ange om du vill använda Bonjour. Bonjour används för att söka efter enheter, skanna och så vidare.
SLP-inställningar	Du kan aktivera eller inaktivera SLP-funktionen. SLP används för push-skanning och nätverkssökning i EpsonNet Config.
WSD-inställningar	Du kan aktivera eller inaktivera WSD-funktionen. När den är aktiverad kan du lägga till WSD-enheter, och skanna från WSD-porten.
LLTD-inställningar	Du kan aktivera eller inaktivera LLTD-funktionen. När detta är aktiverat, visas det på Windows nätverkskarta.
LLMNR-inställningar	Du kan aktivera eller inaktivera LLMNR-funktionen. När det är aktiverat kan du använda namnmatchning utan NetBIOS, även om du inte kan använda DNS.

Protokoll	Beskrivning
SNMPv1/v2c-inställningar	Du kan ange om du vill tillåta SNMPv1/v2c. Detta används för att ställa in enheter, övervakning och så vidare.
SNMPv3-inställningar	Du kan ange om du vill tillåta SNMPv3. Detta används för att ställa in krypterade enheter, övervakning och så vidare.

Inställningsalternativ för protokoll

Bonjour-inställningar

Alternativ	Inställningsvärde och beskrivning
Använd Bonjour	Välj det här för att söka efter eller använda enheter via Bonjour.
Bonjour-namn	Visar Bonjour-namn.
Tjänstenamn f. Bonjour	Visar Bonjour-tjänstens namn.
Plats	Visar Bonjour-platsnamn.
Wide-Area Bonjour	Konfigurera om du vill använda Wide-Area Bonjour.

SLP-inställningar

Alternativ	Inställningsvärde och beskrivning
Aktivera SLP	Välj detta för att aktivera SLP-funktionen. Detta används med nätverkssökning i EpsonNet Config.

WSD-inställningar

Alternativ	Inställningsvärde och beskrivning
Aktivera WSD	Välj detta för att aktivera att lägga till enheter med WSD, och skanna från WSD-porten.
Skanningstimeout (sek)	Ange kommunikationstimeout-värde för WSD-skanning mellan 3 till 3 600 sekunder.
Enhetsnamn	Visar WSD enhetsnamn.
Plats	Visar WSD-platsnamn.

LLTD-inställningar

Alternativ	Inställningsvärde och beskrivning
Aktivera LLTD	Välj detta för att möjliggöra LLTD. Skannern visas i Windows nätverkskarta.
Enhetsnamn	Visar LLTD enhetsnamn.

LLMNR-inställningar

Alternativ	Inställningsvärde och beskrivning
Aktivera LLMNR	Välj detta för att möjliggöra LLMNR. Du kan använda namn-matchning utan NetBIOS även om du inte kan använda DNS.

SNMPv1/v2c-inställningar

Alternativ	Inställningsvärde och beskrivning
Aktivera SNMPv1/v2c	Markera för att aktivera SNMPv1/v2c.
Åtkomstbehörighet	Ställ in åtkomstauktoritet när SNMPv1/v2c är aktiverad. Välj **Skrivskyddad** eller **Läs/Skriv**.
Gemenskapsnamn (endast läsa)	Ange 0 till 32 ASCII (0x20 till 0x7E)-tecken.
Gemenskapsnamn (läsa/skriva)	Ange 0 till 32 ASCII (0x20 till 0x7E)-tecken.

SNMPv3-inställningar

Alternativ		Inställningsvärde och beskrivning
Aktivera SNMPv3		SNMPv3 är aktiverad när rutan markerats.
Användarnamn		Ange mellan 1 och 32 tecken med 1 byte mellanslag.
Autentiseringsinställningar		
	Algoritm	Välj en algoritm för autentisering av SNMPv3.
	Lösenord	Ange lösenord för autentisering för SNMPv3. Ange mellan 8 och 32 tecken i ASCII (0x20–0x7E). Om du inte specificerar detta, lämna det tomt.
	Bekräfta lösenord	Ange lösenordet som du konfigurerade som bekräftelse.
Krypteringsinställningar		
	Algoritm	Välj en algoritm för kryptering av SNMPv3.
	Lösenord	Ange lösenord för kryptering för SNMPv3. Ange mellan 8 och 32 tecken i ASCII (0x20–0x7E). Om du inte specificerar detta, lämna det tomt.
	Bekräfta lösenord	Ange lösenordet som du konfigurerade som bekräftelse.
Kontextnamn		Ange max 32 tecken i Unicode (UTF-8). Om du inte specificerar detta, lämna det tomt. Antalet tecken som kan anges varierar beroende på språk.

Använda ett digitalt certifikat

Om digital certifiering

❏ CA-signerat Certifikat

Det här är ett certifikat som signerats av CA (certifikatutfärdare). Du kan ansöka om att få den från Certificate Authority. Det här certifikatet intygar att skannern finns och används för SSL/TLS-kommunikation så att du kan garantera säkerheten i datakommunikationen.

När den används för SSL/TLS-kommunikation, används den som ett servercertifikat.

När den är konfigurerad för IPsec/IP-filtrering eller IEEE 802.1X-kommunikation, används den som ett klientcertifikat.

❏ CA-certifikat

Det här är ett certifikat som ingår i kedjan för CA-signerat Certifikat, även kallat mellanliggande CA-certifikat. Det används av webbläsaren för att validera sökvägen till skannerns certifikat vid åtkomst till servern för den andra parten eller Web Config.

För CA-certifikatet ska du konfigurera när du vill validera sökvägen för servercertifikatet vid åtkomst från skannern. För skannern konfigurerar du om du vill certifiera sökvägen för CA-signerat Certifikat för SSL/TLS-anslutning.

Du kan erhålla CA-certifikatet för skannern från Certification Authority där CA-certifikatet utfärdades.

Du kan också få CA-certifikatet som används för att validera servern för den andra parten från Certification Authority som har utfärdat CA-signerat Certifikat för den andra servern.

❏ Självsignerat certifikat

Det här är ett certifikat som skannern själv signerar och utfärdar. Det kallas även rotcertifikat. Eftersom utfärdaren själv certifierar är den inte tillförlitlig och kan inte förhindra impersonifiering.

Använd den när du gör säkerhetsinställningar och utför enkel SSL/TLS-kommunikation utan CA-signerat Certifikat.

Om du använder detta certifikat för SSL/TLS-kommunikation kan en säkerhetsvarning visas i webbläsaren, eftersom certifikatet inte är registrerat i en webbläsare. Du kan bara använda detta Självsignerat certifikat för SSL/TLS-kommunikation.

Relaterad information

➡ ”Konfigurera ett CA-signerat Certifikat” på sidan 95
➡ ”Uppdatera ett självsignerat certifikat” på sidan 99
➡ ”Konfigurera ett CA-certifikat” på sidan 99

Konfigurera ett CA-signerat Certifikat

Hämta ett CA-signerat certifikat

När du vill hämta ett CA-signerat certifikat ska du skapa en CSR (certifikatsigneringsförfrågan) och använda den för att ansöka hos en certifikatutfärdare. Du kan skapa en CSR med Web Config och en dator.

Följ stegen nedan när du ska skapa en CSR och hämta ett CA-signerat certifikat med Web Config. CSR får formatet PEM/DER när du skapar certifikatet med Web Config.

1. Öppna Web Config och välj fliken **Nätverkssäkerhet**. Välj sedan **SSL/TLS** > **Certifikat** eller **IPsec/IP Filtering** > **Klientcertifikat** eller **IEEE802.1X** > **Klientcertifikat**.

   Oavsett vad du väljer kan du få samma certifikat och använda det gemensamt.

2. Klicka **Generera** för **CSR**.

   En sida där du kan skapa en CSR öppnas.

3. Ange ett värde för varje alternativ.

   Anmärkning:
   Nyckelns längd och förkortningarna varierar beroende på certifikatutfärdaren. Skapa en begäran enligt reglerna för den certifikatutfärdare det gäller.

4. Klicka på **OK**.

   Ett meddelande om slutförande visas.

5. Välj fliken **Nätverkssäkerhet**. Välj sedan **SSL/TLS** > **Certifikat**, eller **IPsec/IP Filtering** > **Klientcertifikat** eller **IEEE802.1X** > **Klientcertifikat**.

6. Klicka på en av hämtningsknapparna för **CSR** beroende på certifikatutfärdarens specificerade format när du vill hämta en CSR till en dator.

   > ***Viktigt:***
   > *Skapa inte ett CSR igen. Om du gör det kanske du inte kan importera ett utfärdat CA-signerat Certifikat.*

7. Skicka ett CSR till en certifikatutfärdare och skaffa ett CA-signerat Certifikat.

   Följ reglerna för de olika certifikatutfärdarna angående sändningsmetod och format.

8. Spara det utfärdade CA-signerat Certifikat på en dator som är ansluten till skannern.

   Hämtningen av det CA-signerat Certifikat är klar när du sparar certifikatet på en måldestination.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

Inställningsalternativ för CSR

Alternativ	Inställningar och förklaringar
Nyckellängd	Välj nyckellängd för CSR.

Alternativ	Inställningar och förklaringar
Nätverksnamn	Du kan uppge mellan 1 och 128 tecken. Om det är en IP-adress ska det vara en statisk IP-adress. Du kan ange 1 till 5 IPv4-adresser, IPv6-adresser, värdnamn, FQDN genom att separera dem med kommatecken. Det första elementet lagras med gemensamt namn, och övriga element lagras i aliasfältet för certifikatsämnet. Exempel: Skannerns IP-adress: 192.0.2.123, skannernamn: EPSONA1B2C3 Nätverksnamn: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
Organisation/ Organisationsenhet/ Plats/ Stat/provins	Du kan ange mellan 0 och 64 tecken i ASCII (0x20–0x7E). Du kan skilja unika namn åt med komman.
Land	Skriv en landskod med ett tvåsiffrigt nummer enligt ISO-3166.
Avsändarens e-postadress	Du kan ange avsändarens e-postadress i inställningen för postserver. Ange samma e-postadress som **Avsändarens e-postadress** för fliken **Nätverk** > **E-postserver** > **Grundläggande**.

Importera ett CA-signerat certifikat

Importera det erhållna CA-signerat Certifikat till skannern.

Viktigt:

❏ *Kontrollera att rätt datum och klockslag är inställt på skannern. Certifikatet kan vara ogiltigt.*

❏ *Om du hämtar ett certifikat med en CSR som skapats i Web Config kan du importera ett certifikat i taget.*

1. Öppna Web Config och välj sedan fliken **Nätverkssäkerhet**. Välj sedan **SSL/TLS** > **Certifikat**, eller **IPsec/IP Filtering** > **Klientcertifikat** eller **IEEE802.1X** > **Klientcertifikat**.

2. Klicka på **Importera**

   En sida där du kan importera öppnas.

3. Ange ett värde för varje alternativ. Konfigurera **CA-certifikat 1** och **CA-certifikat 2** vid verifiering av certifikatet i webbläsaren som får åtkomst till skannern.

   Inställningarna kan variera beroende på var du hämtar en CSR och certifikatets filformat. Ange värden för nödvändiga inställningar enligt följande.

   ❏ Ett certifikat i formatet PEM/DER som hämtats från Web Config

   ❏ **Privat nyckel**: Konfigureras inte eftersom skannern innehåller en privat nyckel.

   ❏ **Lösenord**: Konfigurera inte.

   ❏ **CA-certifikat 1**/**CA-certifikat 2**: Valfritt

   ❏ Ett certifikat i formatet PEM/DER som hämtats från en dator

   ❏ **Privat nyckel**: Måste anges.

   ❏ **Lösenord**: Konfigurera inte.

   ❏ **CA-certifikat 1**/**CA-certifikat 2**: Valfritt

❏ Ett certifikat i formatet PKCS#12 som hämtats från en dator

❏ **Privat nyckel**: Konfigurera inte.

❏ **Lösenord**: Valfritt

❏ **CA-certifikat 1/CA-certifikat 2**: Konfigurera inte.

4. Klicka på **OK**.

   Ett meddelande om slutförande visas.

Anmärkning:
*Verifiera certifikatinformationen genom att klicka på **Bekräfta**.*

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

CA-signerade certifikat att importera inställningsobjekt

Alternativ	Inställningar och förklaringar
Servercertifikat eller Klientcertifikat	Välj ett certifikats format. För SSL/TLS-anslutning visas Servercertifikat. För IPsec-/IP-filtrering eller IEEE 802.1X visas Klientcertifikat.
Privat nyckel	Om du får ett certifikat i PEM-/DER-format med hjälpa av en CSR skapad från en dator, ska du ange en privat nyckelfil som matchar ett certifikat.
Lösenord	Om filformatet är **Certifikat med privat nyckel (PKCS#12)**, anger du lösenordet för att kryptera den privata nyckeln som är inställd när du får certifikatet.
CA-certifikat 1	Om ditt certifikats format är **Certifikat (PEM/DER)** importerar du ett certifikat från en certifikatutfärdare som utfärdar ett CA-signerat Certifikat som används som servercertifikat. Ange en fil om det behövs.
CA-certifikat 2	Om ditt certifikats format är **Certifikat (PEM/DER)** importerar du ett certifikat från en certifikatutfärdare som utfärdar CA-certifikat 1. Ange en fil om det behövs.

Radera ett CA-signerat certifikat

Du kan radera ett importerat certifikat när det har gått ut eller när en krypterad anslutning inte längre behövs.

Viktigt:
Om du hämtar ett certifikat med en CSR som skapats i Web Config kan du inte importera ett certifikat som raderats.I sådana fall ska du skapa en CSR och hämta ett nytt certifikat.

1. Öppna Web Config och välj sedan fliken **Nätverkssäkerhet**.Välj sedan **SSL/TLS** > **Certifikat** eller **IPsec/IP Filtering** > **Klientcertifikat** eller **IEEE802.1X** > **Klientcertifikat**.

2. Klicka på **Radera**.

3. Bekräfta att du vill ta bort certifikatet i meddelandet som visas.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

Uppdatera ett självsignerat certifikat

Eftersom det Självsignerat certifikat utfärdas av skannern kan du uppdatera det när det har löpt ut eller när innehållet som beskrivs ändras.

1. Gå till Web Config och välj fliken **Nätverkssäkerhet** tab > **SSL/TLS** > **Certifikat**.
2. Klicka på **Uppdatera**.
3. Ange **Nätverksnamn**.

   Du kan ange upp till 5 IPv4-adresser, IPv6-adresser, värdnamn, FQDN:er mellan 1 och 128 tecken och separera dem med kommatecken. Den första parametern finns i det gemensamma namnet och de andra lagras i aliasfältet för certifikatets ämne.

   Exempel:

   Skrivarens IP-adress: 192.0.2.123, Skannernamn: EPSONA1B2C3

   Gemensamt namn: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
4. Ange en giltighetsperiod för certifikatet.
5. Klicka på **Nästa**.

   Ett bekräftelsemeddelande visas.
6. Klicka på **OK**.

   Skannern är uppdaterad.

Anmärkning:
*Du kan kontrollera certifikatinformationen i fliken **Nätverkssäkerhet** > **SSL/TLS** > **Certifikat** > **Självsignerat certifikat** och klicka på **Bekräfta**.*

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

Konfigurera ett CA-certifikat

När du konfigurerar CA-certifikat kan du validera sökvägen till CA-certifikatet för servern som skannern har åtkomst till. Detta kan förhindra avpersonifiering.

Du kan få CA-certifikat från Certification Authority där CA-signerat Certifikat utfärdats.

Importera ett CA-certifikat

Importera CA-certifikat till skannern.

1. Öppna Web Config och välj sedan fliken **Nätverkssäkerhet** > **CA-certifikat**.
2. Klicka på **Importera**.
3. Ange det CA-certifikat du vill importera.
4. Klicka på **OK**.

När importen är klar kommer du tillbaka till skärmen **CA-certifikat** och det importerade CA-certifikat visas.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

Ta bort ett CA-certifikat

Du kan ta bort det importerade CA-certifikat.

1. Gå till Web Config och välj sedan fliken **Nätverkssäkerhet** > **CA-certifikat**.
2. Klicka på **Radera** bredvid CA-certifikat som du vill ta bort.
3. Bekräfta att du vill ta bort certifikatet i meddelandet som visas.
4. Klicka på **Starta om nätverk**, och kontrollera sedan att det borttagna CA-certifikatet inte finns på den uppdaterade skärmen.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

SSL-/TLS-kommunikation med skannern

När servercertifikatet är konfigurerat med SSL-/TLS-kommunikation (Secure Sockets Layer/Transport Layer Security) för skannern, kan du kryptera kommunikationssökvägen mellan datorer. Gör detta om du vill förhindra fjärrstyrd åtkomst och obehörig åtkomst.

Konfigurera grundläggande SSL-/TLS-inställningar

Om skannern stöder HTTPS-serverfunktionen kan du använda en SSL-/TLS-kommunikation för att kryptera kommunikation. Du kan konfigurera och hantera skannern med Web Config och samtidigt säkerställa säkerheten.

Konfigurera krypteringsstyrka och omdirigeringsfunktion.

1. Gå till Web Config och välj fliken **Nätverkssäkerhet** > **SSL/TLS** > **Grundläggande**.

2. Ange ett värde för varje objekt.
   - ❏ Krypteringsstyrka
     Välj nivå på krypteringsstyrkan.
   - ❏ Omdirigera HTTP till HTTPS
     Omdirigera till HTTPS när HTTP nås.
3. Klicka på **Nästa**.
   Ett bekräftelsemeddelande visas.
4. Klicka på **OK**.
   Skannern är uppdaterad.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

Konfigurera ett servercertifikat för skannern

1. Öppna Web Config och välj fliken **Nätverkssäkerhet** > **SSL/TLS** > **Certifikat**.
2. Ange ett certifikat som ska användas i **Servercertifikat**.
   - ❏ Självsignerat certifikat
     Skannern har producerat ett självsignerat certifikat. Välj detta om du inte har ett CA-signerat certifikat.
   - ❏ CA-signerat Certifikat
     Välj detta om du har hämtat och importerat ett CA-signerat certifikat i förväg.
3. Klicka på **Nästa**.
   Ett bekräftelsemeddelande visas.
4. Klicka på **OK**.
   Skannern uppdateras.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34
➡ ”Konfigurera ett CA-signerat Certifikat” på sidan 95
➡ ”Konfigurera ett CA-certifikat” på sidan 99

Krypterad kommunikation med IPsec/IP-filtrering

Om IPsec/IP Filtering

Du kan filtrera trafiken baserat på IP-adresser, tjänster och port genom att använda IPsec/IP-filtreringsfunktionen. Genom att kombinera filter kan du konfigurera att skannern ska acceptera eller blockera angivna klienter och data. Du kan även höja säkerhetsnivån genom att använda IPsec.

Anmärkning:
Datorer som kör Windows Vista eller senare eller Windows Server 2008 eller senare stöder IPsec.

Konfigurera standardpolicy

Konfigurera en standardprincip när du vill filtrera trafiken. Standardprincipen gäller alla användare och grupper som ansluter till skannern. Konfigurera grupprinciper om du vill ha mer exakt kontroll över användare och grupper.

1. Öppna Web Config och välj fliken **Nätverkssäkerhet** > **IPsec/IP Filtering** > **Grundläggande**.
2. Ange ett värde för varje alternativ.
3. Klicka på **Nästa**.

   Ett bekräftelsemeddelande visas.
4. Klicka på **OK**.

   Skannern uppdateras.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

Inställningsalternativ för Standardpolicy

Standardpolicy

Alternativ	Inställningar och förklaringar
IPsec/IP Filtering	Du kan aktivera och inaktivera funktioner för IPsec/IP-nätverk.

❏ **Åtkomstkontroll**

Konfigurera en metod för styrning av trafiken av IP-paket.

Alternativ	Inställningar och förklaringar
Tillåt åtkomst	Välj detta när du vill att konfigurerade IP-paket ska få passera.
Neka åtkomst	Välj detta när du inte vill att konfigurerade IP-paket ska få passera.
IPsec	Välj detta när du vill att konfigurerade IPsec-paket ska få passera.

❏ **IKE Version**

Välj **IKEv1** eller **IKEv2** för **IKE Version**. Välj ett av alternativen enligt enheten som skannern är ansluten till.

❏ IKEv1

Följande alternativ visas när du väljer **IKEv1** för **IKE Version**.

Alternativ	Inställningar och förklaringar
Autentiseringsmetod	Du måste hämta och importera ett CA-signerat certifikat i förväg om du väljer **Certifikat**.
I förväg delad nyckel	Om du väljer **I förväg delad nyckel** för **Autentiseringsmetod**, ska du ange en fördelad nyckel med mellan 1 och 127 tecken.
Bekräfta I förväg delad nyckel	Ange nyckeln som du konfigurerade som bekräftelse.

❏ IKEv2

Följande alternativ visas när du väljer **IKEv2** för **IKE Version**.

Alternativ		Inställningar och förklaringar
Lokal	Autentiseringsmetod	Du måste hämta och importera ett CA-signerat certifikat i förväg om du väljer **Certifikat**.
	ID Typ	Om du väljer **I förväg delad nyckel** som **Autentiseringsmetod**, ska du välja typ av ID för skannern.
	ID	Ange skannerns ID som matchar typen av ID. Du kan inte använda "@", "#", och "=" för första tecknet. **Utmärkande namn**: Ange 1 till 255 1-byte ASCII (0x20 till 0x7E) tecken. Du behöver inkludera "=". **IP-adress**: Ange IPv4- eller IPv6-format. **FQDN**: Ange en kombination mellan 1 och 255 tecken med A–Z, a–z, 0–9, "-", och punkt (.). **E-postadress**: Ange 1 till 255 1-byte ASCII (0x20 till 0x7E) tecken. Du behöver inkludera "@". **Nyckel ID**: Ange 1 till 255 1-byte ASCII (0x20 till 0x7E) tecken.
	I förväg delad nyckel	Om du väljer **I förväg delad nyckel** för **Autentiseringsmetod**, ska du ange en fördelad nyckel med mellan 1 och 127 tecken.
	Bekräfta I förväg delad nyckel	Ange nyckeln som du konfigurerade som bekräftelse.

Alternativ		Inställningar och förklaringar
Fjärr	Autentiseringsmetod	Du måste hämta och importera ett CA-signerat certifikat i förväg om du väljer **Certifikat**.
	ID Typ	Om du väljer **I förväg delad nyckel** för **Autentiseringsmetod** väljer du typen av ID för enheten som du vill autentisera.
	ID	Ange skannerns ID som matchar typen av ID. Du kan inte använda "@", "#", och "=" för första tecknet. **Utmärkande namn**: Ange 1 till 255 1-byte ASCII (0x20 till 0x7E) tecken. Du behöver inkludera "=". **IP-adress**: Ange IPv4- eller IPv6-format. **FQDN**: Ange en kombination mellan 1 och 255 tecken med A–Z, a–z, 0–9, "-", och punkt (.). **E-postadress**: Ange 1 till 255 1-byte ASCII (0x20 till 0x7E) tecken. Du behöver inkludera "@". **Nyckel ID**: Ange 1 till 255 1-byte ASCII (0x20 till 0x7E) tecken.
	I förväg delad nyckel	Om du väljer **I förväg delad nyckel** för **Autentiseringsmetod**, ska du ange en fördelad nyckel med mellan 1 och 127 tecken.
	Bekräfta I förväg delad nyckel	Ange nyckeln som du konfigurerade som bekräftelse.

❏ Inkapsling

Om du väljer **IPsec** som **Åtkomstkontroll** måste du konfigurera en inkapslingsmetod.

Alternativ	Inställningar och förklaringar
Transportläge	Välj detta om du bara använder skannern i samma lokala nätverk. IP-paket lager 4 eller senare krypteras.
Tunnelläge	Om du använder skannern i det Internet-förberedda nätverket, såsom IPsec-VPN, ska du markera det här alternativet. Rubriker och data i IP-paket krypteras. **Fjärrgateway(Tunnelläge)**: Om du väljer **Tunnelläge** för **Inkapsling**, ange en gateway-adress med mellan 1 och 39 tecken.

❏ Säkerhetsprotokoll

Ställ in ett alternativ om du väljer **IPsec** som **Åtkomstkontroll**.

Alternativ	Inställningar och förklaringar
ESP	Välj detta när du vill säkerställa integriteten hos autentiseringen och data samt kryptera data.
AH	Välj detta när du vill säkerställa integriteten hos autentiseringen och data. Du kan fortfarande använda IPsec även om kryptering av data är förbjudet.

❏ **Algoritminställningar**

Det rekommenderas att välja **Valfri** för alla inställningar eller välja ett annat objekt än **Valfri** för varje inställning. Om du väljer **Valfri** för vissa av inställnignarna och ett annat objekt än **Valfri** för övriga inställningar kan enheten inte kommunicera, beroende på den andra enheten du vill autentisera.

Alternativ		Inställningar och förklaringar
IKE	Kryptering	Välj krypteringsalgoritm för IKE. Objekten varierar beroende på version av IKE.
	Autentisering	Välj autentiseringsalgoritm för IKE.
	Nyckelutbyte	Välj nyckeländringsalgoritm för IKE. Objekten varierar beroende på version av IKE.
ESP	Kryptering	Välj krypteringsalgoritm för ESP. Detta är tillgängligt när **ESP** är valt för **Säkerhetsprotokoll**.
	Autentisering	Välj autentiseringsalgoritm för ESP. Detta är tillgängligt när **ESP** är valt för **Säkerhetsprotokoll**.
AH	Autentisering	Välj krypteringsalgoritm för AH. Detta är tillgängligt när **AH** är valt för **Säkerhetsprotokoll**.

Konfigurera gruppolicy

En grupprincip är en eller flera regler som gäller en användare eller användargrupp. Skannern styr IP-paketen i enlighet med de principer som konfigurerats. IP-paket autentiseras i ordningsföljden grupprincip 1 till 10 och därefter en standardprincip.

1. Öppna Web Config och välj fliken **Nätverkssäkerhet** > **IPsec/IP Filtering** > **Grundläggande**.
2. Klicka på en numrerad flik du vill konfigurera.
3. Ange ett värde för varje alternativ.
4. Klicka på **Nästa**.

   Ett bekräftelsemeddelande visas.
5. Klicka på **OK**.

   Skannern uppdateras.

Inställningsalternativ för Gruppolicy

Alternativ	Inställningar och förklaringar
Aktivera denna Gruppolicy	Du kan aktivera och inaktivera en grupprincip.

Åtkomstkontroll

Konfigurera en metod för styrning av trafiken av IP-paket.

Alternativ	Inställningar och förklaringar
Tillåt åtkomst	Välj detta när du vill att konfigurerade IP-paket ska få passera.
Neka åtkomst	Välj detta när du inte vill att konfigurerade IP-paket ska få passera.
IPsec	Välj detta när du vill att konfigurerade IPsec-paket ska få passera.

Lokal adress(skanner)

Välj en IPv4-adress eller IPv6-adress som matchar din nätverksmiljö. Om en IP-adress tilldelats automatiskt kan du välja **Använda automatiskt erhållen IPv4-adress**.

Anmärkning:
Om en IPv6-adress tilldelas automatiskt kanske anslutningen inte är tillgänglig. Konfigurera en statisk IPv6-adress.

Fjärradress(värd)

Ange IP-adressen till en enhet för att styra åtkomsten. IP-adressen får innehålla max 43 tecken. Alla adresser styrs om du inte anger en IP-adress.

Anmärkning:
Om en IP-adress tilldelas automatiskt (dvs. med DHCP) kanske anslutningen inte är tillgänglig. Konfigurera en statisk IP-adress.

Metod för att välja port

Välj en metod för att specificera portar.

❏ Tjänstnamn

Ställ in ett alternativ om du väljer **Tjänstnamn** som **Metod för att välja port**.

❏ Transportprotokoll

Om du väljer **Portnummer** som **Metod för att välja port** måste du konfigurera en inkapslingsmetod.

Alternativ	Inställningar och förklaringar
Valfritt protokoll	Välj detta när du vill styra alla protokolltyper.
TCP	Välj detta när du vill styra data för unicast.
UDP	Välj detta när du vill styra data för broadcast och multicast.
ICMPv4	Välj detta när du vill styra ping-kommandot.

❏ Lokal port

Om du väljer **Portnummer** för **Metod för att välja port** och om du väljer **TCP** eller **UDP** för **Transportprotokoll**, ska du ange portnummer för att styra paketmottagning och separera dem med komma. Du kan ange högst 10 portnummer.

Exempel: 20,80,119,5220

Alla portar styrs om du inte anger ett portnummer.

❏ Fjärrport

Om du väljer **Portnummer** för **Metod för att välja port** och om du väljer **TCP** eller **UDP** för **Transportprotokoll**, ska du ange portnummer för att styra paketsändning och separera dem med komma. Du kan ange högst 10 portnummer.

Exempel: 25,80,143,5220

Alla portar styrs om du inte anger ett portnummer.

IKE Version

Välj **IKEv1** eller **IKEv2** för **IKE Version**. Välj ett av alternativen enligt enheten som skannern är ansluten till.

❏ IKEv1

Följande alternativ visas när du väljer **IKEv1** för **IKE Version**.

Alternativ	Inställningar och förklaringar
Autentiseringsmetod	Ställ in ett alternativ om du väljer **IPsec** som **Åtkomstkontroll**. Det använda certifikatet är gemensamt med standardprincipen.
I förväg delad nyckel	Om du väljer **I förväg delad nyckel** för **Autentiseringsmetod**, ska du ange en fördelad nyckel med mellan 1 och 127 tecken.
Bekräfta I förväg delad nyckel	Ange nyckeln som du konfigurerade som bekräftelse.

❏ IKEv2

Följande alternativ visas när du väljer **IKEv2** för **IKE Version**.

Alternativ		Inställningar och förklaringar
Lokal	Autentiseringsmetod	Ställ in ett alternativ om du väljer **IPsec** som **Åtkomstkontroll**. Det använda certifikatet är gemensamt med standardprincipen.
	ID Typ	Om du väljer **I förväg delad nyckel** som **Autentiseringsmetod**, ska du välja typ av ID för skannern.
	ID	Ange skannerns ID som matchar typen av ID. Du kan inte använda "@", "#", och "=" för första tecknet. **Utmärkande namn**: Ange 1 till 255 1-byte ASCII (0x20 till 0x7E) tecken. Du behöver inkludera "=". **IP-adress**: Ange IPv4- eller IPv6-format. **FQDN**: Ange en kombination mellan 1 och 255 tecken med A–Z, a–z, 0–9, "-", och punkt (.). **E-postadress**: Ange 1 till 255 1-byte ASCII (0x20 till 0x7E) tecken. Du behöver inkludera "@". **Nyckel ID**: Ange 1 till 255 1-byte ASCII (0x20 till 0x7E) tecken.
	I förväg delad nyckel	Om du väljer **I förväg delad nyckel** för **Autentiseringsmetod**, ska du ange en fördelad nyckel med mellan 1 och 127 tecken.
	Bekräfta I förväg delad nyckel	Ange nyckeln som du konfigurerade som bekräftelse.
Fjärr	Autentiseringsmetod	Ställ in ett alternativ om du väljer **IPsec** som **Åtkomstkontroll**. Det använda certifikatet är gemensamt med standardprincipen.
	ID Typ	Om du väljer **I förväg delad nyckel** för **Autentiseringsmetod** väljer du typen av ID för enheten som du vill autentisera.
	ID	Ange skannerns ID som matchar typen av ID. Du kan inte använda "@", "#", och "=" för första tecknet. **Utmärkande namn**: Ange 1 till 255 1-byte ASCII (0x20 till 0x7E) tecken. Du behöver inkludera "=". **IP-adress**: Ange IPv4- eller IPv6-format. **FQDN**: Ange en kombination mellan 1 och 255 tecken med A–Z, a–z, 0–9, "-", och punkt (.). **E-postadress**: Ange 1 till 255 1-byte ASCII (0x20 till 0x7E) tecken. Du behöver inkludera "@". **Nyckel ID**: Ange 1 till 255 1-byte ASCII (0x20 till 0x7E) tecken.
	I förväg delad nyckel	Om du väljer **I förväg delad nyckel** för **Autentiseringsmetod**, ska du ange en fördelad nyckel med mellan 1 och 127 tecken.
	Bekräfta I förväg delad nyckel	Ange nyckeln som du konfigurerade som bekräftelse.

Inkapsling

Om du väljer **IPsec** som **Åtkomstkontroll** måste du konfigurera en inkapslingsmetod.

Alternativ	Inställningar och förklaringar
Transportläge	Välj detta om du bara använder skannern i samma lokala nätverk. IP-paket lager 4 eller senare krypteras.
Tunnelläge	Om du använder skannern i det Internet-förberedda nätverket, såsom IPsec-VPN, ska du markera det här alternativet. Rubriker och data i IP-paket krypteras. **Fjärrgateway(Tunnelläge)**: Om du väljer **Tunnelläge** för **Inkapsling**, ange en gateway-adress med mellan 1 och 39 tecken.

Säkerhetsprotokoll

Ställ in ett alternativ om du väljer **IPsec** som **Åtkomstkontroll**.

Alternativ	Inställningar och förklaringar
ESP	Välj detta när du vill säkerställa integriteten hos autentiseringen och data samt kryptera data.
AH	Välj detta när du vill säkerställa integriteten hos autentiseringen och data. Du kan fortfarande använda IPsec även om kryptering av data är förbjudet.

Algoritminställningar

Det rekommenderas att välja **Valfri** för alla inställningar eller välja ett annat objekt än **Valfri** för varje inställning. Om du väljer **Valfri** för vissa av inställnignarna och ett annat objekt än **Valfri** för övriga inställningar kan enheten inte kommunicera, beroende på den andra enheten du vill autentisera.

Alternativ		Inställningar och förklaringar
IKE	Kryptering	Välj krypteringsalgoritm för IKE. Objekten varierar beroende på version av IKE.
	Autentisering	Välj autentiseringsalgoritm för IKE.
	Nyckelutbyte	Välj nyckeländringsalgoritm för IKE. Objekten varierar beroende på version av IKE.
ESP	Kryptering	Välj krypteringsalgoritm för ESP. Detta är tillgängligt när **ESP** är valt för **Säkerhetsprotokoll**.
	Autentisering	Välj autentiseringsalgoritm för ESP. Detta är tillgängligt när **ESP** är valt för **Säkerhetsprotokoll**.
AH	Autentisering	Välj krypteringsalgoritm för AH. Detta är tillgängligt när **AH** är valt för **Säkerhetsprotokoll**.

Kombination av Lokal adress(skanner) och Fjärradress(värd) i Gruppolicy

	Inställning för Lokal adress(skanner)		
	IPv4	IPv6*[2]	Alla adresser*[3]

Inställning för Fjärradress(värd)	IPv4*1	✓	–	✓
	IPv6*1, *2	–	✓	✓
	Tom	✓	✓	✓

*1 Om **IPsec** har valts för **Åtkomstkontroll**, kan du inte specificera i någon prefixlängd.

*2 Om **IPsec** har valts för **Åtkomstkontroll**, kan du välja en länk-lokal adress (fe80::) men gruppolicyn inaktiveras.

*3 Förutom IPv6 länklokala adresser.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

Referenser för tjänstenamn enligt gruppolicy

Anmärkning:
Otillgängliga tjänster visas, men kan inte väljas.

Tjänstenamn	Protokolltyp	Lokalt portnummer	Fjärrportnummer	Kontrollerade funktioner
Valfri	–	–	–	Alla tjänster
ENPC	UDP	3289	Valfri port	Söker efter en skanner från olika applikationer, såsom Epson Device Admin och en skannerdrivrutin
SNMP	UDP	161	Valfri port	Anskaffa och konfigurera MIB från applikationer, såsom Epson Device Admin och Epson skannerdrivrutin
WSD	TCP	Valfri port	5357	Kontrollera WSD
WS-Discovery	UDP	3702	Valfri port	Söker WSD-skannrar
Network Scan	TCP	1865	Valfri port	Vidarebefordra skannade data från Document Capture Pro
Network Push Scan	TCP	Valfri port	2968	Anskaffa jobbinformation för push-skanning från Document Capture Pro
Network Push Scan Discovery	UDP	2968	Valfri port	Söka efter en dator från skannern
FTP-data (fjärr)	TCP	Valfri port	20	FTP-klient (vidarebefordra skanningsdata) Detta kan dock endast styra en FTP-server som använder fjärrportnummer 20.
FTP-styrning (fjärr)	TCP	Valfri port	21	FTP-klient (kontrollera vidarebefordrade skannade data)
CIFS (fjärr)	TCP	Valfri port	445	CIFS-klient (vidarebefordra skannade data till en mapp)

Tjänstenamn	Protokolltyp	Lokalt portnummer	Fjärrportnummer	Kontrollerade funktioner
NetBIOS Name Service (fjärr)	UDP	Valfri port	137	CIFS-klient (vidarebefordra skannade data till en mapp)
NetBIOS Datagram Service (fjärr)	UDP	Valfri port	138	
NetBIOS Session Service (fjärr)	TCP	Valfri port	139	
HTTP (lokal)	TCP	80	Valfri port	HTTP(S)-server (vidarebefordran av data för Web Config och WSD)
HTTPS (lokal)	TCP	443	Valfri port	
HTTP (fjärr)	TCP	Valfri port	80	HTTP(S) klient (uppdaterar firmware och rotcertifikat)
HTTPS (fjärr)	TCP	Valfri port	443	

Exempel på konfigurering av IPsec/IP Filtering

Endast mottagning av IPsec-paket

Det här exemplet visar hur du enbart konfigurerar en standardprincip.

Standardpolicy:

- ❏ **IPsec/IP Filtering**: **Aktivera**
- ❏ **Åtkomstkontroll**: **IPsec**
- ❏ **Autentiseringsmetod**: **I förväg delad nyckel**
- ❏ **I förväg delad nyckel**: Ange högst 127 tecken.

Gruppolicy: Konfigurera inte.

Ta emot skanningdata och skannerinställningar

Det här exemplet tillåter kommunikation för skanningdata och skannerkonfiguration från specificerade tjänster.

Standardpolicy:

- ❏ **IPsec/IP Filtering**: **Aktivera**
- ❏ **Åtkomstkontroll**: **Neka åtkomst**

Gruppolicy:

- ❏ **Aktivera denna Gruppolicy**: Markera rutan.
- ❏ **Åtkomstkontroll**: **Tillåt åtkomst**
- ❏ **Fjärradress(värd)**: IP-adressen till en klient
- ❏ **Metod för att välja port**: **Tjänstnamn**
- ❏ **Tjänstnamn**: Markera rutan för **ENPC**, **SNMP**, **HTTP (lokal)**, **HTTPS (lokal)** och **Network Scan**.

Endast mottagning från en angiven IP-adress fungerar

I det här exemplet får en viss IP-adress tillgång till skannern.

Standardpolicy:

❏ **IPsec/IP Filtering**: **Aktivera**

❏ **Åtkomstkontroll**:**Neka åtkomst**

Gruppolicy:

❏ **Aktivera denna Gruppolicy**: Markera rutan.

❏ **Åtkomstkontroll**: **Tillåt åtkomst**

❏ **Fjärradress(värd)**: IP-adressen till en administratörs klient

Anmärkning:
Oavsett den konfigurerade principen kan klienten få tillgång till skannern och konfigurera den.

Konfigurera ett certifikat för IPsec-/IP-filtrering

Konfigurera ett klientcertifikat för IPsec-/IP-filtrering. När du ställer in det kan du använda certifikatet som en autentiseringsmetod för IPsec-/IP-filtrering. Gå till **CA-certifikat** om du vill konfigurera certifikatutfärdaren.

1. Gå till Web Config, och välj sedan fliken **Nätverkssäkerhet** > **IPsec/IP Filtering** > **Klientcertifikat**.

2. Importera certifikatet i **Klientcertifikat**.

   Om du redan har importerat ett certifikat som har publicerat av en certifikatutfärdare kan du kopiera certifikatet och använda det i IPsec-/IP-filtrering. För att kopiera väljer du certifikatet från **Kopiera från**, och klickar sedan på **Kopiera**.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

➡ ”Konfigurera ett CA-signerat Certifikat” på sidan 95

➡ ”Konfigurera ett CA-certifikat” på sidan 99

Ansluta skannern till ett IEEE802.1X-nätverk

Konfigurera ett IEEE 802.1X-nätverk

När du konfigurerar IEEE 802.1X till skannern kan du använda den i nätverket som är anslutet till en RADIUS-server, en nätverksbrytare med autentiseringsfunktion eller en åtkomstpunkt.

1. Öppna Web Config och välj fliken **Nätverkssäkerhet** > **IEEE802.1X** > **Grundläggande**.

2. Ange ett värde för varje alternativ.

   Om du vill använda skannern i ett Wi-Fi-nätverk klickar du på **Wi-Fi-inställning** och väljer eller anger ett SSID.

Anmärkning:
Du kan dela inställningar mellan Ethernet och Wi-Fi.

3. Klicka på **Nästa**.

   Ett bekräftelsemeddelande visas.

4. Klicka på **OK**.

   Skannern uppdateras.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

Inställningsalternativ för IEEE 802.1X-nätverk

Alternativ	Inställningar och förklaringar	
IEEE802.1X (trådbundet LAN)	Du kan aktivera eller inaktivera inställningar på sidan (**IEEE802.1X** > **Grundläggande**) för IEEE802.1X (trådbundet LAN).	
IEEE802.1X (Wi-Fi)	Anslutningsstatus för IEEE802.1X (Wi-Fi) visas.	
Anslutningsmetod	Anslutningsmetoden för det aktuella nätverket visas.	
EAP-typ	Välj en autentiseringsmetod mellan skannern och en RADIUS-server.	
	EAP-TLS	Du måste hämta och importera ett CA-signerat certifikat.
	PEAP-TLS	
	PEAP/MSCHAPv2	Du måste konfigurera ett lösenord.
	EAP-TTLS	
Användar-ID	Konfigurera ett ID som ska användas för autentisering av en RADIUS-server. Ange 1 till 128 1-byte ASCII (0x20 till 0x7E)-tecken.	
Lösenord	Konfigurera ett lösenord för autentisering av skannern. Ange 1 till 128 1-byte ASCII (0x20 till 0x7E)-tecken. Om du använder en Windows-server som en RADIUS-server kan du ange upp till 127 tecken.	
Bekräfta lösenord	Ange lösenordet som du konfigurerade som bekräftelse.	
Server-ID	Du kan konfigurera ett server-ID för autentisering med en angiven RADIUS-server. Autentiseraren verifierar om ett server-ID anges i fältet subject/subjectAltName i ett servercertifikat som skickas från en RADIUS-server. Ange 0 till 128 1-byte ASCII (0x20 till 0x7E)-tecken.	
Certifikatverifiering	Du kan ställa in certifikatvalidering oavsett autentiseringsmetod. Importera certifikatet i **CA-certifikat**.	
Anonymt namn	Om du väljer **PEAP-TLS** eller **PEAP/MSCHAPv2** som **EAP-typ** kan du konfigurera ett anonymt namn i stället för ett användar-ID för fas 1 i PEAP-autentisering. Ange 0 till 128 1-byte ASCII (0x20 till 0x7E)-tecken.	

Alternativ	Inställningar och förklaringar	
Krypteringsstyrka	Du kan välja ett av följande.	
	Hög	AES256/3DES
	Medelhög	AES256/3DES/AES128/RC4

Konfigurera ett certifikat för IEEE 802.1X

Konfigurera klientcertifikatet för IEEE802.1X. När du ställer in det kan du använda **EAP-TLS** och **PEAP-TLS** som en autentiseringsmetod för IEEE 802.1X. Gå till **CA-certifikat** om du vill konfigurera certifikatet från certifieringsmyndigheten.

1. Gå till Web Config, och välj sedan fliken **Nätverkssäkerhet** > **IEEE802.1X** > **Klientcertifikat**.
2. Ange ett certifikat i **Klientcertifikat**.

   Om du redan har importerat ett certifikat som har publicerat av en certifieringsmyndighet kan du kopiera certifikatet och använda det i IEEE802.1X. För att kopiera väljer du certifikatet från **Kopiera från**, och klickar sedan på **Kopiera**.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

Lösa problem med avancerad säkerhet

Återställa säkerhetsinställningarna

När du upprättar en mycket säker miljö, såsom IPsec-/IP-filtrering, kan du inte kommunicera med enheter på grund av felaktiga inställningar eller fel i enheten eller servern. I så fall återställs säkerhetsinställningarna för att göra inställningar för enheten igen, eller för att medge tillfällig användning.

Inaktivera säkerhetsfunktionen med Web Config

Du kan inaktivera IPsec/IP Filtering med Web Config.

1. Öppna Web Config och välj fliken **Nätverkssäkerhet** > **IPsec/IP Filtering** > **Grundläggande**.
2. Inaktivera **IPsec/IP Filtering**.

Problem att använda funktionerna för nätverkssäkerhet

Bortglömd på förhand delad nyckel

Konfigurera om en på förhand delad nyckel.

För att ändra nyckeln öppnar du Web Config och väljer fliken **Nätverkssäkerhet** > **IPsec/IP Filtering** > **Grundläggande** > **Standardpolicy** eller **Gruppolicy**.

När du ändrar den i förväg delade nyckeln, konfigurera den i förväg delade nyckeln för datorer.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34
➡ ”Krypterad kommunikation med IPsec/IP-filtrering” på sidan 102

Det går inte att kommunicera med IPsec-kommunikation

Specificera algoritmen som skannern eller datorn inte stöder.

Skannern har stöd för följande algoritmer. Kontrollera datorns inställningar.

Säkerhetsmetoder	Algoritmer
IKE-krypteringsalgoritm	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE-autentiseringsalgoritm	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE-nyckelutväxlingsalgoritm	DH Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30*
ESP-krypteringsalgoritm	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP-autentiseringsalgoritm	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH-autentiseringsalgoritm	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* Endast tillgänglig för IKEv2

Relaterad information

➡ ”Krypterad kommunikation med IPsec/IP-filtrering” på sidan 102

Plötsligt går det inte att kommunicera

IP-adressen för skannern har ändrats eller kan inte användas.

När IP-adressen som registrerats för den lokala adressen på Gruppolicy har ändrats eller inte kan användas går det inte att utföra IPsec-kommunikation. Inaktivera IPsec med skannerns kontrollpanel.

Om DHCP är för gammal startar du om, eftersom IPv6-adressen är för gammal eller inte har hämtats, och sedan kanske den registrerade IP-adressen för skannerns Web Config (**Nätverkssäkerhet**-flik > **IPsec/IP Filtering** > **Grundläggande** > **Gruppolicy** > **Lokal adress(skanner)**).

Använd en statisk IP-adress.

IP-adressen för datorn har ändrats eller kan inte användas.

När IP-adressen som registrerats för fjärradressen på Gruppolicy har ändrats eller inte kan användas går det inte att utföra IPsec-kommunikation.

Inaktivera IPsec med skannerns kontrollpanel.

Om DHCP är för gammal startar du om, eftersom IPv6-adressen är för gammal eller inte har hämtats, och sedan kanske den registrerade IP-adressen för skannerns Web Config (**Nätverkssäkerhet**-flik > **IPsec/IP Filtering** > **Grundläggande** > **Gruppolicy** > **Fjärradress(värd)**).

Använd en statisk IP-adress.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

➡ ”Krypterad kommunikation med IPsec/IP-filtrering” på sidan 102

Det går inte att ansluta efter konfiguration av IPsec/IP-filtrering

Inställningarna för IPsec/IP-filtrering är felaktiga.

Inaktivera IPsec/IP-filtrering från skannerns kontrollpanel. Anslut skannern och datorn och gör inställningar för IPsec/IP-filtrering igen.

Relaterad information

➡ ”Krypterad kommunikation med IPsec/IP-filtrering” på sidan 102

Kan inte öppna skannern efter konfiguration av IEEE 802.1X

Inställningarna för IEEE 802.1X är felaktiga.

Inaktivera IEEE 802.1X och Wi-Fi via skannerns kontrollpanel. Anslut skannern till datorn och konfigurera IEEE 802.1X igen.

Anslut skannern till datorn och konfigurera IEEE 802.1X igen.

Relaterad information

➡ ”Konfigurera ett IEEE 802.1X-nätverk” på sidan 112

Problem att använda ett digitalt certifikat

Kan inte importera ett CA-signerat Certifikat

CA-signerat Certifikat informationen på CSR överensstämmer inte.

Om CA-signerat Certifikat och CSR inte innehåller samma information kan CSR inte importeras. Kontrollera följande:

❏ Försöker du importera certifikatet på en enhet som inte har samma information?

Kontrollera informationen i CSR och importera sedan certifikatet på en enhet som har samma information.

❏ Har du skrivit över den CSR som sparades på skannern efter det att du skickade förfrågan till en certifikatutfärdare?

Hämta det CA-signerade certifikatet igen med ditt CSR.

CA-signerat Certifikat är mer än 5KB.

Du kan inte importera ett CA-signerat Certifikat som är större än 5 KB.

Lösenordet för import av certifikatet är felaktigt.

Ange rätt lösenord. Du kan inte importera certifikatet om du har glömt bort lösenordet. Hämta CA-signerat Certifikat på nytt.

Relaterad information

➡ ”Importera ett CA-signerat certifikat” på sidan 97

Det går inte att uppdatera ett självsignerat certifikat

Nätverksnamn har inte angett.

Du måste ange **Nätverksnamn**.

Tecken som inte stöds har angetts i Nätverksnamn.

Ange mellan 1 och 128 tecken för IPv4, IPv6, värdnamn eller FQDN-format i ASCII (0x20–0x7E).

Ett komma eller mellanslag är inkluderat i det gemensamma namnet.

Om det finns ett komma kommer **Nätverksnamn** att delas i det läget. Ett fel inträffar om ett mellanslag anges före eller efter ett komma.

Relaterad information

➡ ”Uppdatera ett självsignerat certifikat” på sidan 99

Det går inte att skapa en CSR

Nätverksnamn har inte angett.

Du måste ange **Nätverksnamn**.

Tecken som inte stöds har angetts i Nätverksnamn, Organisation, Organisationsenhet, Plats och Stat/provins.

Ange tecken för IPv4, IPv6, värdnamn eller FQDN-format i ASCII (0x20–0x7E).

Ett komma eller mellanslag är inkluderat i Nätverksnamn.

Om det finns ett komma kommer **Nätverksnamn** att delas i det läget. Ett fel inträffar om ett mellanslag anges före eller efter ett komma.

Relaterad information

➡ ”Hämta ett CA-signerat certifikat” på sidan 95

Varningar om ett digitalt certifikat visas

Meddelanden	Orsak/åtgärd
Ange ett Servercertifikat.	**Orsak:** Du har inte valt en fil som ska importeras. **Åtgärd:** Välj en fil och klicka på **Importera**.
CA-certifikat 1 är inte angivet.	**Orsak:** CA-certifikat 1 har inte angetts, endast CA-certifikat 2 har angetts. **Åtgärd:** Importera CA-certifikat 1 först.
Ogiltigt värde nedan.	**Orsak:** Filens sökväg och/eller lösenordet innehåller tecken som inte stöds. **Åtgärd:** Kontrollera att rätt tecken angetts i posten.
Ogiltigt datum och tid.	**Orsak:** Datum och klockslag har inte ställts in på skannern. **Åtgärd:** Ställ in datum och klockslag med Web Config eller EpsonNet Config.
Ogiltigt lösenord.	**Orsak:** Lösenordet som angetts för CA-certifikatet och det angivna lösenordet matchar inte varandra. **Åtgärd:** Ange rätt lösenord.

Meddelanden	Orsak/åtgärd
Ogiltig fil.	**Orsak:** Du importerar inte en certifikatfil med X509-format. **Åtgärd:** Kontrollera att du väljer rätt certifikat som skickats av en betrodd certifikatutfärdare.
	Orsak: Filen som du importerade är för stor. Den maximala filstorleken är 5 KB. **Åtgärd:** Om du valt rätt fil kan certifikatet vara skadat eller förfalskat.
	Orsak: Kedjan i certifikatet är inte giltig. **Åtgärd:** Mer information om certifikatet finns på certifikatutfärdarens webbplats.
Kan inte använda Servercertifikat som innehåller fler än tre CA-certifikat.	**Orsak:** Certifikatfilen i PKCS#12-format innehåller mer än 3 CA-certifikat. **Åtgärd:** Importera varje certifikat som konverterats från PKCS#12-format till PEM-format eller importera en certifikatfil i PKCS#12-format som innehåller högst 2 CA-certifikat.
Certifikat har upphört att gälla. Kontrollera om certifikat är giltigt eller kontrollera datum och tid på produkten.	**Orsak:** Certifikatet har gått ut. **Åtgärd:** ❏ Om certifikatet har gått ut ska du hämta och importera ett nytt certifikat. ❏ Om certifikatet inte har gått ut ska du kontrollera att rätt datum och klockslag ställts in på skannern.
Privat nyckel är obligatoriskt.	**Orsak:** Det finns ingen parad privat nyckel med certifikatet. **Åtgärd:** ❏ Om certifikatet är i PEM/DER-formatet och det hämtats med en CSR via en dator ska du ange den privata nyckelfilen. ❏ Om certifikatet är i PKCS#12-formatet och det hämtats med en CSR via en dator ska du skapa en fil som innehåller den privata nyckeln.
	Orsak: Du har importerat ett PEM/DER-certifikat som hämtats med en CSR med Web Config på nytt. **Åtgärd:** Om certifikatet är i PEM/DER-formatet och det hämtats med en CSR via Web Config kan du bara importera det en gång.

Meddelanden	Orsak/åtgärd
Fel vid inställning.	**Orsak:** Det går inte att avsluta konfigureringen eftersom det blev fel i kommunikationen mellan skannern och datorn eller filen inte går att läsa på grund av fel. **Åtgärd:** Importera filen igen när du har kontrollerat den angivna filen och kommunikationen.

Relaterad information

➡ ”Om digital certifiering” på sidan 95

Ett CA-signerat certifikat har raderats av misstag

Det finns ingen säkerhetskopieringsfil för det CA-signerade certifikatet.

Importera certifikatet igen om du inte har en säkerhetskopia.

Om du hämtar ett certifikat med en CSR som skapats i Web Config kan du inte importera ett certifikat som raderats. Skapa en CSR och hämta ett nytt certifikat.

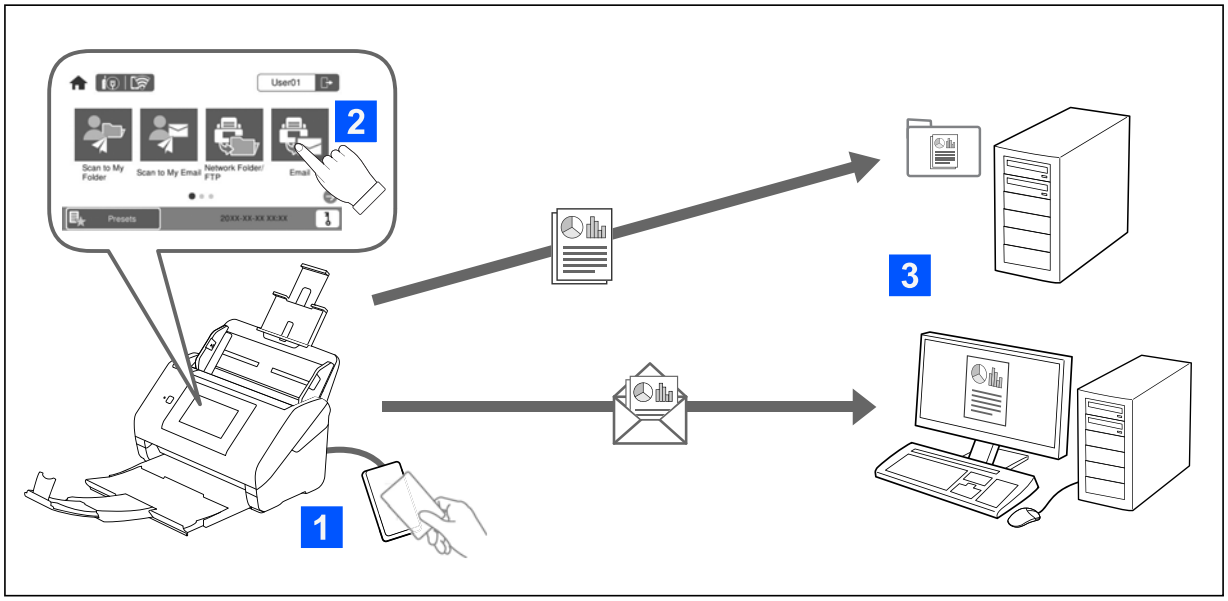
Relaterad information

➡ ”Importera ett CA-signerat certifikat” på sidan 97

➡ ”Radera ett CA-signerat certifikat” på sidan 98

Autentiseringsinställningar

Om Autentiseringsinställningar



När Autentiseringsinställningar är aktiverad krävs användarautentisering för att starta skannign. Du kan konfigurera skanningmetoder som kan användas av varje användare och förhindra oavsiktlig användning.

Du kan specificera den autentiserade användarens e-postadress som skanningmål (Skanna t. min e-post), eller spara varje användares data i en personlig mapp (Skanna till min mapp). Du kan även specificera andra skanningmetoder.

Anmärkning:

❏ *Du kan inte skanna från en dator eller en smart enhet när Autentiseringsinställningar är aktiverat.*

❏ *Utöver Autentiseringsinställningar som introducerats i denna bruksanvisning kan du även skapa ett autentiseringssystem med en autentiseringsserver. För att skapa ett system, använd Document Capture Pro Server Authentication Edition (det förkortade namnet är Document Capture Pro Server AE). Kontakta ditt lokala Epson-kontor för mer information.*

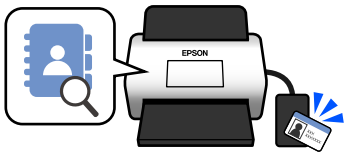
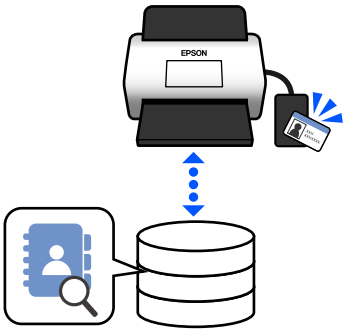
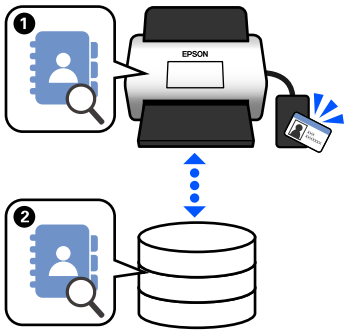
Tillgängliga funktioner för Autentiseringsinställningar

Skanningfuntion på kontrollpanelen	Autentiseringsinställningar	
	Vid aktivering	Vid avaktivering
Skanna till min mapp Sparar bilder i den mapp som tilldelats autentiserad användare.	✓	-
Skanna till min e-post Skickar bilder till den e-postadress som tilldelats den autentiserade användaren.	✓	-
Skanna till nätv.mapp/FTP Sparar bilder till en mapp i nätverket.	✓	✓

Skanningfuntion på kontrollpanelen	Autentiseringsinställningar	
	Vid aktivering	Vid avaktivering
Skanna till dator Sparar bilder till en ansluten dator med jobb som skapats i Document Capture Pro (Windows)/Document Capture (Mac OS). * När Autentiseringsinställningar är aktiverad kan du använda jobb som registrerats i **Förinställ.**.	✓*	✓
Skanna till e-post Skickar bilder till den e-postadress som du konfigurerat.	✓	✓
Skanna till moln Skickar bilder till den molntjänst som du konfigurerat.	✓	✓
Skanna till USB-enhet Sparar bilder till en USB-enhet som är ansluten till skannern. Detta är endast tillgängligt när ingen autentiseringsenhet är ansluten till skannern.	✓	✓
Skanna till WSD Sparar bilder till en ansluten dator med WSD-funktion.	-	✓
Förinställ. Du kan registrera upp till 48 förinställda skanningfunktioner. Du kan allokera upp till fem Förinställ. till användare som registrerats i Lokal DB. Allokerad Förinställ. är endast tillgänglig för användaren. Förinställ. som inte registrerats av en autentiserad användare kan användas av alla användare.	✓	✓

Om Autentiseringsmetod

Den här skannern kan erbjuda autentisering med följande metoder utan att behöva skapa en autentiseringsserver.

	Lokal DB	**LDAP**	**Lokal DB och LDAP**
Plats för användarinformation	**Skannerns minne** Denna autentiseringsmetod kontrollerar användarinformationen som registrerats för skannern och jämför den med användaren som använder skanningfunktionen.	**LDAP-server*** Det här är autentiseringsmetoden som söker användarinformation för LDAP-servern som synkroniserats med skrivaren. Eftersom upp till 300 användarinformationsobjekt från LDAP-servern kan sparas temporärt på skannern som ett cache-minne, autentisering kan utföras med cache om LDAP-servern ligger nere. * Servern som erbjuder en katalogtjänst som kan kommunicera med LDAP.	**Skannerminne och LDAP-server** Kontrollera användarinformationen som registrerats i skannern först (❶), och om ingen träff finns, kan du kontrollera användarinformationen mot LDAP-servern (❷).
			
Antal registrerade användare	50 (skannerns minne)	Obegränsat (LDAP-server)	50 (skannerns minne) Obegränsat (LDAP-server)
Skannerns cache-minne	-	300	Max 300 (50 av cache-enheterna delas med Användarinställningar i Lokal DB)
Inloggningssätt	Du kan använda någon av följande metoder. ❏ Håll upp ett autentiseringskort, eller ange ett **Användar-ID** och **Lösenord** ❏ Håll upp ett autentiseringskort, eller ange ett **ID-nummer** ❏ Ange ett **Användar-ID** och **Lösenord** ❏ Ange ett **Användar-ID** ❏ Ange ett **ID-nummer**		
Gränsvärden för funktionen ”Skanna till”	Konfigurera individuellt för varje användare	Samma inställningar för alla LDAP användare	Lokal DB-användare: konfigurera individuellt LDAP-använare: samma inställningar för alla användare
Allokera Förinställ. till användare	Upp till 5 per användare	- (Kan inte konfigureras individuellt)	Lokal DB användare: upp till 5 per användare LDAP användare: -

Mjukvara för inställning

Konfigurera med Web Config eller Epson Device Admin.

❏ När du använder Web Config, kan du konfigurera skrivaren enbart genom att använda en webbläsare.

”Web Config” på sidan 34

❏ När du använder Epson Device Admin, kan du konfigurera skrivaren enbart genom att använda en konfigurationsmall.

”Epson Device Admin” på sidan 35

Använda skannerns firmware

Innan du aktiverar Autentiseringsinställningar, uppdaterar du skannerns firmware till den senaste versionen. Anslut skannern till Internet i förväg.

Viktigt:

Stäng inte av datorn eller skannern medan du uppdaterar.

Vid konfiguration från Web Config:

Välj fliken **Enhetshantering** > **Firmware-uppdatering**, och följ sedan anvisningarna på skärmen om du vill uppdatera firmware.

Vid konfiguration från Epson Device Admin:

Välj **Home** > **Firmware** > **Update** och följ sedan anvisningarna på skärmen om du vill uppdatera firmware.

Anmärkning:

Om senaste firmware redan installerad behöver du inte uppdatera.

Anslutning och konfiguration av autentiseringsenhet

Om du vill ansluta och använda en autentiseringsenhet, såsom en IC-kortläsare behöver du först konfigurera enheten. Detta är inte nödvändigt om du inte använder en autentiseringsenhet.

Relaterad information

➡ ”Ansluta autentiseringsenheten” på sidan 128

➡ ”Autentiseringsenhetsinställningar” på sidan 129

Kompatibel lista för kortläsare

Den här listan garanterar inte funktionerna för kortläsare i listan.

Ja: stöds (ID-information kan läsas med standardkortläsarinställningar.)

Nej: ej kompatibel

Fabrikat	Modell	Modellnummer	Autentiseringskort							Läge
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
RF IDEAS	pcProx Plus	RDR-80081AKU	Ja	Ja*1	Ja*1	Ja*1	Nej	Nej	Nej	Tangentbord
RF IDEAS	pcProx	RDR-7081BKU	Ja*1	Nej	Ja	Ja	Nej	Nej	Nej	Tangentbord
RF IDEAS	pcProx	RDR-7581AKU	Ja	Nej	Ja*1	Ja*1	Nej	Nej	Nej	Tangentbord
ELATEC	TWN3 MIFARE	T3DT-MB2BEL T3DT-MB2WEL	Nej	Nej	Ja	Ja	Nej	Nej	Nej	Tangentbord
ELATEC	TWN3 MIFARE NFC	T3DT-FB2BEL T3DT-FB2WEL	Ja	Nej	Ja	Ja	Ja	Ja	Ja	Tangentbord
ELATEC	TWN4 MULTI-TECH	T4DT-FB2BEL-PI T4DT-FB2WEL-PI	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Tangentbord
ELATEC	TWN4 Multi-Tech 2 BLE-PI	T4LK-FB4BLZ-PI	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Tangentbord
ELATEC	TWN4 Slim	T4QC-FC3B7	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Tangentbord
HID Global	OMNIKEY 5427	OMNIKEY5427CK OMNIKEY5427CK gen2	Ja	Ja	Ja	Ja	Ja	Nej	Ja	Tangentbord*1

Fabrikat	Modell	Modellnummer	Autentiseringskort							Läge
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
ACS	ACR122U	ACR122U	Nej	Nej	Ja*2	Ja*2	Ja	Nej	Ja*2	PC/SC
ACS	ACR1252	ACR1252	Nej	Nej	Ja*2	Ja*2	Ja	Ja	Ja*2	PC/SC
Sony	PaSoRi	RC-S330/S	Nej	Nej	Ja*2	Ja*2	Ja*2	Ja*2	Ja*2	PaSoRi
Sony	PaSoRi	RC-S380/P RC-S380/S	Nej	Nej	Ja*2	Ja*2	Ja*2	Ja*2	Ja*2	PaSoRi
DMZ	Leitor RFID Universal	DMZ008	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Tangentbord
DMZ	Leitor RFID Multi-125	DMZ087	Nej	Ja	Nej	Nej	Nej	Nej	Nej	Tangentbord
DMZ	Leitor RFID Mifare	DMZ088	Nej	Nej	Ja	Ja	Nej	Nej	Nej	Tangentbord
DMZ	Biometric & RFID Reader	DMZ073	Nej	Ja	Nej	Nej	Nej	Nej	Nej	Tangentbord
inepro	SCR708	SCR708	Ja*1	Ja*1	Ja*1	Ja*1	Ja*1	Ja*1	Ja*1	Tangentbord
Y Soft	YU030888 001	MU0388	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Tangentbord
Cartadis	TCM3 Cartadis MiFare Card Reader	ZTCM3-MIFARE	Nej	Nej	Ja	Ja	Nej	Nej	Ja	Tangentbord

Fabrikat	Modell	Modellnummer	Autentiseringskort							Läge
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/Lite-S		
MICI Network Co., Ltd.	EM & Mifare Card Reader	mCR-600	Nej	Nej	Ja	Ja	Nej	Nej	Ja	Tangentbord
NTware	MiCard Multi-Tech4-PI	T4DT-FB4WUF-PI	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Tangentbord
NTware	MiCard Plus-2-V2	RDR-80081AGU-NT2-20	Ja*1	Ja*1	Ja*1	Ja*1	Nej	Nej	Nej	Tangentbord
NTware	MiCard V3 Multi	MiCard V3 Multi	Ja	Ja	Ja	Ja	Ja	Ja	Nej	Tangentbord

*1 Du behöver ändra inställningarna för kortläsaren genom att använda den inbyggda programvaran som tillhandahålls av kortläsartillverkaren.

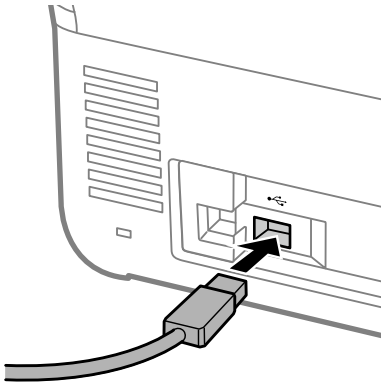
*2 Om du behöver använda data i ett visst området i kortet som inte är standard-ID för kortet som ett autentiserings-ID genom att konfigurera produktinställningar ska du kontakta din Epson-partner eller lokala representant för mer information om ett sätt att konfigurera produkten.

Ansluta autentiseringsenheten

Viktigt:

När du ansluter autentiseringsenheten till flera skannrar använder du en produkt med samma modellnummer.

Anslut kortläsarens USB-kabel till den externa USB-gränssnittsporten på skannern.



Åtgärdskontroll för autentiseringsenhet

Du kan kontrollera anslutningsstatus och autentiseringskortientifiering på skannerns kontrollpanel.

Information visas om du väljer **Inst.** > **Enhetsinformation** > **Autentisera enhetsstatus**.

Autentiseringsenhetsinställningar

Välj läsformat för autentiseringsinformation mottagen från ett autentiseringskort.

Du kan konfigurera följande läsmetod för autentiseringsenheten.

❏ Läs det aktuella området i autentiseringskortet, såsom anställningsnummer och personal-ID.

❏ Använd autentiseringskortinformationen förutom UID (autentiseringskortinformation, såsom serienummer).
Du kan använda ett verktyg för att generera funktionsparametrar. Kontakta återförsäljaren för mer information.

Anmärkning:
Använda autentiseringskort från olika tillverkare:

När UID används för kortinformation (kort-ID-information såsom serienumret) kan du använda en blandning av olika typer av autentiseringskort. Det här kan inte blandas när annan kortinformation används.

Vid konfiguration från Web Config:

Välj fliken **Enhetshantering** > **Kortläsare**.

Vid konfiguration från Epson Device Admin:

Välj **Administrator Settings** > **Authentication Settings** > **Card Reader** från konfigurationsmallen.

Objekt	Förklaring
Vendor ID	Konfigurera leverantörs-ID för autentiseringsenheten som begränsar användning från 0000 till FFFF genom att använda 4 alfanumeriska tecken. Om du inte vill begränsa den, ange 0000.
Product ID	Konfigurera produkt-ID för autentiseringsenheten som begränsar användning från 0000 till FFFF genom att använda 4 alfanumeriska tecken. Om du inte vill begränsa den, ange 0000.
Driftsparameter	Konfigurera åtgärdsparametern för autentiseringsenheten mellan 0 och 8192 tecken. A–Z, a–z, 0–9, +, /, =, mellanslag och radmatning är tillgängliga.
Kortläsare	Välj konverteringsformat för autentiseringsenheten. Du kan kontrollera formatdetaljerna. Se den medföljande länken i artikelbeskrivningen.
Format för att spara Autentiseringskort-ID	Välj konverteringsformat för autentiseringsinformation på ett ID-kort. Du kan kontrollera formatdetaljerna. Se den medföljande länken i artikelbeskrivningen.
Ställ in intervall för kort-ID	Aktivera specifikationen för läspositionen.
Textens startposition	Specificera startposition för texten för att läsa ID-information. Du kan uppge mellan 1 och 4096 tecken.
Antal tecken	Specificera antalet tecken som ska läsas från startposition för ID-information. Du kan uppge mellan 1 och 4096 tecken.

Registrera och konfigurera information

Konfiguration

Skapa nödvändiga inställningar beroende på vilken Autentiseringsmetod du använder.

Viktigt:

Innan du startar konfigurationen ska du kontrollera att tidsinställningen för skannern är korrekt.

Om tidsinställningen är felaktig visas felmeddelandet ”Licensen har gått ut”, vilket kan leda till fel i konfigurationen av skannern. För användning av en säkerhetsfunktion, såsom SSL-/TLS-kommunikation eller IPsec måste rätt tid ställas in. Du kan göra följande konfigurationer av tiden.

❏ *Fliken Web Config:* ***Enhetshantering*** > ***Datum och tid*** > ***Datum och tid****.*

❏ *Skannerns kontrollpanel:* ***Inst.*** > ***Grundl. inställn.*** > ***Datum-/tidsinställningar****.*

Inställningar	Lokal DB	LDAP	Lokal DB och LDAP
Aktivera autentisering Du behöver aktivera autentisering innan du gör autentiseringsinställningar. ”Aktivera autentisering” på sidan 131	✓	✓	✓
Autentiseringsinställningar Konfigurera Autentiseringsmetod och hur användaren autentiseras. ”Autentiseringsinställningar” på sidan 131	✓	✓	✓
Registrering av Användarinställningar Registrera inställningarna för varje användare. Du kan även registrera användare gruppvis med en CSV-fil. ”Registrering av Användarinställningar” på sidan 133	✓	–	✓
Synkronisera med LDAP-server Gör synkroniseringsinställningar för LDAP-server. ”Synkronisera med LDAP-server” på sidan 139	–	✓	✓
Konfigurera E-postserver Konfigurera inställningar för e-postserver. Konfigurera detta med funktioner som kräver e-postsererinställningar, såsom Skanna t. min e-post. ”Konfigurera e-postservern” på sidan 142	✓	✓	✓
Konfigurera Skanna till min mapp Ställ in målmappar. Ställ in detta vid användning av funktionen Skanna till min mapp. ”Konfigurera Skanna till min mapp” på sidan 143	✓	✓	✓

Inställningar	Lokal DB	LDAP	Lokal DB och LDAP
Anpassa En-touch-funktionerna Konfigurera detta när objekt visas på skannerns kontrollpanel. Du kan bara visa ikonerna du behöver på kontrollpanelen eller ändra ikonernas ordning. "Anpassa En-touch-funktionerna" på sidan 145	✓	✓	✓

Aktivera autentisering

Du behöver aktivera autentisering innan du gör autentiseringsinställningar.

Vid konfiguration från Web Config:

Välj **På (Enhet/LDAP-server)** från fliken **Produktsäkerhet** > **Grundläggande** > **Autentisering**.

Vid konfiguration från Epson Device Admin:

I konfigurationsmallen väljer du **På (Enhet/LDAP-server)** från **Administrator Settings** > **Authentication Settings** > **Basic** > **Authentication**.

Anmärkning:
Om du aktiverar Autentiseringsinställningar på skannern, Låsinställning aktiveras det också för kontrollpanelenl. Kontrollpanelen kan inte låsas upp när Autentiseringsinställningar är aktiverad.

Även om du inaktiverar Autentiseringsinställningar, förblir Låsinställning aktiverad. Om du vill inaktivera det kan du göra inställningar från kontrollpanelen eller Web Config.

Relaterad information

➡ "Konfigurera Låsinställning från kontrollpanelen" på sidan 83
➡ "Konfigurera Låsinställning från Web Config" på sidan 83

Autentiseringsinställningar

Konfigurera Autentiseringsmetod och hur användaren autentiseras.

Vid konfiguration från Web Config:

Välj fliken **Produktsäkerhet** > **Autentiseringsinställningar**.

Vid konfiguration från Epson Device Admin:

Välj **Administrator Settings** > **Authentication Settings** > **Authentication Settings** från konfigurationsmallen.

Objekt	Förklaring
Autentiseringsmetod	Välj Autentiseringsmetod. ❏ Lokal DB Autentisera med Användarinställningar som registrerats på skrivaren. Det är nödvändigt att registrera användaren på skannern. ❏ LDAP Autentisera användarinformationen för LDAP-servern som synkroniserats med skannern. Du måste konfigurera inställningar för LDAP-servern i förväg. ❏ Lokal DB och LDAP Autentisera med användarinformationen som registrerats för skrivaren eller LDAP-servern som synkroniserats med skannern. Det är nödvändigt att registrera användarinformationen på skannern och konfigurera LDAP-servern.
Hur en användare autentiseras	Välj hur du vill autentisera en användare. ❏ Kort eller Användar-ID och lösenord Använd ett autentiseringskort för att autentisera användare. Du kan även använda ett användar-ID och lösenord för att autentisera. ❏ Användar-ID och lösenord Använd ett användar-ID och lösenord för att autentisera användare. Du kan inte använda ett autentiseringskort för att autentisera när du väljer den här funktionen. ❏ Användar-ID Använd bara ett användar-ID för att autentisera användare. Du behöver inte konfigurera ett lösenord. ❏ Kort eller ID-nummer Använd ett autentiseringskort för att autentisera användare. Du kan också använda ett ID-nummer. ❏ ID-nummer Använd bara ett ID-nummer för att autentisera användare.
Tillåt att användare registrerar autentiseringskort	Aktivera om du vill tillåta användare registrera autentiseringskortet för systemet. Om du väljer **LDAP** för **Autentiseringsmetod**, kan du inte konfigurera det. För mer information om hur användare kan registrera sina autentiseringskort, se ”Registrera ett autentiseringskort” i *Användarhandbok*.
Det minsta antalet siffror i ID-nummer	Välj minsta nummer för siffror i ID-numret.
Buffrar för LDAP autentiserade användare	När du använder LDAP-serverautentisering kan du ställa in huruvida det ska användas för att cachelagra användarinformation.
Använd användarinformation i SMTP-autentisering	När du använder ett användar-ID och lösenord för autentisering kan du ställa in huruvida användarinformationen ska användas för SMTP-autentisering. Systemet använder senaste inloggade användar-ID och lösenord.
Begränsningar för LDAP-autentiserade användare	Om du använder LDAP, kan du konfigurera funktioner som är tillgängliga för användaren.

Registrering av Användarinställningar

Registrera Användarinställningar som används för användarautentisering. Du kan registrera med någon av följande metoder.

❏ Registrering av Användarinställningar en i taget (Web Config)

❏ Registrera flera Användarinställningar Med en batch och CSV-fil (Web Config)

❏ Registrera flera User Settings till flera skannrar som en batch med en konfigurationsmalll (Epson Device Admin)

Relaterad information

➡ ”Registrera Användarinställningar individellt (Web Config)” på sidan 133

➡ ”Registrera flera Användarinställningar Med en CSV-fil (Web Config)” på sidan 134

➡ ”Registrera User Settings för flera skannrar som en batch (Epson Device Admin)” på sidan 137

Registrera Användarinställningar individellt (Web Config)

Öppna Web Config och välj fliken **Produktsäkerhet** > **Användarinställningar** > **Lägg till**, och öppna Användarinställningar.

Objekt	Förklaring
Användar-ID	Ange användar-ID du vill använda för autentiserign inom ett område på 1 till 83 byte som kan uttryckas i Unicode (UTF-8). Eftersom användar-ID inte är skiftlägeskänsligt kan du använda versaler och gemena bokstäver för att logga in.
Visning av användarnamn	Ange användarnamnet som visas på skannerns kontrollpanel inom 32 tecken med Unicode (UTF-16). Du kan lämna detta tomt.
Lösenord	Ange lösenordet för att använda autentisering med 32 tecken i ASCII. Lösenordet är skiftlägeskänsligt. Lämna det här fältet tomt om du väljer **Användar-ID** för **Hur en användare autentiseras**.
Autentiseringskort-ID	Ange lösenordet för att använda autentisering med 116 tecken i ASCII. Du kan lämna detta tomt. När du godkänner **Tillåt att användare registrerar autentiseringskort** för **Autentiseringsinställningar**, registreras det registrerade resultatet av användare.
ID-nummer	Detta objekt visas när **Kort eller ID-nummer** eller **ID-nummer** har valts i **Autentiseringsinställningar** > **Hur en användare autentiseras**. Ange ett nummer som faller någonstans mellan det nummer som konfigurerats i **Autentiseringsinställningar** > **Det minsta antalet siffror i ID-nummer** och är upp till 8 siffror.
Skapa automatiskt	Detta objekt visas när **Kort eller ID-nummer** eller **ID-nummer** har valts i **Autentiseringsinställningar** > **Hur en användare autentiseras**. Klicka för att automatiskt generera ett ID-nummer med samma antal siffror du har valt i **Det minsta antalet siffror i ID-nummer**.
Avdelning	Ange användarnamnet som visas inom 40 tecken med Unicode (UTF-16). Du kan lämna detta tomt.

Objekt	Förklaring
E-postadress	Ange användarens e-postadress för att använda autentisering med 200 tecken i ASCII. Detta används som mål för **Skanna t. min e-post**. Du kan lämna detta tomt.
Skanna till min mapp	Ange de sparade destinationerna individuellt när du väljer **Enskild** i **Skanna till min mapp** > **Inställningstyp**. Se följande för mer information om inställningsobjekt. "Konfigurera Skanna till min mapp" på sidan 143
Begränsningar	Du kan begränsa funktionerna för varje användare. Välj funktionen som du tillåter att användas.
Förinställningar	Du kan ställa in upp till fem förinställningar som bara är tillgängliga för den valda användaren från Förinställningar som registrerats i skannern. ❏ Förinställningar som inte allokerats till en användare kan användas av användaren. Förinställningar som inte registrerats av en autentiserad användare kan användas av alla användare. ❏ Om en användare endast har en Förinställningar tillgänglig, som automatiskt läses in efter autentisering. Om flera Förinställningar är tillgängliga visas en lista över Förinställningar efter autentisering. ❏ Du kan inte skapa eller visa Förinställningar som använder funktioner som har begränsats i **Begränsningar**.

Registrera flera Användarinställningar Med en CSV-fil (Web Config)

Ange inställningar för varje användare i en CSV-fil och registrera dem som en batch.

Skapa en CSV-fil

Skapa en CSV-fil för att importera Användarinställningar.

Anmärkning:
Om du registrerar en eller flera Användarinställningar i förväg och sedan exporterar en formaterad fil (CSV-fil), kan du använda den registrerade inställningen som en referens för att ange konfiguration av objekt.

1. Öppna Web Config och välj fliken **Produktsäkerhet** > **Användarinställningar**.
2. Klicka på **Exportera**.
3. Välj filformat för **Filformat**.

   Välj detta genom att se nedan.

Objekt	Förklaring
CSV UTF-16 (tabulatorseparerad)	Välj när du redigerar filen med Microsoft Excel. Varje parameter omsluts av "[ ]" (hakparanteser). Ange parametrar i "[ ]". När du uppdaterar filen rekommenderar vi att du skriver över filen. Om du nyligen har sparat filen väljer du Unicode-text (*.txt) för filformat.

Objekt	Förklaring
CSV UTF-8 (kommaseparerad)	Välj när du redigerar filen med en textredigerare eller makro utan Microsoft Excel.
CSV UTF-8 (semikolonseparerad)	

4. Klicka på **Exportera**.

5. Redigera och spara denna CSV-fil i ett kalkylarksprogram, såsom Microsoft Excel eller i en textredigerare.

> ***Viktigt:***
> *När du redigerar filen ska du inte ändra kodnings- och rubrikinformation.*

Inställningsalternativ för CSV-fil

Objekt	Inställningar och förklaringar
UserID	Ange användar-ID för att använda atuentisering mellan 1 och 83 byte i Unicode.
UserName	Ange användarnamnet som visas på skrivarens kontrollpanel inom 32 tecken med Unicode. Du kan lämna detta tomt.
Password	Ange lösenordet för att använda autentisering med 32 tecken i ASCII. Vid import ställs det här lösenordet in istället för **EncPassword**. Lämna det här fältet tomt om du väljer **Användar-ID** för **Hur en användare autentiseras**. Vid export är det här alltid tomt.
AuthenticationCardID	Ange läsresultat för autentiseringskort. När du godkänner **Tillåt att användare registrerar autentiseringskort** för **Autentiseringsinställningar**, registreras det registrerade resultatet av användare. Ange max 116 tecken ASCII. Du kan lämna detta tomt.
IDNumber	Detta objekt visas när **Kort eller ID-nummer** eller **ID-nummer** har valts i **Autentiseringsinställningar** > **Hur en användare autentiseras**. Ange ett nummer som faller någonstans mellan det nummer som konfigurerats i **Autentiseringsinställningar** > **Det minsta antalet siffror i ID-nummer** och är upp till 8 siffror. Ett ID-nummer kan inte dupliceras. Om det dupliceras får du ett varningsmeddelande om fel vid import av filen. När det lämnas tomt tilldelas det automatiskt en siffra.
Department	Ange ett annat avdelningsnamn för att särskilja användare. Ange med högst 40 tecken i Unicode. Du kan lämna detta tomt.
MailAddress	Ange e-postadress för användare. Detta används som mål för **Skanna t. min e-post**. Du kan använda A-Z, a-z, 0-9, !#'%&'*+-./=?^_{|}~@. Ange 200 tecken eller mindre. Du kan inte använda "," (komma) för första tecknet. Du kan lämna detta tomt.
FolderProtocol	Ställ in typ av Skanna till min mapp-funktion. Nätverksmapp/FTP (SMB): 0, FTP: 1
FolderPath	Ställ in destination för att spara för Skanna till min mapp-funktionen.

Objekt	Inställningar och förklaringar
FolderUserName	Ställ in användarnamn för Skanna till min mapp-funktionen.
FolderPassword	Ställ in ett lösenord för att autentisera destinationsmappen för Skanna till min mapp-funktionen inom 32 ASCII-tecken. Vid import ställs det här lösenordet in istället för **EncPassword**. Vid export är det här alltid tomt.
FtpPassive	Ställ in anslutningsläge för FTP-server när **FTP** är vald som **Typ** för Skanna till min mapp-funktionen. Aktivt läge: 0, Passivt läge: 1
FtpPort	Ställ in portnummer för att skicka skannat data till FTP-server från 0 till 65535 när **FTP** är vald som **Typ** för Skanna till min mapp-funktionen.
ScanToMemory	Konfigurera begrsänsningar för Skanna till USB-enhet. Ej tillåten: 0, Tillåten: 1
ScanToMail	Konfigurera begrsänsningar för Skanna till e-post. Du kan konfigurera **Skanna till min e-post** endast när **Skanna till e-post** har aktiverats. Ej tillåten: 0, Tillåten: 1
ScanToFolder	Konfigurera begrsänsningar för Skanna till nätverksmapp/FTP. Du kan konfigurera **Skanna till min mapp** endast när **Skanna till nätverksmapp/FTP** har aktiverats. Ej tillåten: 0, Tillåten: 1
ScanToCloud	Konfigurera begrsänsningar för Skanna till moln. Ej tillåten: 0, Tillåten: 1
ScanToComputer	Konfigurera begrsänsningar för Skanna till dator. Ej tillåten: 0, Tillåten: 1
PresetIndex	Ställer in de Förinställningar du vill associera med användaren. Du kan ställa in upp till fem registreringsnummr för Förinställningar som separeras av komman.
EncPassword	Vid export av användarinformation krypteras parameterkonfigurationen för **Password** och sedan kodas värdet av BASE64 och utskriften. Vid import med det nya lösenordet för **Password**, ignoreras det här värdet. Om **Password** är tomt används det här värdet och lösenordet förblir som det var före exporten.
EncFolderPassword	Vid export krypteras parametern som ställts in för [**FolderPassword**] och sedan kodas värdet med BASE64 och matas ut. Vid import med det nya lösenordet för **FolderPassword**, ignoreras det här värdet. Om **FolderPassword** är tomt används det här värdet och lösenordet förblir som det var före exporten.

Importera en CSV-fil

1. Öppna Web Config och välj fliken **Produktsäkerhet** > **Användarinställningar**.

2. Klicka på **Importera**.
3. Välj filen som du vill importera.
4. Klicka på **Importera**.
5. Efter att du kontrollerat den information som visas klickar du på **OK**.

Registrera User Settings för flera skannrar som en batch (Epson Device Admin)

Du kan registrera User Settings som används i Lokal DB som en batch genom att använda en LDAP-server eller en CSV/ENE-fil.

Anmärkning:
*ENE-filen är en binär fil som tillhandahålls av Epson som krypterar och sparar information för **Contacts** såsom personlig information och Användarinställningar. Den kan exporteras från Epson Device Admin och ett lösenord kan konfigureras. Detta är praktiskt när du vill importera Användarinställningar från en säkerhetskopieringsfil.*

Importera från CSV-/ENE-fil

1. Välj **Administrator Settings** > **Authentication Settings** > **User Settings** från konfigurationsmallen.
2. Klicka på **Import**.
3. Välj **CSV or ENE File** i **Import Source**.
4. Klicka på **Browse**.

   Skärmen för filval visas.
5. Välj filen som du vill importera för att öppna den.
6. Välj importmetod.
   - ❏ Overwrite and Add: skriver över om samma ID finns; lägger till ett nytt ID om det inte finns.
   - ❏ Replace All: ersätter allt med användarinställningar du vill imortera.
7. Klicka på **Import**.

   Bekräftelseskärmen för inställningar visas.
8. Klicka på **OK**.

   Valideringsresultatet visas.

   Anmärkning:
   - ❏ *Om antalet importerade användarinställningar överskrider antalet som kan importeras visas ett meddelande där du ombeds radera vissa användarinställningar. Radera alla extra användarinställningar före import.*
   - ❏ *Välj de användarinställningar som du vill radera före import och klicka sedan på **Delete**.*

9. Klicka på **Import**.

   Användarinformationen importeras till konfigurationsmallen.

Importera från LDAP-server

1. Välj **Administrator Settings** > **Authentication Settings** > **User Settings** från konfigurationsmallen.
2. Klicka på **Import**.
3. Välj **LDAP** i **Import Source**.
4. Klicka på **Settings**.

   Inställningarna för **LDAP Server** visas.

   Anmärkning:
   Denna LDAP-serverinställning är den inställning som används för att importera användarinformation från LDAP-servern till servern. Den importerade (kopierade) användarinställningsinformationen används för att autentisera användare av själva skannern.

   *Å andra sidan, när du väljer **LDAP** eller **Local DB and LDAP** som autentiseringsmetod, autentiseras användare genom att kommunicera med LDAP-servern.*

5. Konfigurera varje objekt.

   När användarinformation importeras från en LDAP-server kan du utöver LDAP-inställningarna göra följande inställningar.

   För mer information, se Relaterad information.

Objekt			Förklaring
LDAP Server Settings	LDAP Server Type		Gör det möjligt att välja typ av LDAP-server.
Search Settings	Search Filter		Du kan konfigurera texten som används för LDAP-sökfilter. Välj **Custom** för att redigera söktexten.
	Options	Type	Du kan konfigurera typen för att spara mål för **Scan To My Folder**.
		Connection Mode	När **Type** är inställt på **FTP**, kan du konfigurera FTP-anslutningsläge.
		Port Number	När **Type** är inställt på **FTP**, kan du konfigurera portnumret du vill använda.

6. Utför anslutningstestet enligt önskemål genom att klicka på **Connection Test**.

   Anskaffar och visar 10 användarinställningar från LDAP-servern.

7. Klicka på **OK**.
8. Välj importmetod.

   ❏ Overwrite and Add: skriver över om samma ID finns; lägger till ett nytt ID om det inte finns.

   ❏ Replace All: ersätter allt med användarinställningar du vill imortera.

9. Klicka på **Import**.

   Bekräftelseskärmen för inställningar visas.

10. Klicka på **OK**.

    Valideringsresultatet visas.

11. Klicka på **Import**.

    Användarinformationen importeras till konfigurationsmallen.

Relaterad information

➡ ”Konfigurera en LDAP-server” på sidan 139
➡ ”Konfigurera sökinställningar för en LDAP-server” på sidan 141

Synkronisera med LDAP-server

Gör inställningar av LDAP-server för skannern.

Gör inställningar för både primär och sekundär server, efter behov.

Anmärkning:
*Inställningarna för **LDAP-server** delas med **Kontakter**.*

Tillgängliga tjänster

Följande katalogtjänster stöds.

Tjänstenamn	Version
Active Directory	Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
OpenLDAP	Ver.2.3, Ver.2.4

Konfigurera en LDAP-server

För att använda en LDAP-server behöver du konfigurera LDAP-servern.

Vid konfiguration från Web Config:

Välj fliken **Nätverk** > **LDAP-server** > **Grundläggande (Primär server)** eller **Grundläggande (Sekundär server)**.

Om du väljer **Kerberos-autentisering** som **Autentiseringsmetod**, väljer du **Nätverk** > **Kerberosinställningar** för att göra inställningar för Kerberos.

Vid konfiguration från Epson Device Admin:

Välj **Network** > **LDAP server** > **Server Settings (Primary Server)** eller **Server Settings (Secondary Server)** från konfigurationsmallen.

Om du väljer **Kerberos-autentisering** som **Autentiseringsmetod**, väljer du **Network** — **Security** > **Kerberosinställningar** för att göra inställningar för Kerberos.

Objekt	Inställningar och förklaringar
Använd LDAP-server	Välj **Använd** eller **Använd inte**.
LDAP-serveradress	Ange LDAP-serveradressen. Ange mellan 1 och 255 tecken med IPv4-, IPv6- eller FQDN-format. För FQDN-format kan du använda alfanumeriska tecken i ASCII (0x20–0x7E) och binestreck, förutom för början och slutet av adressen.
Portnummer för LDAP-server (Port number)	Ange LDAP-servers portnummer mellan 1 och 65535.
Säker anslutning	Ange autentiseringsmetoden som skannern ska använda för åtkomst till LDAP-servern.
Certifikatverifiering	LDAP-serverns certifikat är autentiserat när detta är aktiverat. Vi rekommenderar att du ställer in detta på **Aktivera**. För att utföra konfigurationen behöver **CA-certifikat** importeras till skannern.
Söktimeout (sek)	Ställ in tidslängden för sökning mellan 5 och 300 sekunder.
Autentiseringsmetod	Välj autentiseringsmetod. Om du väljer **Kerberos-autentisering**, gör du inställningarna för Kerberos i förväg. För att utföra Kerberos-autentisering, krävs följande miljö. ❏ Skannern och DNS-servern kan kommunicera. ❏ Tiden för skannern, KDC-servern och servern som krävs för autentisering (LDAP-server, SMTP-server, filserver) synkroniseras. ❏ När tjänsteservern tilldelas som IP-adress registreras FQDN för tjänsteservern på den omvända sökzonen för DNS-servern.
Kerberos-resurs som ska användas	Om du väljer **Kerberos-autentisering** för **Autentiseringsmetod**, välj den Kerberos-sfär som du vill använda.
Administratörs-DN / Användarnamn	Ange användarnamnet för LDAP-servern med 128 tecken eller mindre i Unicode (UTF-8). Du kan inte använda kontrolltecken som 0x00–0x1F och 0x7F. Denna inställning används inte när **Anonym autentisering** är vald som **Autentiseringsmetod**. Om du inte vill registrera detta, lämna det tomt.
Lösenord	Ange lösenorden för LDAP-serverautentisering med 128 tecken eller mindre i Unicode (UTF-8). Du kan inte använda kontrolltecken som 0x00–0x1F och 0x7F. Denna inställning används inte när **Anonym autentisering** är vald som **Autentiseringsmetod**. Om du inte vill registrera detta, lämna det tomt.

Inställningar för Kerberos

Om du väljer **Kerberos-autentisering** som **Autentiseringsmetod**-inställning måste du göra inställningar för Kerberos. Du kan registrera upp till 10 Kerberos-inställningar.

Vid konfiguration från Web Config:

Välj fliken **Nätverk** > **Kerberosinställningar**.

Vid konfiguration från Epson Device Admin:

Välj **Network** > **Security** > **Kerberosinställningar** från konfigurationsmallen.

Objekt	Inställningar och förklaringar
Resurs (domän)	Ange sfären för Kerberos-autentisering med max 255 tecken i ASCII (0x20–0x7E). Om du inte vill registrera detta, lämna det tomt.
KDC-adress	Ange adressen på Kerberos-autentiseringsservern. Ange 255 tecker eller mindre antingen i IPv4-, IPv6- eller FQDN-format. Om du inte vill registrera detta, lämna det tomt.
Portnummer (Kerberos)	Ange Kerberos-servers portnummer mellan 1 och 65535.

Konfigurera sökinställningar för en LDAP-server

Konfigurerar sökattribut för användarinställningar.

Vid konfiguration från Web Config:

Välj fliken **Nätverk** > **LDAP-server** > **Sökinställningar (autentisering)**.

Vid konfiguration från Epson Device Admin:

Välj **Administrator Settings** > **Authentication Settings** > **LDAP server** > **Search Settings (Authentication)** från konfigurationsmallen.

Objekt	Inställningar och förklaringar
Search Base (Distinguished Name)	Specificera startposition för sökning av användarinformationen när du söker den från LDAP-servern. Ange mellan 0 och 128 tecken i Unicode (UTF-8). Om du inte söker för egenmäktig attribut, lämna detta tomt. Exempel på den lokala serverkatalogen: dc=server,dc=local
User ID Attribute	Specificera attributnamnet som skall visas när du söker efter ID-nummer. Ange mellan 1 och 255 tecken i ASCII. Det första tecknet skall vara a–z eller A–Z. Exempel: cn, uid
User name Display Attribute	Specificera attributnamnet som skall visas som användarnamn. Ange mellan 0 och 255 tecken i ASCII. Det första tecknet skall vara a–z eller A–Z. Du kan lämna det här tom. Exempel: cn, name
Authentication Card ID Attribute	Specificera attributnamnet som skall visas som kort-ID för autentisering. Ange mellan 0 och 255 tecken i ASCII. Det första tecknet skall vara a–z eller A–Z. Du kan lämna det här tom. Exempel: cn, sn
ID Number Attribute	Specificera attributnamnet som skall visas när du söker efter ID-nummer. Ange mellan 1 och 255 tecken i ASCII. Det första tecknet skall vara a–z eller A–Z. Exempel: cn, id
Department Attribute	Specificera attributnamnet som skall visas som avdelningsnamn. Ange mellan 0 och 255 tecken i ASCII. Det första tecknet skall vara a–z eller A–Z. Du kan lämna det här tom. Exempel: ou, ou-cl
Email Address Attribute	Specificera attributnamnet som skall visas när du söker efter e-postadresser. Ange mellan 1 och 255 tecken i ASCII. Det första tecknet skall vara a–z eller A–Z. Exempel: mail

Objekt	Inställningar och förklaringar
Save To Attribute	Specificera attributnamnet som används för att spara destinationen för Scan To My Folder. Ange mellan 0 och 255 tecken i ASCII. Exempel: homeDirectory

Kontrollera LDAP-serverns anslutning

Utför anslutningstestet till LDAP-servern genom att använda parameteruppsättningen på **LDAP-server** > **Sökinställningar**.

1. Öppna Web Config och välj fliken **Nätverk** > **LDAP-server** > **Anslutningstest**.
2. Välj **Starta**.

   Anslutningstestet startades. Efter testet, kontrollera rapporten som visas.

Referens för anslutningstest av LDAP-server

Meddelanden	Förklaring
Anslutningstest lyckades.	Detta meddelande visas när anslutningen till servern lyckades.
Anslutningstest misslyckades. Kontrollera inställningarna.	Detta meddelande visas av följande orsaker: ❏ LDAP-serverns adress eller portnummer är fel. ❏ Det kom till en timeout. ❏ **Använd inte** är vald som **Använd LDAP-server**. ❏ Om **Kerberos-autentisering** är vald som **Autentiseringsmetod** är inställningar som **Resurs (domän)**, **KDC-adress** och **Portnummer (Kerberos)** fel.
Anslutningstest misslyckades. Kontrollera Datum och tid på din produkt eller server.	Detta meddelande visas när anslutningen misslyckas eftersom tidsinställningarna för skannern och LDAP-servern inte matchar varandra.
Autentisering misslyckades. Kontrollera inställningarna.	Detta meddelande visas av följande orsaker: ❏ **Användarnamn** och/eller **Lösenord** är fel. ❏ Om **Kerberos-autentisering** är vald som **Autentiseringsmetod**, tiden/datumen kan inte konfigureras.
Det går inte att komma åt produkten förrän bearbetningen är klar.	Detta meddelande visas när skannern är upptagen.

Konfigurera e-postservern

När du använder **Skanna t. min e-post**, konfigurera du e-postserver.

Anmärkning:
*Du kan konfigurera **Skanna t. min e-post** endast när **Skanna till e-post** har aktiverats.*

Vid konfiguration från Web Config:

Välj fliken **Nätverk** > **E-postserver** > **Grundläggande**.

Vid konfiguration från Epson Device Admin:

Välj **Common** > **Email Server** > **Mail Server Settings** från konfigurationsmallen.

Objekt	Inställningar och förklaringar	
Autentiseringsmetod	Ange autentiseringsmetoden som skannern ska använda för åtkomst till e-postservern.	
	Av	Autentisering är inaktiverad vid kommunikation med meddelandeservern.
	SMTP AUT.	E-postservern behöver ha stöd för SMTP-autentisering.
	POP före SMTP	När du väljer det här objektet, ska du konfigurera POP3-servern.
Autentiseringskonto	Om du väljer **SMTP AUT.** eller **POP före SMTP** som **Autentiseringsmetod**, anger du det autentiserade kontonamnet. Ange mellan 0 och 255 tecken i ASCII (0x20–0x7E).	
Autentiserat lösenord	Om du väljer **SMTP AUT.** eller **POP före SMTP** som **Autentiseringsmetod**, anger du det autentiserade lösenordet. Ange mellan 0 och 20 tecken i ASCII (0x20–0x7E).	
Avsändarens e-postadress	Ange avsändarens e-postadress. Ange mellan 0 och 255 tecken i ASCII (0x20–0x7E) förutom : ( ) < > [ ] ; ¥. Det första tecknet kan inte vara en punkt ".".	
SMTP-serveradress	Ange mellan 0 och 255 tecken med A–Z a–z 0–9 . -. Du kan använda IPv4- eller FQDN-format.	
SMTP-serverportnummer	Ange ett nummer mellan 1 och 65535.	
Säker anslutning	Ange säker anslutningsmetod för e-postservern.	
	Saknas	Om du väljer **POP före SMTP** i **Autentiseringsmetod**, är anslutningsmetoden inställd på **Saknas**.
	SSL/TLS	Detta är tillgängligt när **Autentiseringsmetod** är satt till **Av** eller **SMTP AUT.**.
	STARTTLS	Detta är tillgängligt när **Autentiseringsmetod** är satt till **Av** eller **SMTP AUT.**.
Certifikatverifiering	Certifikatet är validerat när detta är aktiverat. Vi rekommenderar att du ställer in detta på **Aktivera**.	
POP3-serveradress	Om du väljer **POP före SMTP** som **Autentiseringsmetod**, anger du POP3-serveradressen. Ange mellan 0 och 255 tecken med A–Z a–z 0–9. Du kan använda IPv4- eller FQDN-format.	
POP3-serverportnummer	Om du väljer **POP före SMTP** som **Autentiseringsmetod**, anger du portnumret. Ange ett nummer mellan 1 och 65535.	

Konfigurera Skanna till min mapp

Spara de skannade bilderna i den mapp som tilldelats varje användare. Du kan ställa in följande som en dedikerad mapp.

Anmärkning:
*Du kan konfigurera **Scan To My Folder** endast när **Skanna till nätverksmapp/FTP** har aktiverats.*

Spara till inställningar	Autentiseringsmetod	Plats för inställningar av mappsökväg
Specificera en nätverksmapp för hela Autentiseringsinställningar för att automatiskt skapa en personlig mapp under den specificerade mappen med namnet för ditt användar-ID.	❏ Lokal DB ❏ LDAP ❏ Lokal DB och LDAP	Skannerinställningar (Skanna till min mapp)
Tilldela olika nätverksmappar individuellt till varje användare.	Lokal DB	Skanner (Användarinställningar)
	LDAP	LDAP-attribut
	Lokal DB och LDAP	Skanner (Användarinställningar) eller LDAP-attribut

Vid konfiguration från Web Config:

Välj fliken **Produktsäkerhet** > **Skanna till nätverksmapp/FTP**.

Vid konfiguration från Epson Device Admin:

Välj **Administrator Settings** > **Authentication Settings** > **Skanna till nätverksmapp/FTP** > **Scan to My Folder** från konfigurationsmallen.

Objekt		Förklaring
Spara till Inställning	Inställningstyp	❏ **Delad**: Skapar automatiskt en mapp som döpts efter användarens ID under mappsökvägen eller URL som specificerats i **Spara till** och sparar skanningsresultatet till den mappen. ❏ **Enskild**: Ställ in destinationen att spara skanningsresultatet på, för alla användare. Lokal DB användare kan ställas in i användarinställningarna. LDAP användare använder lagringsplats som anskaffas från LDAP-serverns sökattribut.
	Typ	Välj sändningsprotokoll enligt skanningutmatningsmålet. För en nätverksmapp: **Nätverksmapp (SMB)** För en FTP-server: **FTP**
	Spara till	Specificera sökvägen eller URL för utgående sökväg. Ange med högst 160 tecken i Unicode (UTF-16).
	Anslutningsläge	Ställ in när du väljer **FTP** i **Typ**. Välj ett anslutningsläge för FTP-servern.
	Portnummer	Ställ in när du väljer **FTP** i **Typ**. Ange portnumret för att skicka de skannade data till en FTP-server mellan 0 och 65535.

Objekt		Förklaring
Autentiseringsinställningar	Inställningstyp	Konfigurera när du väljer **Enskild** som **Inställningstyp** i **Spara till Inställning**. Ställ in Användarnamn och Lösenord för att öppna mappen. ❏ **Delad**: Använd en gemensam **Användarnamn** och **Lösenord** för alla användare. ❏ **Enskild**: För Lokal DB-användare, konfigurerar du **Användarnamn** och **Lösenord** individuellt i **Användarinställningar**. LDAP-användare kan inte konfigureras individuellt. **Användarnamn** och **Lösenord** konfigureras genom detta objekt som används som en batch.
	Användarnamn	Ange användarnamnet för att komma åt målmappen med den utmatade skanningen. Ange med högst 30 tecken i Unicode (UTF-16). Konfigurera detta när du använder **Delad** eller LDAP-server.
	Lösenord	Ange lösenordet som överensstämmer med **Användarnamn**. Ange med högst 20 tecken i Unicode (UTF-16). Konfigurera detta när du använder **Delad** eller LDAP-server.

Förbjud måländring för Skanna till nätverksmapp/FTP

Objekt	Förklaring
Förbjud manuell inmatning av destination	Vid aktivering kan användaren inte ändra standardmål.

Anpassa En-touch-funktionerna

Du kan bara visa nödvändiga ikoner genom att redigera ikonlayouten på startskärmen för kontrollpanelen.

Vid konfiguration från Web Config:

Välj fliken **Produktsäkerhet** > **Anpassa En-touch-funktionerna**.

Vid konfiguration från Epson Device Admin:

Välj **Administrator Settings** > **Authentication Settings** > **Customize One-touch Functions** från konfigurationsmallen.

Anmärkning:
I följande fall visas inte ikonerna för de specificerade funktionerna på startskärmen.

❏ *När du väljer funktioner som inte är tillåtna på grund av **Begränsningar**.*

❏ *När e-postadressen för en inloggad användare som inte är registrerad. (Skanna t. min e-post)*

❏ *När målmappen inte är konfigurerad. (Skanna till min mapp)*

Objekt	Förklaring
Maximala funktioner per skärm	Välj layouten som visas på kontrollpanelen. Bilden ändras enligt den valda layouten.

Objekt	Förklaring
Skärm(ar)	Välj antalet sidor.
Antal	Väljer de funktioner som du vill visa för varje numrerad position.

Job History Rapporter med Epson Device Admin

Du kan skapa en Job History-rapport för varje grupp och varje användare genom att använda Epson Device Admin. Du kan spara upp till 3000 instanser med användningshistorik till skannern. Du kan skapa rapporten genom att specificera en period eller ställa in ett regelbundet schema.

För att skriva ut Job History som en rapport, väljer du **Options** > **Epson Print Admin Serverless/Authentication Settings** > **Manage the Epson Print Admin Serverless/Authentication compatible devices** från färgbandsmenyn på skärmen Enhetslista.

För detaljer kring hur du skapar en användarrapport, se dokumentation för Epson Device Admin.

Objekt som kan inkluderas i rapporten

Du kan skriva ut följande objekt i användarrappporten.

Date/Job ID/Operation/User ID/Department/Result/Result details/Scan: Destination type/Scan: Destination/Scan: Paper Size/Scan: 2-Sided/Scan: Color/Scan: Pages/Devices: Model/Devices: IP Address/Devices: Serial Number/Devices: Department/Devices: Location/Devices: Remark/Devices: Note

Logga in som en administratör från kontrollpanelen

Du kan använda följande metoder för att logga in som administratör från skannerns kontrollpanel.

1. Tryck på  uppe till höger på skärmen.
   - ❏ När Autentiseringsinställningar är aktiverad visas ikonen på skärmen **Välkommen** (autentiseringsstandby-skärm).
   - ❏ När Autentiseringsinställningar inaktiveras visas ikonen på hemskärmen.
2. Tryck på **Ja** när bekräftelseskärmen visas.
3. Ange administratörslösenordet.

   Ett komplett inloggningsmeddelande visas och sedan visas hemskärmen på kontrollpanelen.

Tryck på  uppe till höger på hemskärmen för att logga ut.

Inaktivera Autentiseringsinställningar

Du kan inaktivera Autentiseringsinställningar med Web Config.

Anmärkning:
Användarinställningar som registrerats i skannern sparas även om Autentiseringsinställningar inaktiveras. Du kan ta bort dem genom att återställa skannern till dess standardinställningar.

1. Öppna Web Config.
2. Välj fliken **Produktsäkerhet** > **Grundläggande** > **Autentisering**.
3. Välj **Av**.
4. Klicka på **Nästa**.
5. Klicka på **OK**.

Anmärkning:
Även om du inaktiverar Autentiseringsinställningar, förblir Låsinställning aktiverad. Om du vill inaktivera det kan du göra inställningar från kontrollpanelen eller Web Config.

Relaterad information

➡ ”Konfigurera Låsinställning från kontrollpanelen” på sidan 83
➡ ”Konfigurera Låsinställning från Web Config” på sidan 83

Radera Autentiseringsinställningar Information (Återställ inställningarna)

För att radera all Autentiseringsinställningar information (Kortläsare, Autentiseringsmetod, Användarinställningar, och så vidare), återställer du alla skannerinställningar till standardvärden vid tiden för inköpet.

Välj **Inst.** > **Systemadministration** > **Återställ inställningarna** > **Alla inställningar** på kontrollpanelen.

Viktigt:
Alla kontakter och andra nätverksinställningar raderas också. Raderade inställningar kan inte återställas.

Lösa problem

Kan inte läsa autentiseringskortet

Kontrollera följande.

❏ Kontrollera om autentiseringsenheten är korrekt ansluten till skannern.
Anslut autentiseringsenheten till den externa USB-porten på skannerns baksida.

❏ Kontrollera att autentiseringsenheten och autentiseringskortet stöds.

Underhåll

Rengöra skannern utvändigt

Torka bort fläckar på höljet med en torr trasa eller en fuktig trasa med rengöringsmedel och vatten.

Viktigt:

- ❏ *Använd aldrig alkohol, thinner eller något frätande lösningsmedel för att rengöra skannern. Deformering eller missfärgning kan uppstå.*
- ❏ *Låt inget vatten tränga in i produkten. Detta kan orsaka felfunktion.*
- ❏ *Öppna aldrig skannerns hölje.*

1. Tryck på knappen ⏻ för att stänga av skannern.
2. Koppla ur AC-adaptern från skannern.
3. Rengör det yttre höljet med en trasa som fuktats med ett milt rengöringsmedel och vatten.

   Anmärkning:
   Torka pekskärmen med en mjuk, torr trasa.

Rengöra skannern invändigt

Efter att skannern använts ett tag kan papper och damm på valsen eller på glasytan inuti skanner orsaka kvalitetsförsämringar vid pappersmatning och skanning. Rengör skannern invändigt i intervaller om 5,000 skanningar.

Du kan kontrollera det senaste antalet skanningar på kontrollpanelen eller i Epson Scan 2 Utility.

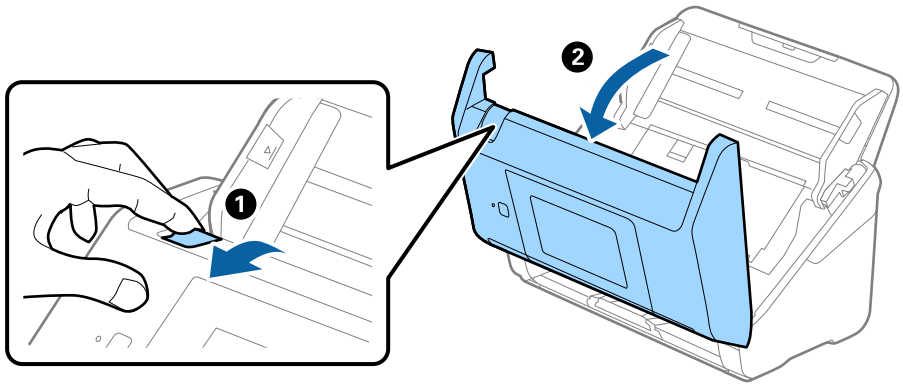
Om en yta får fläckar som är svåra att få bort ska du använda ett Epson-rengöringskit för att ta bort fläckar. Använd en liten mängd rengöringsmedel för rengöringstrasan för att ta bort fläckar.

Viktigt:

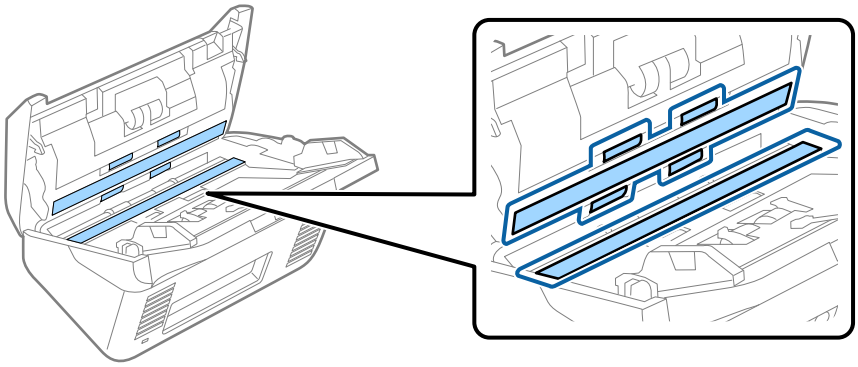
- ❏ *Använd aldrig alkohol, thinner eller något frätande lösningsmedel för att rengöra skannern. Deformering eller missfärgning kan uppstå.*
- ❏ *Spraya aldrig några vätskor eller smörjmedel på skannern. Skada på utrustning eller kretsar kan orsaka onormal drift.*
- ❏ *Öppna aldrig skannerns hölje.*

1. Tryck på knappen ⏻ för att stänga av skannern.
2. Koppla ur AC-adaptern från skannern.

3. Dra i spaken för att öppna skannerlocket.



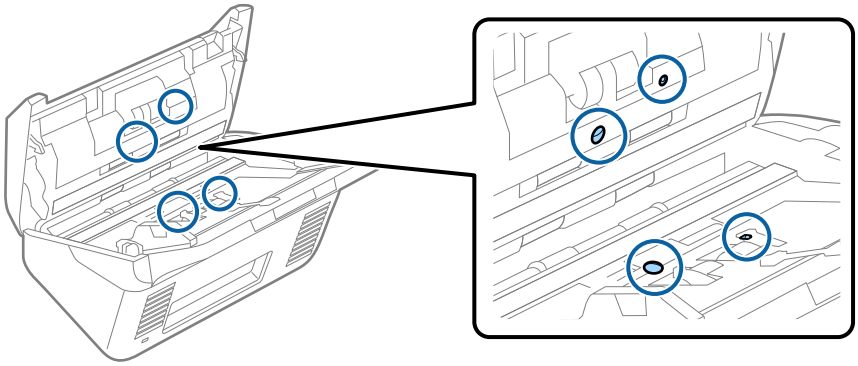
4. Torka bort fläckar på plastrullen och glaset på undersidan av skannern med en mjuk trasa eller ett äkta rengöringskit från Epson.



Viktigt:

- ❏ *Var inte våldsam i hanteringen av glaset.*
- ❏ *Använd inte någon borste eller hårt verktyg. Alla repor på glaset kan påverka skanningkvaliteten.*
- ❏ *Spraya inte glasrengöringsmedel direkt på glasytan.*

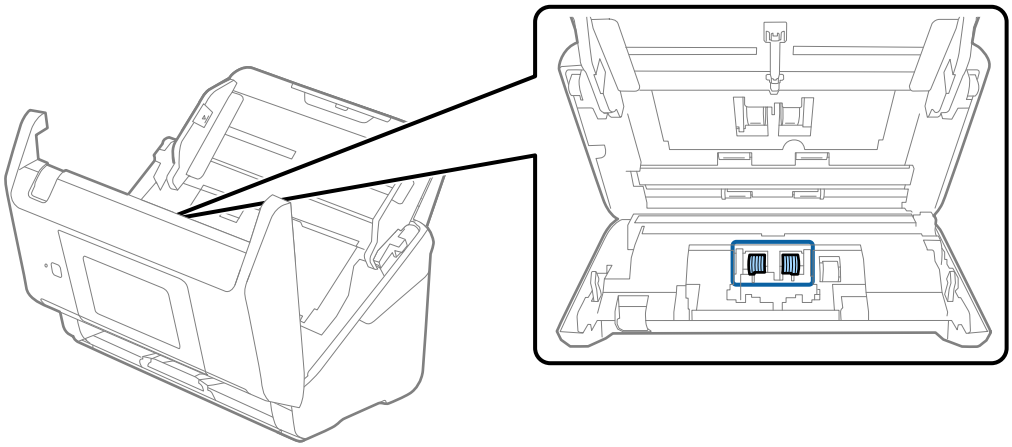
5. Torka bort fläckar på sensorerna med en bomullspad.



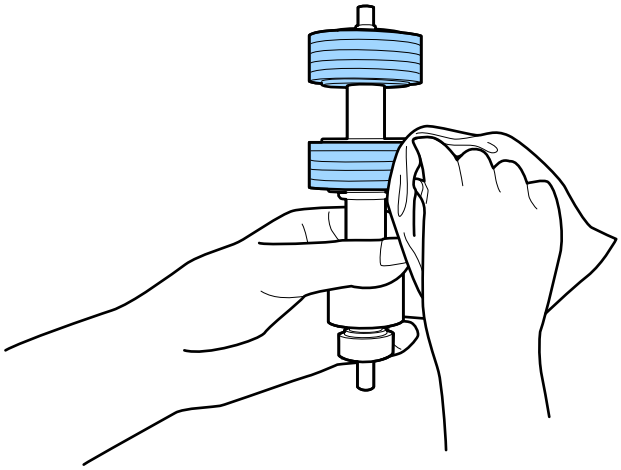
> ***Viktigt:***
> *Använd inte vätskor, såsom rengöringsmedel på en bomullspad.*

6. Öppna luckan och ta sedan bort separationsrullen.

   Se ”Byta rullmonteringskit” för mer information.

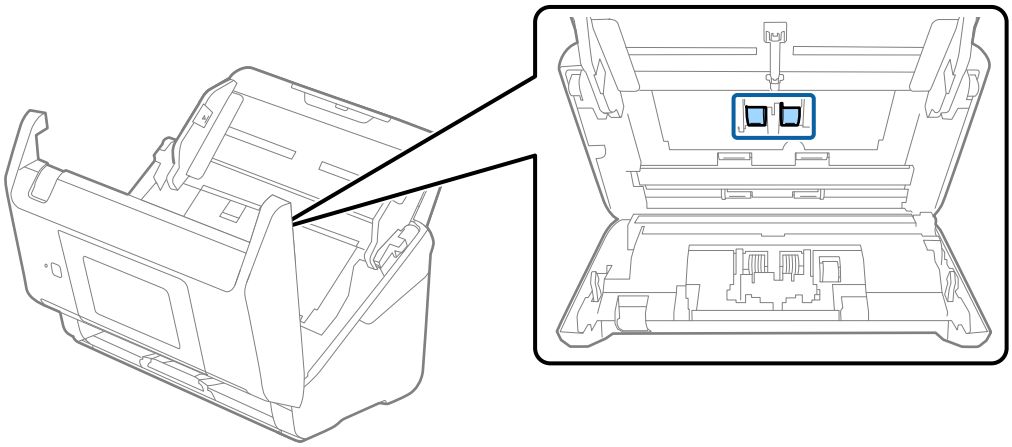


7. Torka bort damm eller smuts på separationsrullen med ett Epson-rengöringskit eller en mju, fuktig trasa.

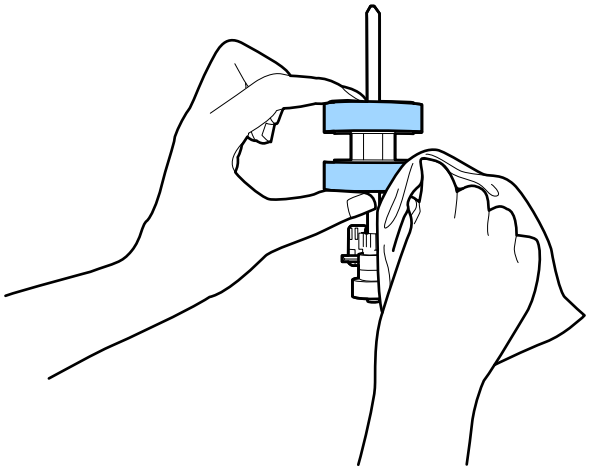


> ***Viktigt:***
> *Använd bara Epson-rengöringskit eller en mjuk, fuktig trasa för att rengöra rullen. Om du använder en torr trasa kan det skada rullens yta.*

8. Öppna luckan och ta sedan bort pickup-rullen.
   Se ”Byta rullmonteringskit” för mer information.



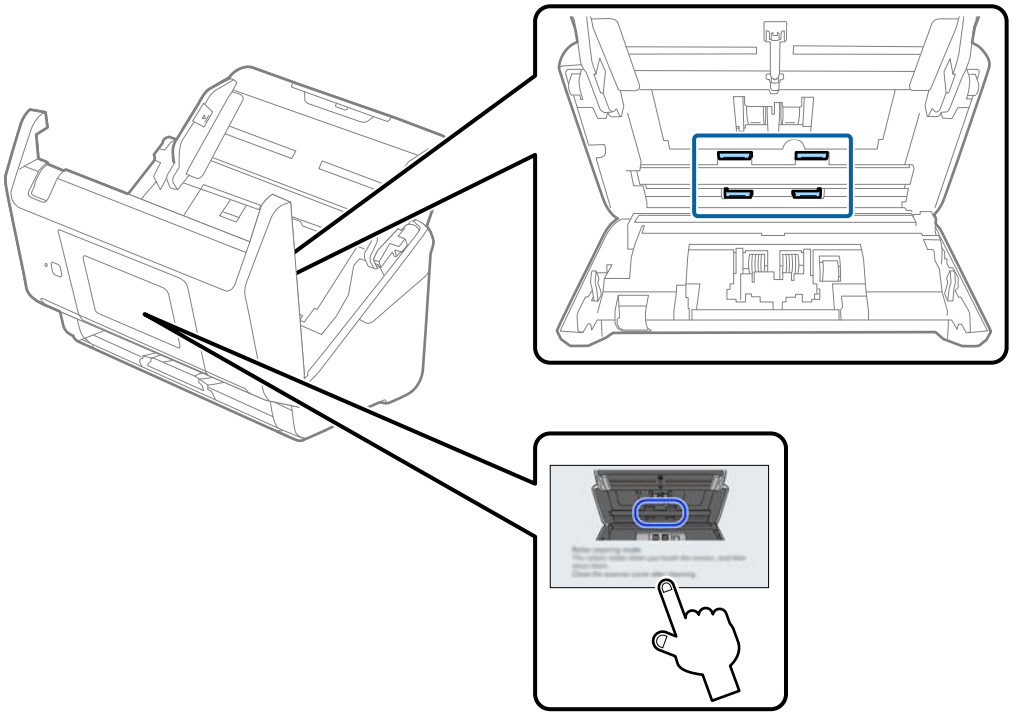
9. Torka bort damm eller smuts på pickuprullen med ett Epson-rengöringskit eller en mju, fuktig trasa.



> ***Viktigt:***
> *Använd bara Epson-rengöringskit eller en mjuk, fuktig trasa för att rengöra rullen. Om du använder en torr trasa kan det skada rullens yta.*

10. Stäng skannerlocket.
11. Koppla in AC-adaptern och slå på skannern.
12. Välj **Underhåll av skanner** från hemskärmen.
13. På skärmen **Underhåll av skanner** väljer du **Rengöring av rulle**.
14. Dra i spaken för att öppna skannerlocket.
    Skannern öppnar rengöringsläget för rullen.

15. Snurra långsamt rullarna längst ned genom att trycka var som helst på LCD-skärmen. Torka av ytan på rullarna med ett äkta Epson-rengöringskit eller en mjuk trasa fuktad med vatten. Upprepa detta tills rullarna är rena.



> ***Obs!***
>
> *Var försiktig så du inte fastnar med händerna i mekanismen när du använder rullen. Det kan orsaka personskada.*

16. Stäng skannerlocket.

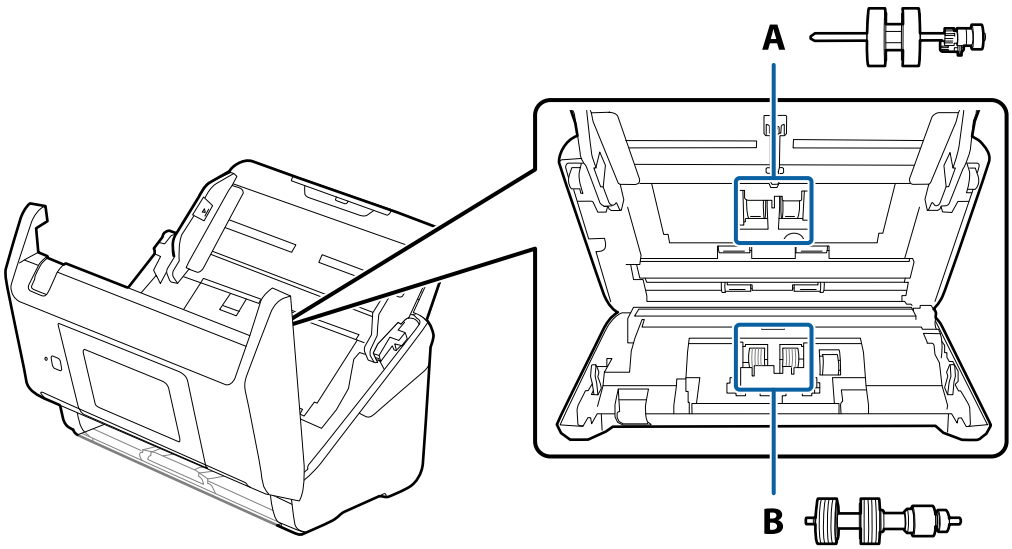
    Skannern stänger rengöringsläget för rullen.

Relaterad information

➡ ”Byta rullmonteringskit” på sidan 154

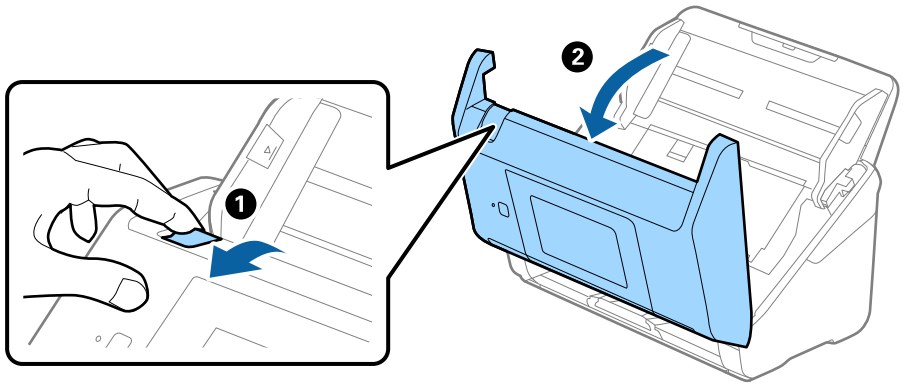
Byta rullmonteringskit

Rullmonteringskitet (pickup-rullen och separationsrullen) behöver bytas när antalet skanningar överskrider livscykeln för rullarna. När ett bytesmeddelande visas på kontrollpanelen eller datorn ska du följa stegen nedan för att verkställa bytet.

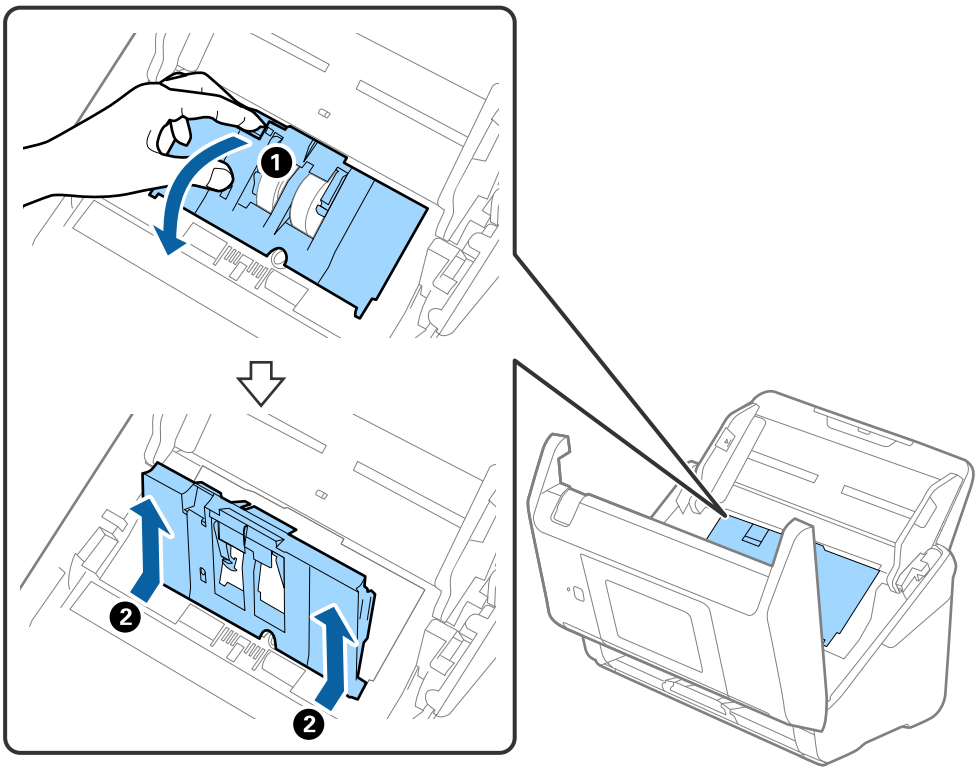


A: pickup-rulle, B: separationsrulle

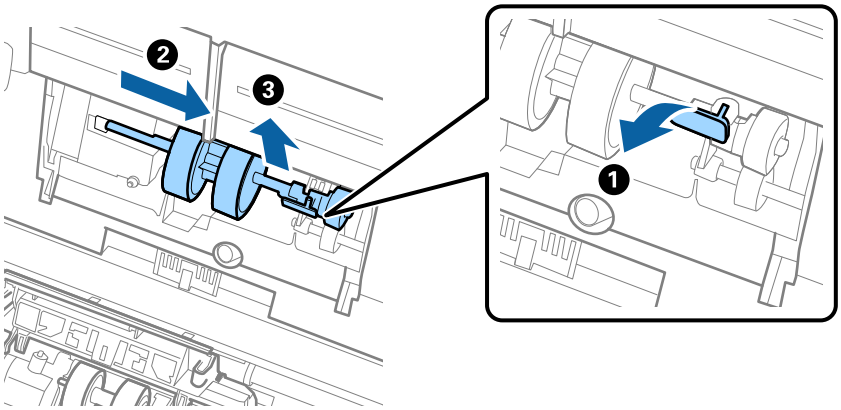
1. Tryck på knappen ⏻ för att stänga av skannern.
2. Koppla ur AC-adaptern från skannern.
3. Dra i spaken för att öppna skannerlocket.



4. Öppna luckan på pickup-rullen och skjut den sedan åt sidan för att ta bort den.

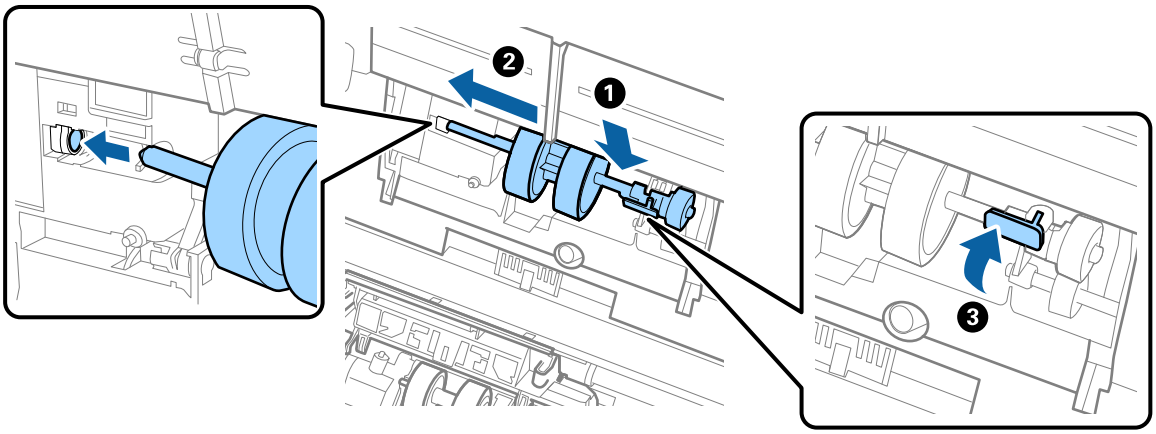


5. Dra fixturen nedåt för rullaxeln och skjut sedan på den och ta bort de installerade pickup-rullarna.

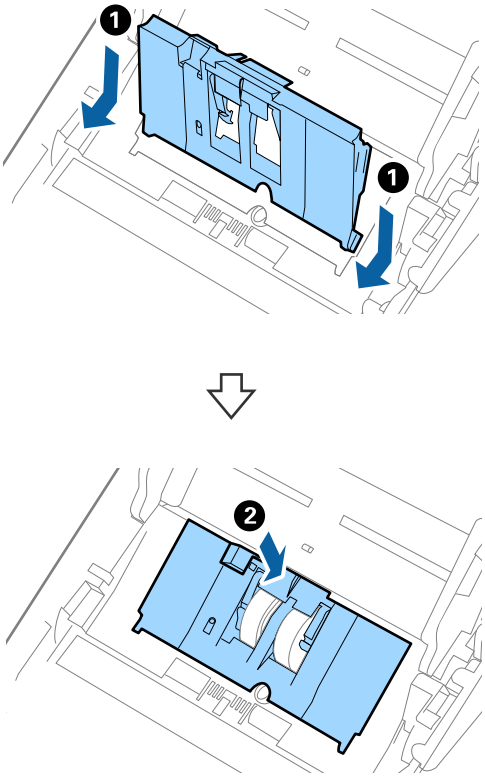


> ***Viktigt:***
> *Dra inte ut pickup-rullen med tvång. Detta kan påverka skdan invändigt i skannern.*

6. Samtidigt som du håller ned fixturen skjuter du den nya pickup-rullen åt vänster och för in den i hålet i skannern. Tryck på fixturen för att säkra den.

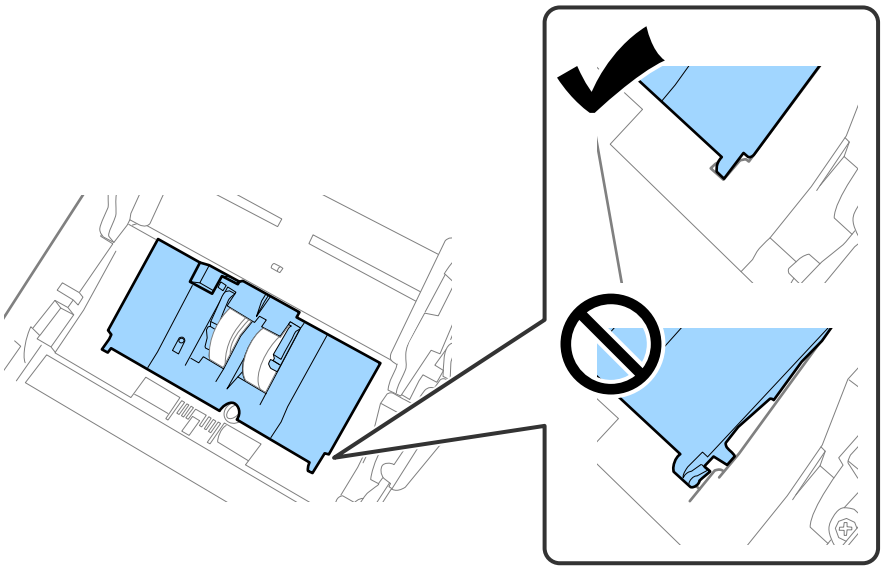


7. Sätt kanten på luckan över pickup-rullen i skåran och skjut på den. Stäng luckan ordentligt.

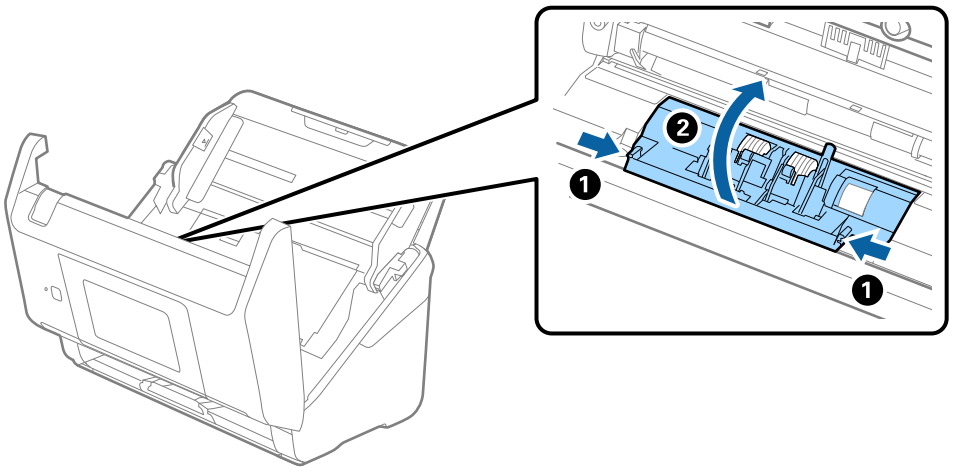


Viktigt:

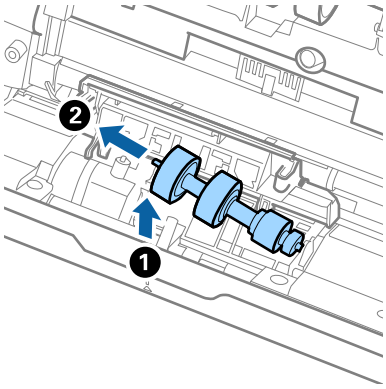
- ❏ *Kontrollera att pickup-locket är stängt.*
- ❏ *Se till att matarvalsarna installerats korrekt om luckan är svår att stänga.*
- ❏ *Installera inte luckan när den är uppställd.*



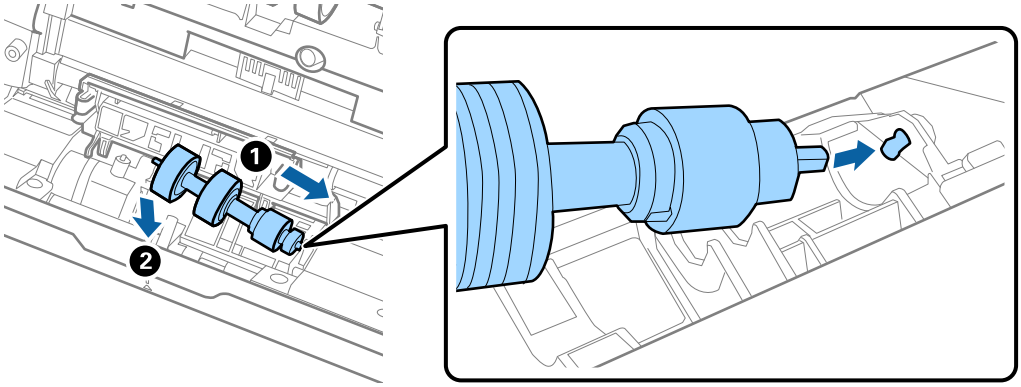
8. Tryck på krokarna på båda ändar av separationsrullslocket för att öppna luckan.



9. Lyft i sidan av separationsrulen och skjut sedan på den och ta bort de installerade separationsrullarna.



10. Mata in den nya separationsrullaxeln in i hålet på höger sida och sänk sedan ned rullen.



11. Stäng separationsrullocket.

> ***Viktigt:***
> *Om locket är svårt att stänga ska du se till att separationsrullarna är korrekt installerade.*

12. Stäng skannerlocket.

13. Koppla in AC-adaptern och slå på skannern.

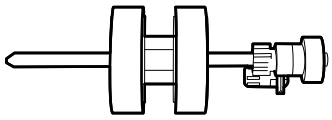
14. Återställ skanningsantalet på kontrollpanelen.

Anmärkning:
Kassera pickup-rullen och separationsrullen i enlighet med de regler och föreskrifter som gäller hos din lokala myndighet. Ta inte isär dem.

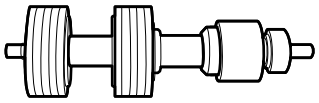
Koder för valsmonteringskit

Delar (pickup-rulle och separationsvals) ska bytas när antalet skanningar överskrider servicenumret. Du kan kontrollera det senaste antalet skanningar på kontrollpanelen eller i Epson Scan 2 Utility.

A



B



A: pickup-rulle, B: separationsvals

Delarnas namn	Koder	Livscykel
Valsmonteringskit	B12B819671 B12B819681 (endast Indien)	200,000*

* Detta nummer uppnåddes genom konsekvent skanning med Epsons testoriginalspapper, och är en guide till bytescykeln. Bytescykeln kan variera beroende på olika papperstyper, såsom papper som genererar mycket damm eller papper med en grov yta, som kan förkorta livscykeln.

Återställa antalet skanningar

Återställer antalet skanningar efter byte av valssatsen.

1. Välj **Inst.** > **Enhetsinformation** > **Återställ antal skanningar** > **Antalet skan. efter byte av underhållsvals** från startskärmen.
2. Tryck på **Ja**.

Relaterad information

➡ ”Byta rullmonteringskit” på sidan 154

Energispar

Du kan spara energi genom att använda viloläge eller automatiskt avstängningsläge när ingen åtgärd utförs av skannern. Du kan ställa in tidsperioden innan skannern övergår i viloläge och stängs av automatiskt. All ökning kommer att påverka produktens energieffektivitet. Tänk på miljön innan du gör några ändringar.

1. Välj **Inst.** på startskärmen.
2. Välj **Grundl. inställn.**.

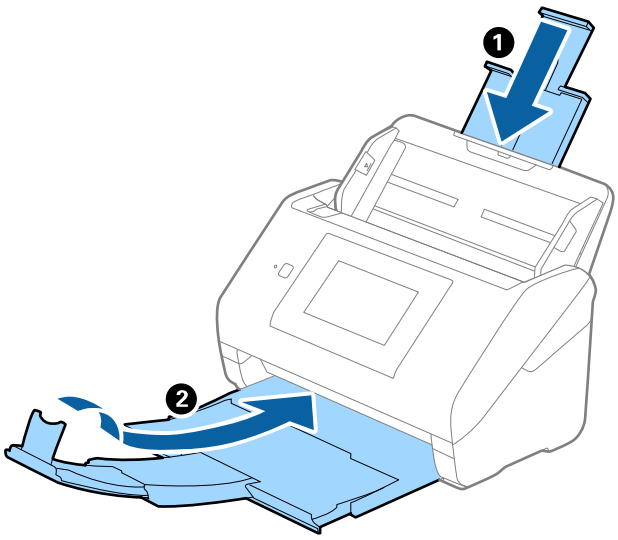
3. Välj **Avstängningsinst.** och ange sedan inställningarna.

   Anmärkning:
   Tillgängliga funktioner kan variera beroende på köpplatsen.

Transportera skannern

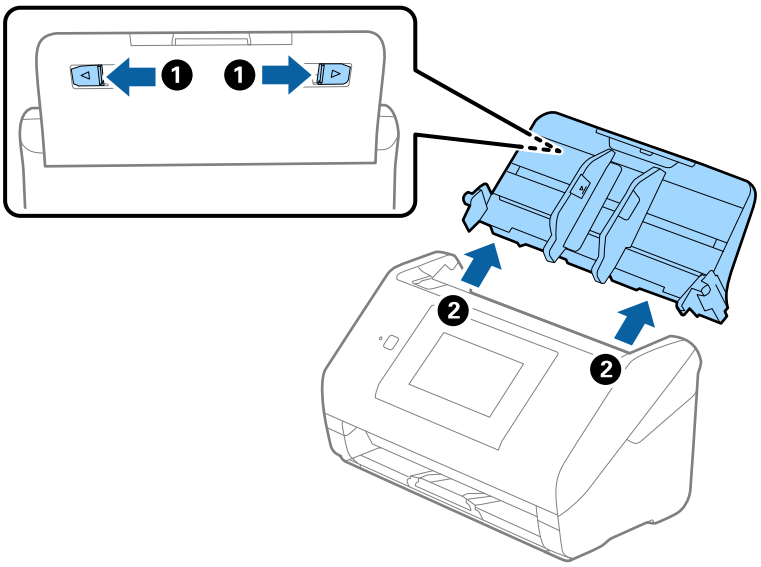
Om du måste transportera skannern en längre sträcka, följ stegen nedan för hur man packar ner skannern.

1. Tryck på knappen ⏻ för att stänga av skannern.
2. Koppla ur AC-adaptern.
3. Ta bort inmatningsförlängningen och utmatningsfacket.
4. Stäng inmatningsförlängningen och utmatningsfacket.



> ***Viktigt:***
> *Se till att stänga utmatningsfacket ordentligt; annars kan det skadas under transporten.*

5. Ta bort inmatningsfacket.



6. Sätt fast förpackningsmaterialet som medföljde skannern och packa ned skannern i originalkartongen, eller en liknande kartong som passar skannern.

Säkerhetskopiera inställningar

Du kan exportera inställningsvärdets konfiguration från Web Config till filen. Du kan använda den för säkerhetskopiering av kontakter, byte av skanner etc.

Den exporterade filen kan inte redigeras, eftersom den exporteras som en binär fil.

Exportera inställningarna

Exportera inställningarna för skannern.

1. Öppna Web Config och välj fliken **Enhetshantering** > **Inställningsvärde för export och import** > **Exportera**.

2. Välj de inställningar som du vill exportera.

   Välj de inställningar som du vill exportera. Om du väljer den överordnade kategorin, väljs även undergrupper. Däremot kan underkategorier som orsakar fel genom att dupliceras inom samma nätverk (såsom IP-adresser och så vidare) inte väljas.

3. Ange ett lösenord för att koda den exporterade filen.

   Du behöver ett lösenord för att importera filen. Lämna detta tomt, om du inte vill koda filen.

4. Klicka på **Exportera**.

> ***Viktigt:***
> *Om du vill exportera skannerns nätverksinställningar som enhetens namn och IPv6-adress, välj **Aktivera för att välja de enskilda inställningarna för enheten.** och markera fler poster. Använd endast utvalda värden för ersättningsskanner.*

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

Importera inställningarna

Importera den exporterade Web Config-filen till skannern.

> ***Viktigt:***
> *När du importerar värden som innehåller individuell information såsom ett skannernamn eller en IP-adress, måste du se till att samma IP-adress inte finns i samma nätverk.*

1. Gå till Web Config, och välj sedan fliken **Enhetshantering** > **Inställningsvärde för export och import** > **Importera**.
2. Välj den exporterade filen och ange sedan det kodade lösenordet.
3. Klicka på **Nästa**.
4. Välj inställningarna du vill importera och klicka sedan på **Nästa**.
5. Klicka på **OK**.

Inställningarna tillämpas på skannern.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

Återställ inställningarna

På kontrollpanelen väljer du **Inst.** > **Systemadministration** > **Återställ inställningarna**, och sedan väljer du objekten som ska återställas till standard.

- ❏ Nätverksinställningar: återställ nätverksrelaterade inställningar till initial status.
- ❏ Alla utom Nätverksinställningar: återställ övriga inställningar till initial status, förutom nätverksrelaterade inställningar.
- ❏ Alla inställningar: återställ alla inställningar till initial status vid köp.

> ***Viktigt:***
> *Om du väljer och kör **Alla inställningar**, kommer alla inställningsdata som registrerats på skannern inklusive kontakter och autentiseringsanvändarinställningar att raderas. Raderade inställningar kan inte återställas.*

Uppdatera applikationer och firmware

Du kanske kan lösa vissa problem och förbättra eller lägga till funktioner genom att uppdatera programmen och den fasta programvaran. Se till att du har den senaste versionen av programmen och den fasta programvaran.

> ***Viktigt:***
> ❏ *Stäng inte av datorn eller skannern medan du uppdaterar.*

Anmärkning:
*När skannern kan anslutas till Internet, kan du uppdatera den inbyggda programvaran från Web Config. Välj fliken **Enhetshantering** > **Firmware-uppdatering**, kontrollera meddelandet som visas och klicka sedan på **Starta**.*

1. Se till att skannern och datorn är ansluten, samt att datorn är ansluten till Internet.

2. Starta EPSON Software Updater och uppdatera programmen eller den fasta programvaran.

   Anmärkning:
   Operativsystemen för Windows Server stöds inte.

   ❏ Windows 10

   Klicka på startknappen och välj sedan **Epson Software** > **EPSON Software Updater**.

   ❏ Windows 8.1/Windows 8

   Ange programvarans namn i sökfältet och välj sedan den ikon som visas.

   ❏ Windows 7

   Klicka på startknappen och välj sedan **Alla program** eller **Program** > **Epson Software** > **EPSON Software Updater**.

   ❏ Mac OS

   Välj **Finder** > **Gå** > **Program** > **Epson Software** > **EPSON Software Updater**.

Anmärkning:
Om du inte hittar det program som du vill uppdatera i listan kan du inte uppdatera med hjälp av EPSON Software Updater. Sök efter senaste programversioner på din lokala Epson webbplats.

http://www.epson.com

Uppdatera skannerns inbyggda programvara med hjälp av kontrollpanelen

Om skannern kan anslutas till internet kan du uppdatera dess inbyggda programvara via kontrollpanelen. Du kan också ställa in skannern så att den regelbundet kontrollerar om det finns uppdateringar för inbyggd programvara och meddela dig om det finns några tillgängliga.

1. Välj **Inst.** på startskärmen.

2. Välj **Systemadministration** > **Uppdatering av fast programvara** > **Uppdatera**.

   Anmärkning:
   *Välj **Meddelande** > **På** om du vill ställa in skannern så att den regelbundet kontrollerar om det finns tillgängliga uppdateringar för inbyggd programvara.*

3. Kontrollera meddelandet som visas på skärmen och starta sökning efter tillgängliga uppdateringar.

4. Om ett meddelande om att en uppdatering av inbyggd programvara är tillgänglig visas på LCD-skärmen ska du följa instruktionerna på skärmen för att starta uppdateringen.

   Viktigt:
   - ❏ *Stäng inte av eller koppla från skannern tills uppdateringen är klar. Annars kanske den inte fungerar.*
   - ❏ *Om uppdateringen av inbyggd programvara inte slutförs eller misslyckas startar inte skannern normalt och ”Recovery Mode” visas på LCD-skärmen nästa gång den startas. I detta fall måste du uppdatera den inbyggda programvaran igen med en dator. Anslut skannern till datorn med en USB-kabel. Medan ”Recovery Mode” visas på skannern kan du inte uppdatera den inbyggda programvaran via en nätverksanslutning. Gå till den lokala Epson-webbplatsen via datorn och hämta sedan den senaste inbyggda programvaran för skannern. Se instruktionerna på hemsidan för nästa steg.*

Uppdatera firmware med Web Config

När skannern kan anslutas till Internet, kan du uppdatera den inbyggda programvaran från Web Config.

1. Öppna Web Config och välj fliken **Enhetshantering** > **Firmware-uppdatering**.

2. Klicka på **Starta**, och följ sedan anvisningarna på skärmen.

   Firmware-bekräftelsen startar och firmware-informationen visas om uppdaterad firmware finns.

Anmärkning:
Du kan också uppdatera firmware med Epson Device Admin. Du kan visuellt kontrollera firmware-informationen i enhetslistan. Detta är viktigt när du vill uppdatera firmware för flera enheter. Mer information finns i guiden Epson Device Admin eller hjälpavsnittet.

Relaterad information

➡ ”Kör Web-Config i en webbläsare” på sidan 34

Uppdatera firmware utan Internet-anslutning

Du kan hämta enhetens firmware från webbplatsen för Epson på datorn och sedan ansluta enheten och datorn med USB-kabeln för att uppdatera firmware. Prova följande om du inte kan uppdatera via nätverket.

Anmärkning:
Innan du uppdaterar ska du se till att skannerdrivrutinen Epson Scan 2 är installerad på din dator. Om Epson Scan 2 inte är installerat ska du installera det på nytt.

1. Kontrollera webbplatsen för Epson för senaste firmware-uppdateringspubliceringar.

   http://www.epson.com

   - ❏ Om det finns firmware för din skanner hämtar du den och går till nästa steg.

❏ Om det inte finns någon information om firmware på webbplatsen använder du redan senaste firmware.

2. Anslut daton som innehåller hämtad firmware till skrivaren med USB-kabeln.

3. Dubbelklicka på den hämtade .exe-filen.
   Epson Firmware Updater startar.

4. Följ instruktionerna på skärmen.