EPSON

DS-900WN DS-800WN

Administratörshandbok

NPD7398-00 SV

Upphovsrätt

Varumärken

- ❏ Microsoft, Windows, Windows Server, Microsoft Edge, SharePoint, and Internet Explorer are trademarks of the Microsoft group of companies.
- ❏ Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- ❏ Chrome, Chromebook and Android are trademarks of Google LLC.
- ❏ Wi-Fi®, Wi-Fi Direct®, and Wi-Fi Protected Access® are registered trademarks of Wi-Fi Alliance®. Wi-Fi Protected Setup™, WPA2™, WPA3™ are trademarks of Wi-Fi Alliance®.
- ❏ The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- ❏ The Mopria™ word mark and the Mopria™ Logo are registered and/or unregistered trademarks of Mopria Alliance, Inc. in the United States and other countries. Unauthorized use is strictly prohibited.
- ❏ Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- ❏ Allmänt meddelande: alla andra varumärken tillhör sina respektive ägare och används enast i identifieringssyfte.

Innehållsförteckning

Upphovsrätt

Varumärken

Introduktion

Kommentarer till administratörslösenordet

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

Använda Epson Open Platform

Montera en autentiseringsenhet

Underhåll

Introduktion

Innehållet i detta dokument

Detta dokument erbjuder följande information för skanneradministratörer.

❏ Nätverksinställningar

❏ Förbereda skanningfunktionen

❏ Aktivera och hantera säkerhetsinställningar

❏ Utföra dagligt underhåll

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

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.

Referenser för operativsystem

Windows

I den här användarhandboken syftar termer som "Windows 11", "Windows 10", "Windows 8.1", "Windows 8", "Windows 7", "Windows Server 2022", "Windows Server 2019", "Windows Server 2016", "Windows Server 2012 R2", "Windows Server 2012", "Windows Server 2008 R2" och "Windows Server 2008" på följande operativsystem. Dessutom används ”Windows” som referens till alla versioner.

- ❏ Microsoft® Windows® 11 operativsystem
- ❏ Microsoft® Windows® 10 operativsystem
- ❏ Microsoft® Windows® 8.1 operativsystem
- ❏ Microsoft® Windows® 8 operativsystem
- ❏ Microsoft® Windows® 7 operativsystem
- ❏ Microsoft® Windows Server® 2022 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
- ❏ Microsoft® Windows Server® 2008 operativsystem

Mac OS

I den här handboken används "Mac OS" för att hänvisa till Mac OS X 10.9 eller senare samt macOS 11 eller senare.

Kommentarer till administratörslösenordet

Kommentarer till administratörslösenordet

Enheten gör det möjligt för dig att genom att konfigurera ett aministratörslösenord förhindra obehöriga tredje parter från att öppna eller ändra enhetsinställningar eller nätverksinställningar som finns lagrade på enheten när den är ansluten till ett nätverk.

Om du konfigurera ett administratörslösenord behöver du ange lösenordet när du ändrar inställningar i konfigurationsprogramvaran, såsom Web Config.

Det initiala administratörslösenordet är konfigurerat på skannern, men du kan ändra det till valfritt lösenord.

Initialt administratörslösenord

Det initiala lösenordet för administratören beror på den etikett som sitter på produktens baksida. Om det finns en ”PASSWORD”-etikett fäst på baksidan anger du numret med 8 siffror som visas på etiketten. Om det inte finns någon ”PASSWORD”-etikett påklistrad anger du serienumret på etiketten som finns på produktens baksida för det initiala administratörslösenordet.

Vi rekommenderar att du ändrar det initiala administratörslösenordet från standardinställningen.

Anmärkning:
Inget användarnamn är konfigurerat enligt standard.

Åtgärder som kräver administratörslösenord

Om du ombeds ange administratörslösenordet under följande åtgärder anger du administraötrlösenordet som är konfigurerat på produkten.

- ❏ När du loggar avancerade inställningar för Web Config
- ❏ Vid användning av en meny på kontrollpanelen som har låsts av aministratören
- ❏ När du ändrar enhetsinställningar i applikationen
- ❏ Vid uppdatering av firmware för enheten
- ❏ Ange, ändra eller återställ administratörslösenordet

Ändra administratörslösenord

Du kan göra ändringar från produktens kontrollpanel eller i Web Config.

När du ändrar lösenordet måste det nya lösenordet vara 8 till 20 tecken långt och endast innehålla enkla alfanumeriska tecken och symboler.

Återställa administratörslösenord

Du kan återställa administratörslösenordet från produktens kontrollpanel eller i webbkonfigurationen.

Om du har glömt lösenordet och inte kan återställa till standardinställningar behöver produkten repareras. Kontakta din lokala återförsäljare.

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 15
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 21

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. "Registrera en e-postserver" på sidan 44 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 53
Jag vill spara bilder till en mapp i nätverket. (Skanna till nätverksmapp/FTP)	1. Skapa en mapp i nätverket är du vill spara bilderna. "Skapa en nätverksmapp" på sidan 47 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 53
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 66

Konfigurera grundläggande säkerhetsfunktioner

Syfte	Obligatoriska inställningar
Jag vill förhindra att administratören ändrar skannerinställningarna.	Konfigurera ett administratörslösenord för skannern. "Administratörsinställningar" på sidan 74
Jag vill inaktivera användning av skannrar med USB-anslutningar.	Inaktivera externt gränssnitt. "Inaktivera externt gränssnitt" på sidan 82

Konfigurera avancerade säkerhetsfunktioner

Syfte	Obligatoriska inställningar
Jag vill kontrollera vilka protokoll som ska användas.	Aktivera eller inaktivera protokollen. "Kontrollera med protokoll" på sidan 89
Jag vill kryptera kommunikationssökvägen.	1. Konfigurera ditt digitala certifikat. "Använda ett digitalt certifikat" på sidan 92 2. Konfigurera SSL/TLS-kommunikation. "SSL-/TLS-kommunikation med skannern" på sidan 97
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 98
Jag vill använda en skanner i ett IEEE802.1X nätverk.	Installera IEEE802.1X för skannern. "Ansluta skannern till ett IEEE802.1X-nätverk" på sidan 109

Synkronisering av skannern med ett autentiseringssystem

Införskaffa en produktnyckel från den dedikerade webbplatsen och aktivera Epson Open Platform på din skanner.

"Använda Epson Open Platform" på sidan 118

Använda ett autentiseringsalternativ (Epson Print Admin/Epson Print Admin Serverless)

Du måste ha en licensnyckel för att använda alternativet.

Kontakta din återförsäljare för mer information.

Anmärkning:
Du kan inte använda Epson Print Admin Serverless när systemet är synkroniserat med Epson Open Platform.

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 installationsenheten.

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

https://epson.sn

Du kan visa bruksanvisningen i Manualer för webbfilm. Öppna följande URL.

https://support.epson.net/publist/vlink.php?code=NPD7509

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 28
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 31

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.)

Observera när en Wi-Fi 5 GHz-anslutning används

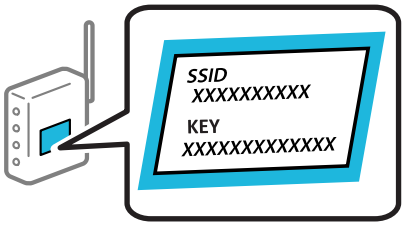
Den här produkten använder normalt W52 (36ch) som kanal vid anslutning till Wi-Fi Direct (Simple AP). Eftersom kanalen för anslutning via trådlöst LAN (Wi-Fi) väljs automatiskt, kan kanalen som används skilja sig åt när den används samtidigt som en Wi-Fi Direct-anslutning. Om kanalerna skiljer sig åt, kan datakommunikationen med skannern vara långsam. Anslut till SSID i 2,4 GHz-bandet om det inte stör användningen. I frekvensbandet 2,4 GHz kommer kanalerna som används att vara desamma.

När du ställer in det trådlösa nätverket på 5 GHz rekommenderar vi att du inaktiverar Wi-Fi Direct.

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 den trådlösa routern 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.*
   - ❏ *Om du inte kan se SSID, du vill ansluta till, använder du mjukvaran eller en app för att konfigurera Wi-Fi från din dator eller smartenhet, såsom en smartphone eller surfplatta. För mer information, öppna "https://epson.sn" i din webbläsare för åtkomst till webbplatsen och ange ditt produktnamn, gå sedan till **Inställning**.*

Relaterad information

➡ "Kontrollera nätverksanslutningens status" på sidan 27

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 27

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 27

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.

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

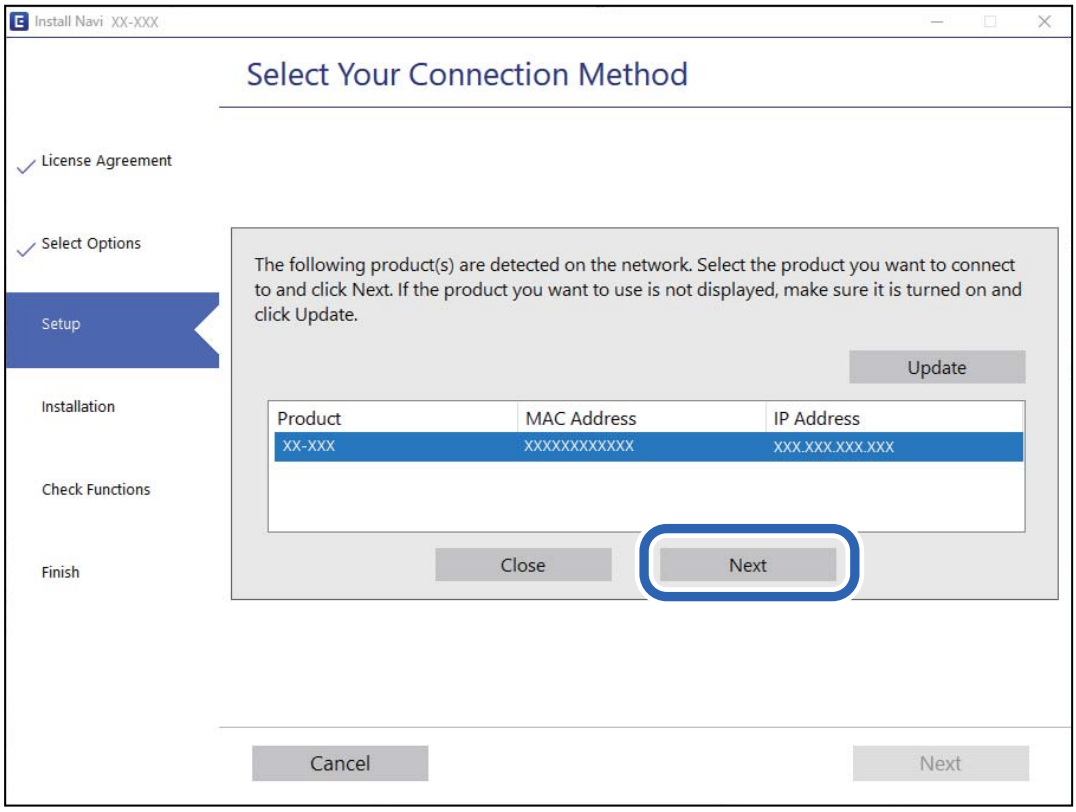
https://epson.sn

Du kan visa bruksanvisningen i Manualer för webbfilm. Öppna följande URL.

https://support.epson.net/publist/vlink.php?code=NPD7509

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 26

Ansluta med Wi-Fi Direct

Anslut smartenheten direkt till skannern utan en trådlös router.

Se följande för mer information.

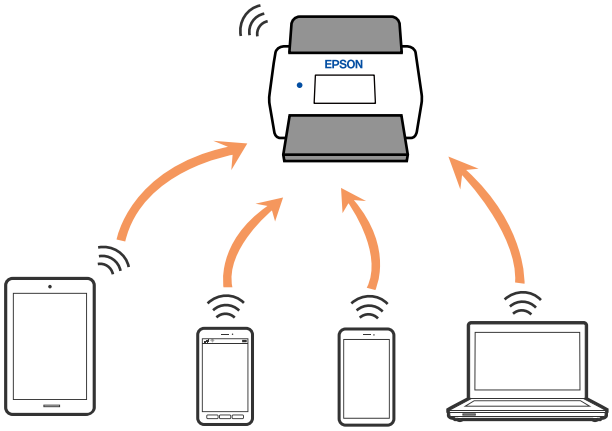
”Ansluta en smartenhet och skanner direkt (Wi-Fi Direct)” på sidan 23

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.

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

https://epson.sn

Du kan visa bruksanvisningen i Manualer för webbfilm. Öppna följande URL.

https://support.epson.net/publist/vlink.php?code=NPD7509

Välja anslutningssätt

Följ instruktionerna på skärmen. På skärmen **Välj Tillval att installera** 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 32

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. Öppna följande webbplats och ange sedan produktnamnet för att använda skannern från en smartenhet. Gå till **Inställning** och starta konfigurationen.

https://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.

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

https://epson.sn

Du kan visa bruksanvisningen i Manualer för webbfilm. Öppna följande URL.

https://support.epson.net/publist/vlink.php?code=NPD7509

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 19

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.

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

https://epson.sn

Välja att ändra anslutningssätt

Följ instruktionerna i varje fönster. På skärmen **Välj Tillval att installera** 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**

Irland, Storbritannien, Österrike, Tyskland, Liectenstein, Schweiz, Frankrike, Belgien, Luxemburg, Nederländerna, Italien, Portugal, Spanien, Danmark, Finland, Norge, Sverige, Island, Kroatien, Cypern, Grekland, Norra Makedonien, Serbien, Slovenien, Malta, Bosnien och Herzegovina, Kosovo, Montenegro, Albanien, Bulgarien, Tjeckiska republiken, Estland, Ungern, Lettland, Litauen, Polen, Rumänien, Slovakien, Israel, Australien, Nya Zeeland, Taiwan	**Tabell B**
Turkiet	DS-900WN: Serienummer som inleds med XDA8: **Tabell A** Serienummer som inleds med XDA7: **Tabell B**
	DS-800WN: Serienummer som inleds med XDA2: **Tabell A** Serienummer som inleds med XD9Z: **Tabell B**

Tabell A

Standarder	IEEE 802.11b/g/n*1
Frekvensområde	2 400–2 483,5 MHz
Maximal radiofrekvensstyrka utsänd	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-stöd

Funktion	Stöds
Epson Scan 2	IPv4, IPv6
Document Capture Pro/Document Capture	IPv4

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

Använd	Destination (server)	Protokoll	Portnummer
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

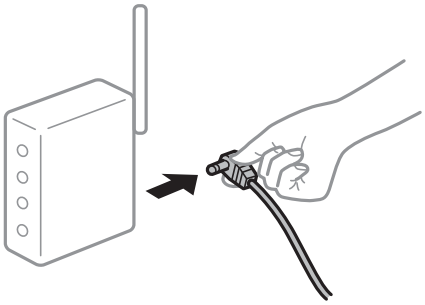
Problemet kan bero på ett av de följande orsaken.

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

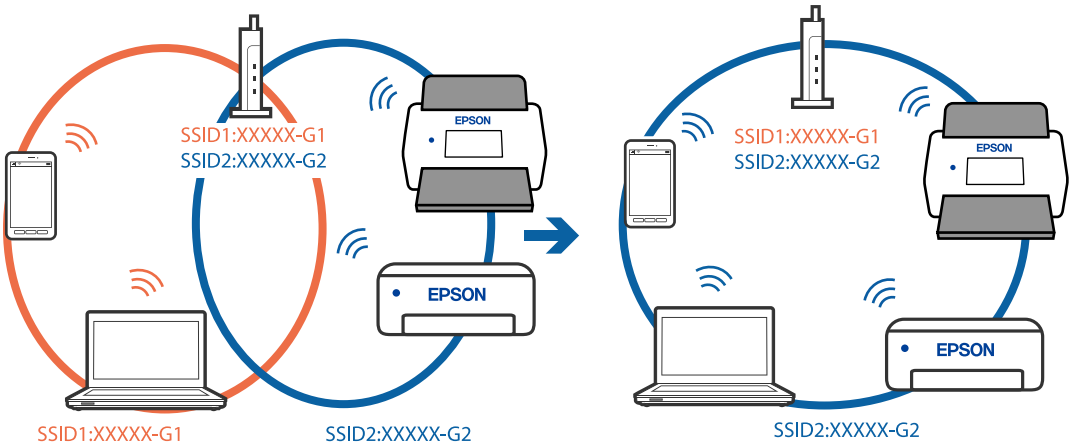
Utför anslutningsinställningarna igen så att de matchar till den nya trådlösa routern.

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.

   ”Hur du kör Web Config i en webbläsare” på sidan 37
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

Program för konfiguration av skanneråtgärder (Web Config)

Web Config är ett program som körs i en webbläsare, till exempel Microsoft Edge eller Safari, på en dator eller smartenhet. Du kan bekräfta skannerns status och ändra inställningar för nätverkstjänsten eller skannern. Använd Web Config genom att ansluta skannern och datorn eller enheten till samma nätverk.

Det finns stöd för följande webbläsare. Använd den senaste versionen.

Microsoft Edge, Windows Internet Explorer, Firefox, Chrome, Safari

Anmärkning:
Du kan bli ombedd att ange administratörslösenordet när du använder den här enheten. Se följande för information om administratörslösenordet.

"Kommentarer till administratörslösenordet" på sidan 10

Relaterad information

➡ "Kan inte komma åt Web Config" på sidan 63

Hur du kör Web Config i en webbläsare

Skannern levereras med en inbyggd programvara som kallas Web Config (en webbsida där du kan göra inställningar). För att öppna Web Config anger du bara IP-adressen för en nätverksansluten skanner i din 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.

   Exempel på IP-adress: 192.168.100.201

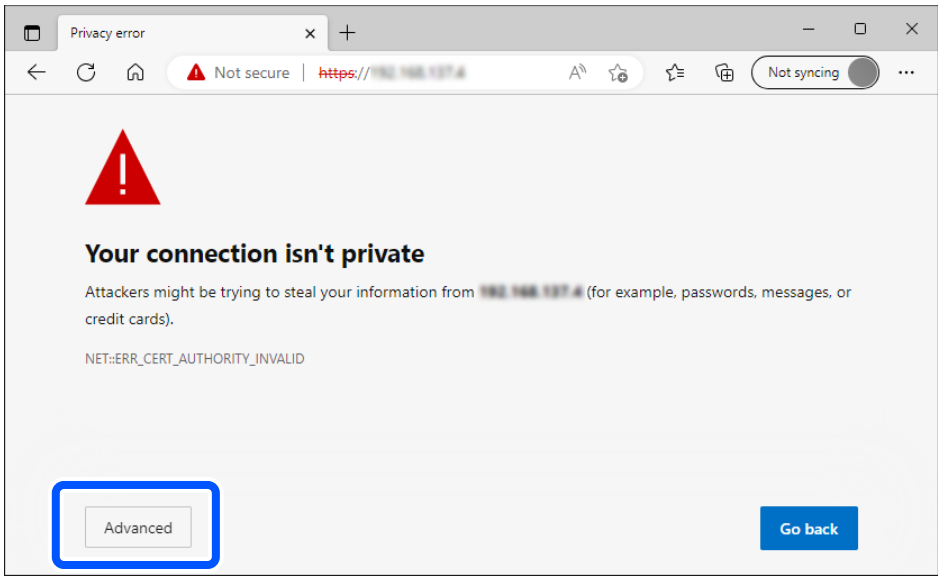
2. Öppna en webbläsare på en dator eller smartenhet och ange sedan skannerns IP-adress i adressfältet.

   Format: http://skannerms IP-adress/

   Exempel: http://192.168.100.201/

   Om en varningsskärm visas i din webbläsare kan du på ett säkert sätt ignorera varningen och visa webbsidan (Web Config). 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. Beroende på webbläsare kan du behöva klicka på **Avancerade inställningar** för att visa webbsidan.

Exempel: För Microsoft Edge



Anmärkning:

❏ *Om varningsskärmen inte visas, gå vidare till nästa steg.*

❏ *För IPv6-adresser använder vi följande format.*

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

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

3. För att ändra skannerinställningarna behöver du logga in som en Web Config-administrator.

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

   Följande ger de initiala värdena för Web Config-administratörsinformationen.

   ·Användarnamn: inget (blank)

   ·Lösenord: Beroende på den etikett som sitter på produkten.

   Om det finns en ”PASSWORD”-etikett fäst på baksidan anger du numret med 8 siffror som visas på etiketten. Om det inte finns någon ”PASSWORD”-etikett påklistrad anger du serienumret på etiketten som finns på produktens baksida för det initiala administratörslösenordet.

   Anmärkning:

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

   ❏ *Du loggas ut automatiskt efter omkring 20 minuters inakivitet.*

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.

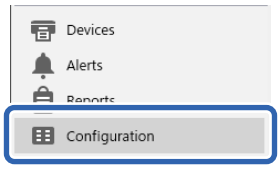
Du kan hämta Epson Device Admin från webbplatsen för Epson-support. För detaljer kring hur du använder detta program, se dokumentation eller hjälp för Epson Device Admin.

Konfigurationsmall

Skapa konfigurationsmallen

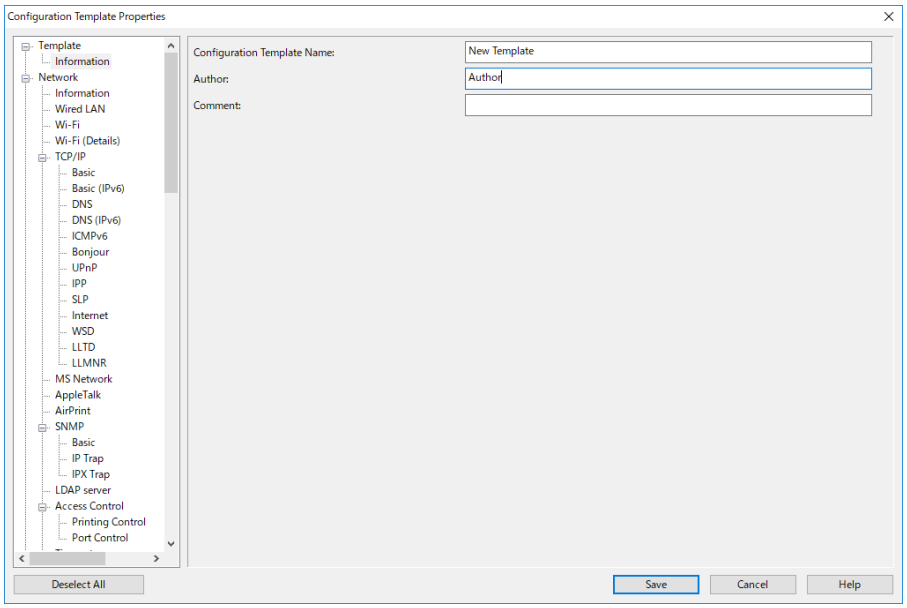
Skapa konfigurationsmallen.

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).

Alternativ	Förklaring
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.

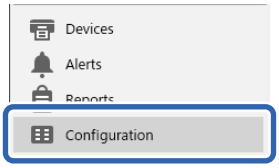
1. I färgbandsmenyn för enhetslistskärmen väljer du ***Options*** *>* ***Password manager****.*

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

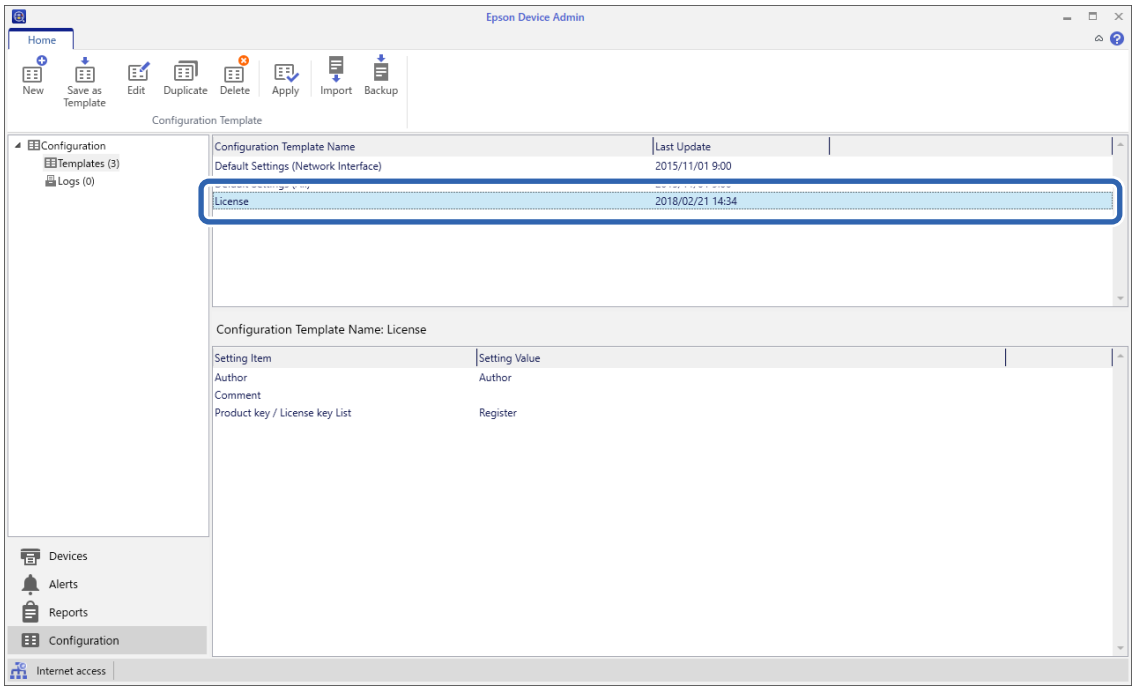
3. Välj lämplig skanner och klicka sedan på ***Edit****.*

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.

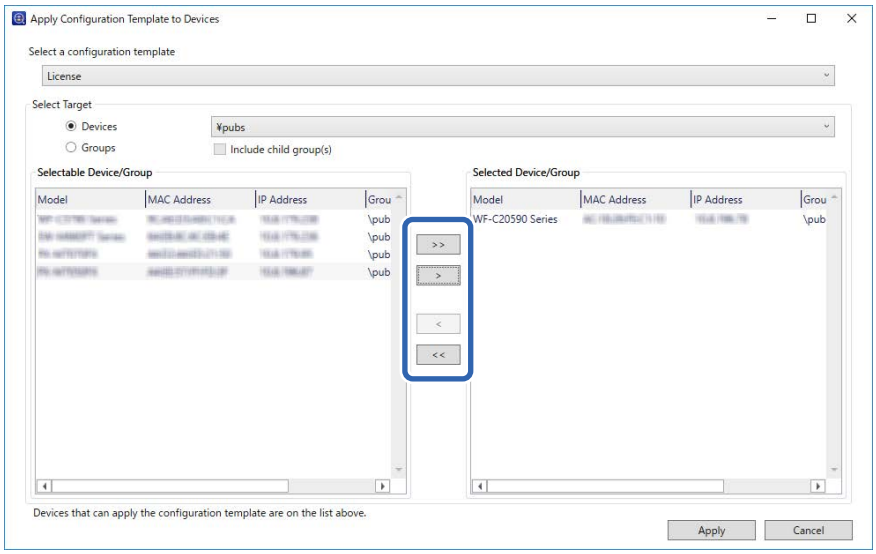
4. Välj den konfigurationsmall du vill verkställa.

   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

Registrera en e-postserver

Kontrollera följande innan du konfigurerar e-postservern.

❏ Skannern är ansluten till ett nätverk.

❏ Konfigurationsuppgifter för e-postserver

När du använder en Internet-baserad e-postserver ska du kontrollera inställningsinformationen från leverantören eller webbplatsen.

Registrering

Öppna Web Config och välj fliken **Nätverk** > **E-postserver** > **Grundläggande**.

”Hur du kör Web Config i en webbläsare” på sidan 37

Du kan också utföra inställningar för begränsning via skannerns kontrollpanel. Välj **Inst.** > **Nätverksinställningar** > **Avancerat** > **E-postserver** > **Serverinställningar**.

Inställningsalternativ för e-postserver

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	Konfigurera e-postadressen som används för att skicka e-post från skannern. Trots att du kan använda en befintlig e-postadress rekommenderar vi att du skaffar den och konfigurerar en e-postadress så att den kan särskiljas från e-post som skickats från skannern. 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 (endast Web Config)	Certifikatet är validerat när detta är aktiverat. Vi rekommenderar att du konfigurerar detta till **Aktivera** när **Säker anslutning** är inställt på något annat än **Saknas**.	

Objekt	Inställningar och förklaringar
POP3-serveradress	Om du väljer **POP före SMTP** som **Autentiseringsmetod**, ange serveradressen för servern som tar emot e-post (POP3-server). Ange mellan 0 och 255 tecken med A–Z a–z 0–9 . Du kan använda IPv4- eller FQDN-format.
POP3-serverportnummer	Ställ in när du väljer **POP före SMTP** i **Autentiseringsmetod**. Ange ett nummer mellan 1 och 65535.

Relaterad information

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

Kontrollera en e-postserveranslutning

1. Välj anslutningstestmenyn.
   - ❏ **Vid konfiguration från Web Config:**
     Välj fliken **Nätverk** tab > **E-postserver** > **Anslutningstest** > **Starta**.
   - ❏ **När du gör inställningar från kontrollpanelen:**
     Välj **Inst.** > **Nätverksinställningar** > **Avancerat** > **E-postserver** > **Kontrollera anslutning**.

   Anslutningstest för e-postservern startas.
2. Kontrollera testresultaten.
   - ❏ Testet genomförs när meddelandet **Anslutningstest lyckades.** visas.
   - ❏ Om ett fel visas följer du instruktionerna i meddelandet för att rensa felet.
     ”Referens för anslutningstest av e-postserver” på sidan 45

Referens för anslutningstest av e-postserver

Meddelande	Orsak
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
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

Meddelande	Orsak
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 ❏ Namn på upplösning 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 meddelande visas när en SMTP felmatchning uppstår mellan en server och en klient, eller när servern inte stöder 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 servers 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..
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.

Skapa en nätverksmapp

Skapa en nätverksmapp på din dator. Anslut datorn eller smartenheten till samma nätverk som skannern.

Metoden att ställa in den delade mappen varierar beroende av din miljö. Det här är ett exempel på hur du skapar en nätverksmapp på skrivbordet för en dator under följande miljö.

- ❏ Operativsystem: Windows 10
- ❏ Plats för att skapa delad mapp: Skrivbord
- ❏ Mappsökväg: C:\Users\xxxx\Desktop\scan_folder (skapa en nätverksmapp som kallas ”scan_folder” på skrivbordet)

1. Logga in på datorn där du vill skapa nätverksmappen med ett användarkonto som har administratörsbehörighet.

   Anmärkning:
   Om du inte vill veta vilket användarkonto som har administratörsbehörighet ska du undersöka detta med din datoradministratör.

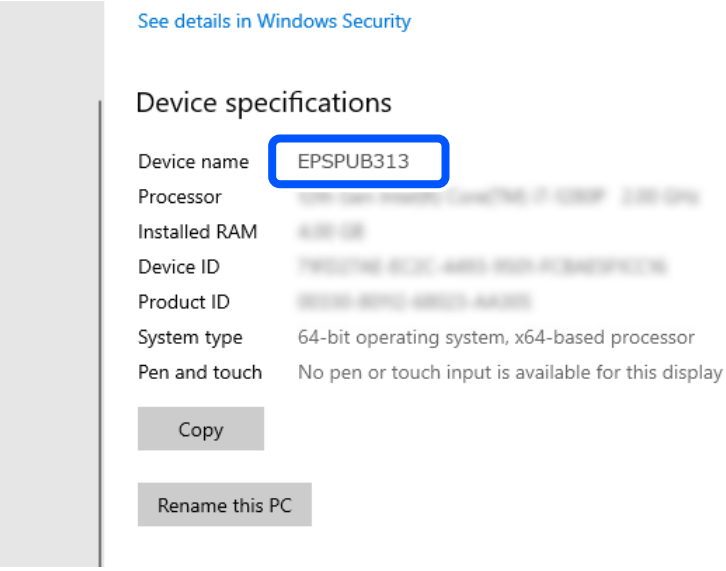
2. Se till att enhetsnamnet (datornamn) inte innehåller dubbla byte-tecken. Klicka på startknappen för Windows och välj sedan **Inställningar** > **System** > **Om**.

   Anmärkning:
   Om det finns dubbla byte-tecken i enhetens namn kan sparandet misslyckas.

3. Kontrollera att strängen som visas i **Enhetsspecifikationer** > **Enhetsnamn** inte innehåller några tecken med dubbla byte.

   Det ska inte vara några problem om enhetsnanet endast innehåller tecken med enkla byte. Stäng skärmen.

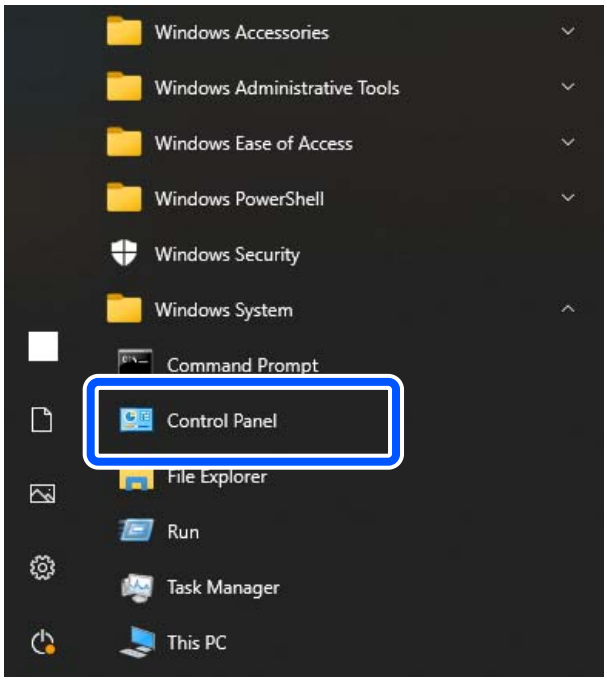
   Exempel: EPSPUB313



> ***Viktigt:***
>
> *Om enhetsnamnet innehåller tecken med dubbla byte använder du en dator som inte har tecken för dubbla byte eller så byter du namn på enheten.*
>
> *Om du behöver ändra enhetens namn ska du kontrollera med datorns administratör i förväg, eftersom det kan påverka datorhantering och åtkomst till resurser.*

Sedan kontrollerar du inställningarna för din dator.

4. Klicka på startknappen och välj sedan Windows system **Windows-system** > **Kontrollpanelen**.



5. Öppna Kontrollpanelen och klicka sedan på > **Nätverk och Internet** > **Nätverks- och delningscenter** > **Ändra adapterinställningar**

   Nätverksprofilen visas.

6. Se till att **Slå på fil- och skrivardelning** är markerat under **Fil- och skrivardelningg** för nätverksprofilen (aktuell profil).

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

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

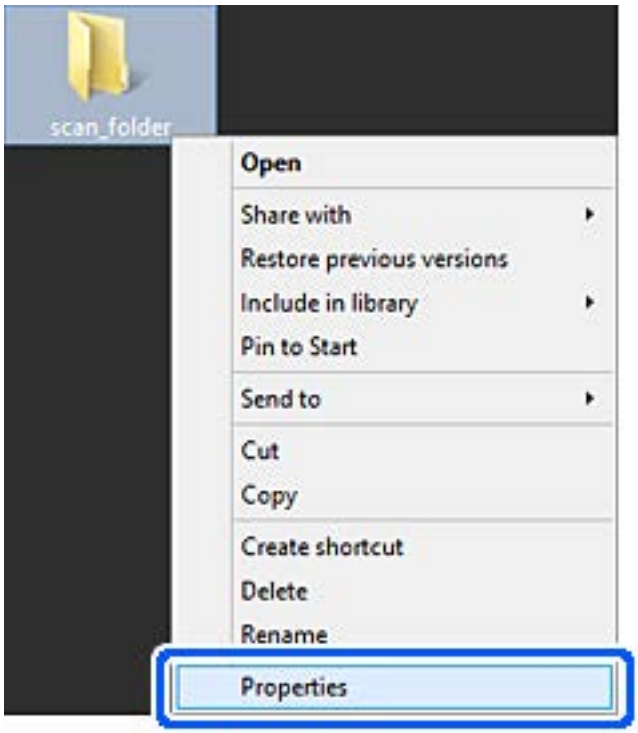
   Skapa sedan en nätverksmapp.

7. Skapa och byt namn på en mapp på ditt skrivbord.

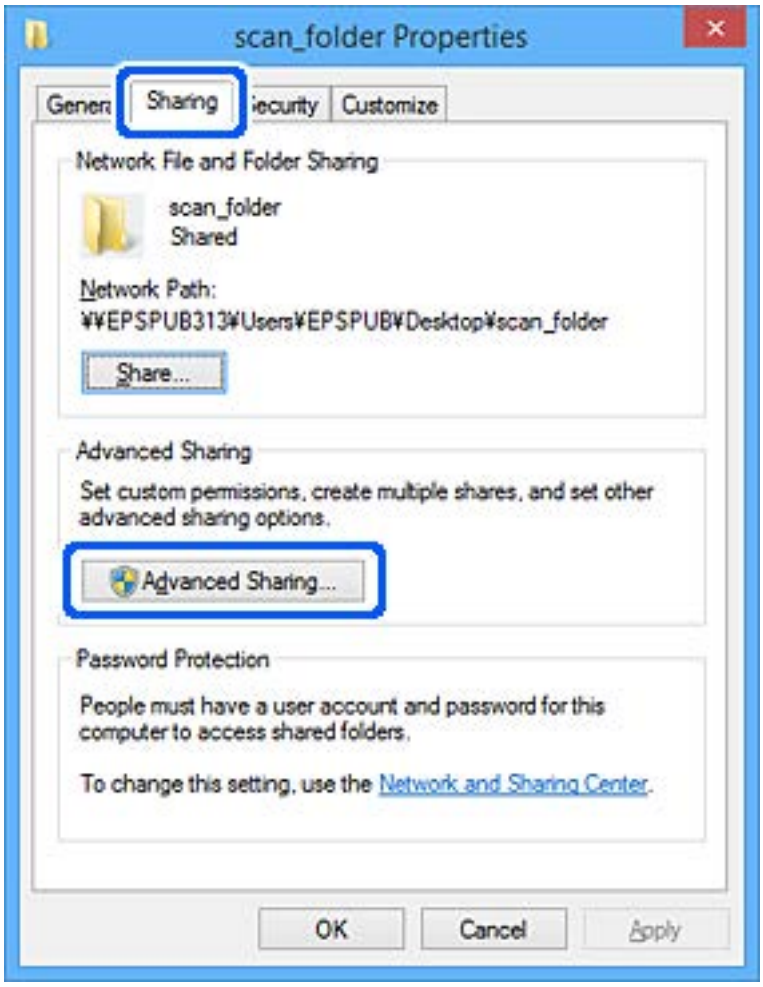
   För mappnamnet anger du 1 till 12 alfanumeriska tecken. Om namnet har mer än 12 tecken, kan skrivaren kanske inte komma åt mappen beroende av miljön.

   Exempel: scan_folder

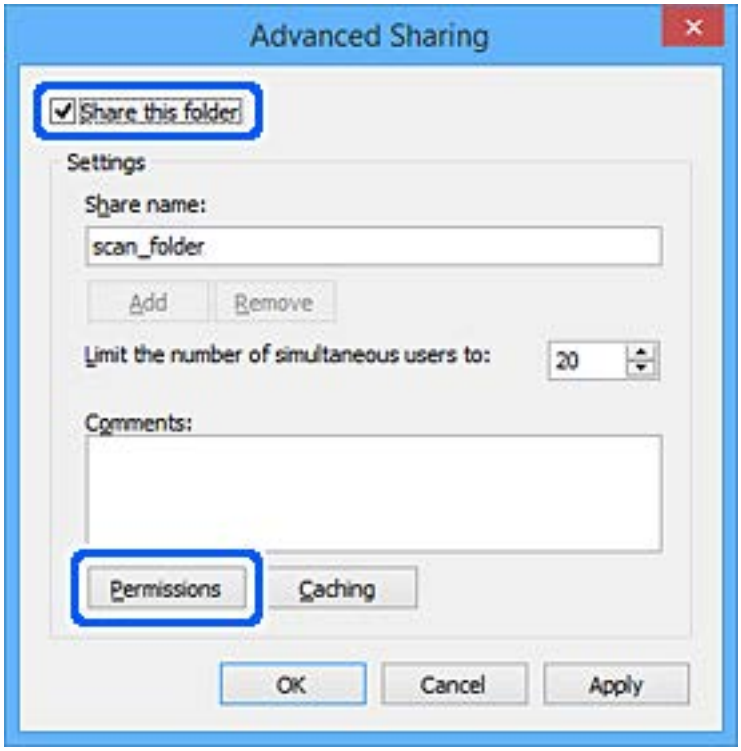
8. Högerklicka på mappen och välj sedan **Egenskaper**.



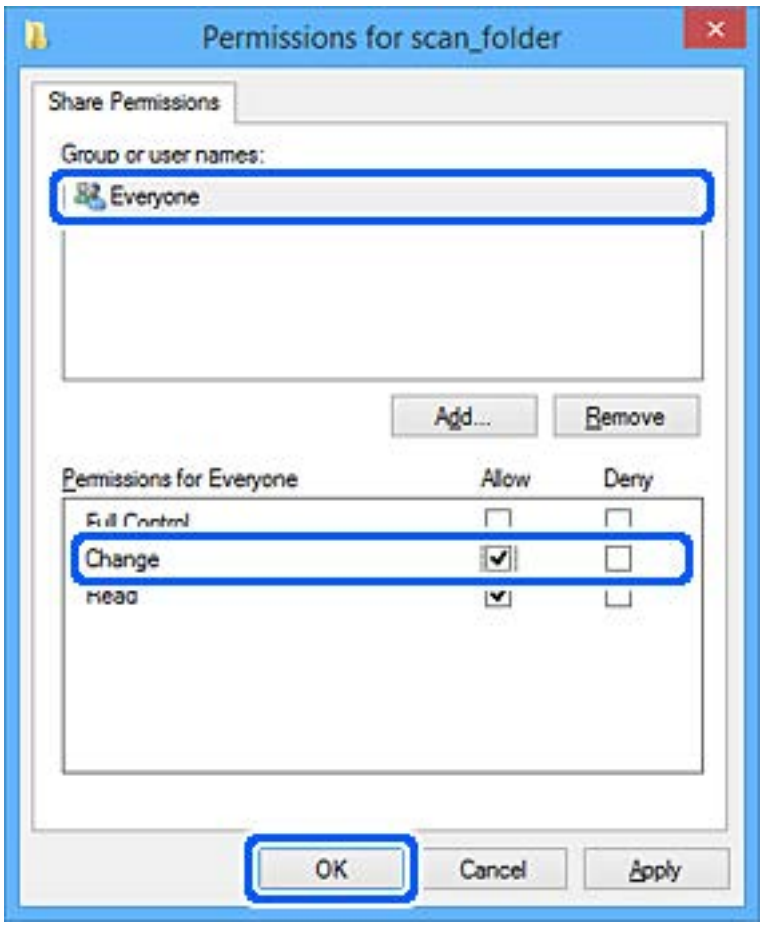
9. Klicka på **Avancerad delning** i fliken **Delning**.



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



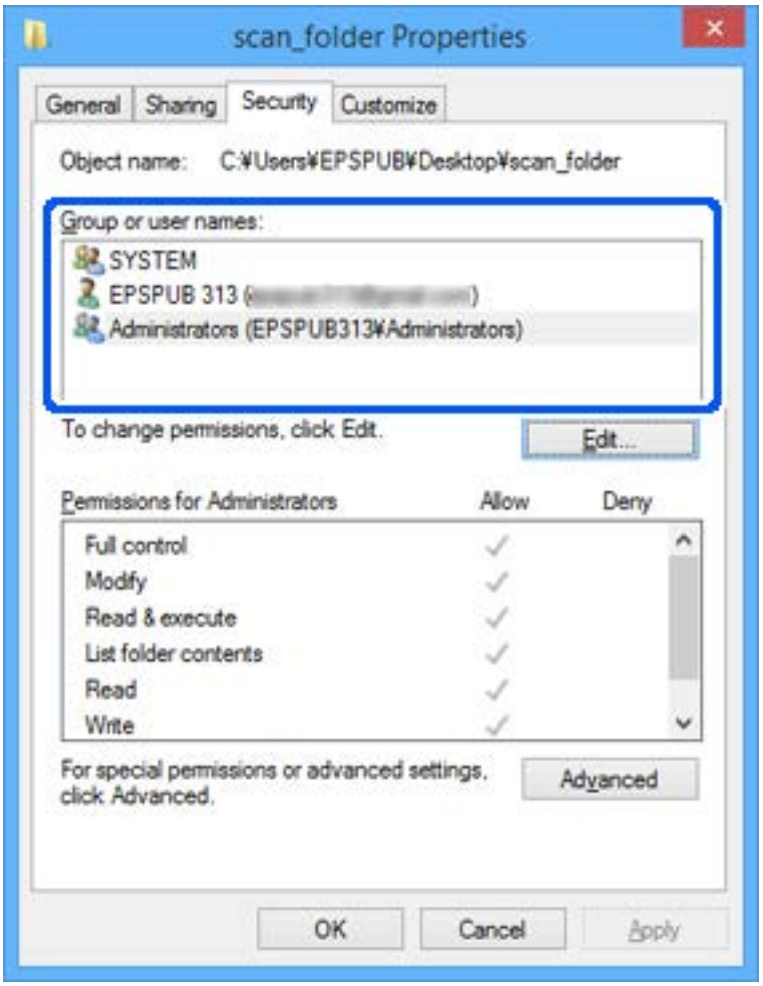
11. Välj gruppen **Alla** i **Grupp- eller användarnamn**, välj **Tillåt** i **Ändra** och klicka sedan på **OK**.



12. Klicka på **OK** för att stänga skärmen och återgå till fönstret för Egenskaper.

    Anmärkning:
    Du kan markera vilka grupper eller användare som ska ha åtkomst till nätverksmappen på fliken ***Säkerhet*** *>* ***Grupp- eller användarnamn****.*

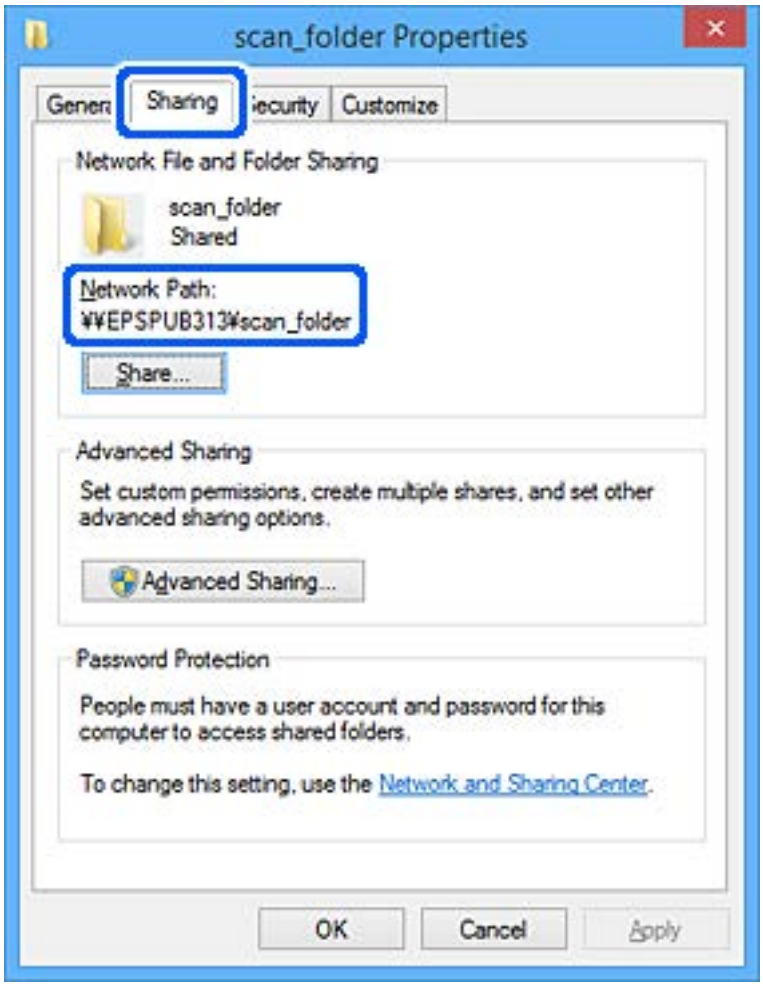
    Exempel: När användaren loggat in på datorn liksom Administratörer kan få åtkomst till nätverksmappen



13. Välj fliken **Delning**.

    Nätverksvägen för nätverksmappen visas. Det här används vid registrering i skannerns kontaktlista. Skriv ned den.

Exempel: \\EPSPUB313\scan_folder



14. Klicka på **Stäng** eller **OK** för att stänga fönstret.

Detta slutför skapande av en nätverksmapp.

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 59

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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

Alternativ för destinationsinställning

Alternativ	Inställningar och förklaringar
Vanliga inställningar	
Namn	Ange ett namn i kontakterna med 30 tecken eller mindre i Unicode (UTF-16). Om du inte specificerar detta, lämna det tomt.
Indexord	Ange ett namn med högst 30 tecken i Unicode (UTF-16) 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-16), utan "\\". Ange nätverksvägen som visas på mappens egenskapsskärm. Se följande för information om att ställa in nätverksvägen. "Skapa en nätverksmapp" på sidan 47
Användarnamn	Ange användarnamn för åtkomst till en nätverksmapp med 30 tecken eller mindre i Unicode (UTF-16). Men undvik att använda styrtecken (0x00 till 0x1F, 0x7F).
Lösenord	Ange ett lösenord för tillgång till en nätverksmapp mellan 0 och 20 tecken i Unicode (UTF-16). 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 Unicode (UTF-16), utelämna "ftp://" eller "ftps://".
Användarnamn	Ange användarnamn för åtkomst till en FTP-server med 30 tecken eller mindre i Unicode (UTF-16). 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 ett lösenord för tillgång till en FTP-server mellan 0 och 20 tecken i Unicode (UTF-16). 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 Unicode (UTF-16), utelämna "ftp://" eller "https://".
Användarnamn	Ange användarnamn för åtkomst till en server med 30 tecken eller mindre i Unicode (UTF-16). Men undvik att använda styrtecken (0x00 till 0x1F, 0x7F). Om du inte specificerar detta, lämna det tomt.
Lösenord	Ange ett lösenord för tillgång till en server mellan 0 och 20 tecken i Unicode (UTF-16). 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.

* SharePoint Online stöds inte vid skanning till nätverksmappen från skannerns kontrollpanel.

Om ddu vill spara den skannade bilden till SharePoint Online, använder du Document Capture Pro efter installation av SharePoint Online Connector. Se manualen för Document Capture Pro för instruktioner.

https://support.epson.net/dcp/

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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

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.
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
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

Alternativ	Inställningar och förklaringar
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.

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	Aktiverar Bonjour och AirPrint (Skanningtjänst). Den här knappen är bara tillgänglig när AirPrint inaktiverats. ***Anmärkning:*** *Om AirPrint inaktiverats kommer också, Mopria-skanning från Chromebooks, Windows, och Mopria Scan-appen inaktiveras.*

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** (eller **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.

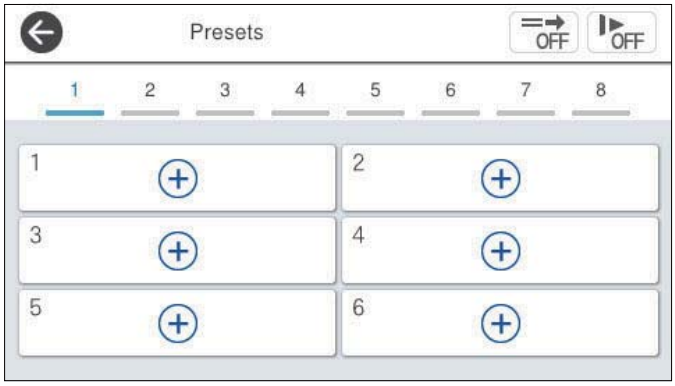
Anmärkning:

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

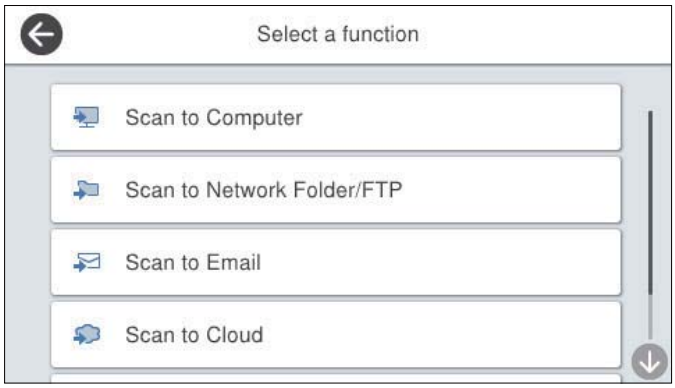
  *Välj fliken **Skanna** > **Förinställningar**.*
- *Om du väljer **Skanna till dator** vid registrering kan du registrera jobbet skapat i Document Capture Pro som **Förinställningar**. Detta är endast tillgängligt för datorer som är anslutna via ett nätverk. Registrera jobbet i Document Capture Pro i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

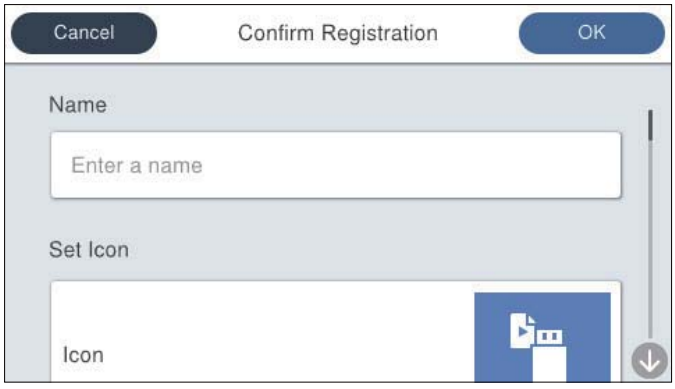
5. Gör förinställningarna.

   ❏ **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.

   ❏ **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 69
- ❏ 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 70
- ❏ Ta bort ikon: Tar bort ikonen från startskärmen.
  ”Ta bort ikon” på sidan 71
- ❏ Flytta ikon: Ändrar visningsordningen för ikonerna.
  ”Flytta ikon” på sidan 72
- ❏ Återställ ikonernas standardvisning: Återställer standardvisningsinställningarna för startskärmen.

Ändrar Layout på startskärmen

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

2. Välj **Rad** eller **Matris**.

   Rad:

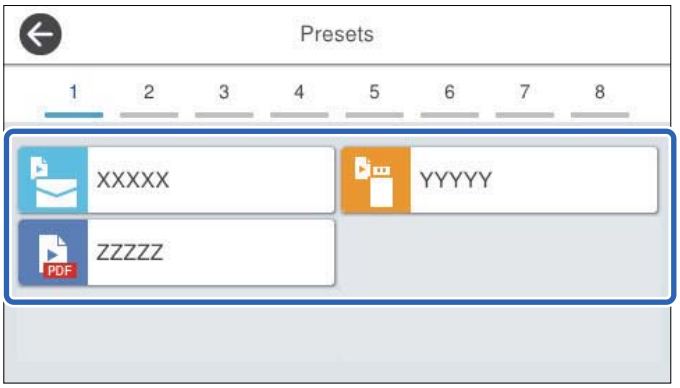
   Matris:

3. Välj för att återgå och kontrollera startskärmen.

Lägg till ikon

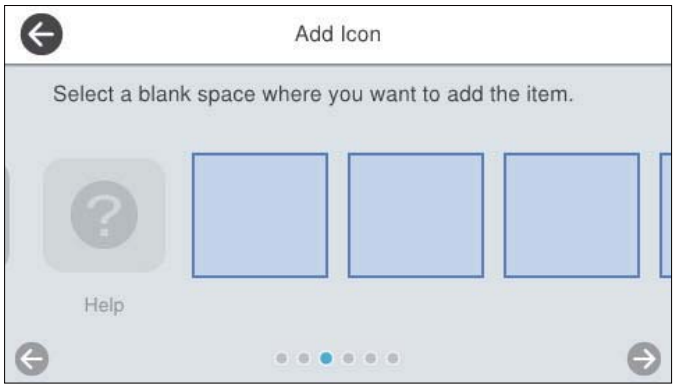
1. Välj **Inst.** > **Redigera Hem** > **Lägg till ikon** på skannerns kontrollpanel.
2. Välj **Funktion** eller **Förinställ.**.
   - ❏ Funktion: Visar standardvisningsinställningarna för startskärmen.
   - ❏ Förinställ.: Visar registrerade förinställningar.

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



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

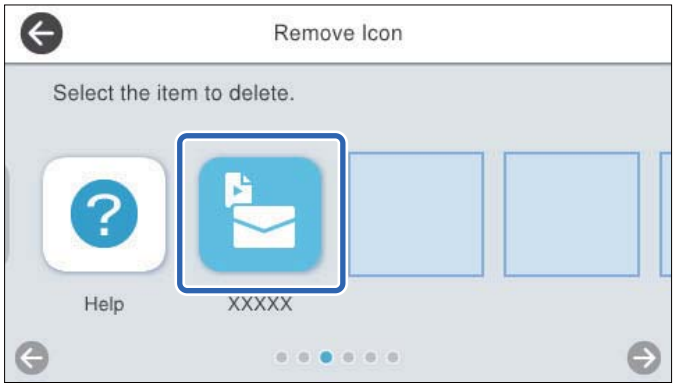
   Upprepa procedur 3 till 4 om du vill lägga till flera ikoner.



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.



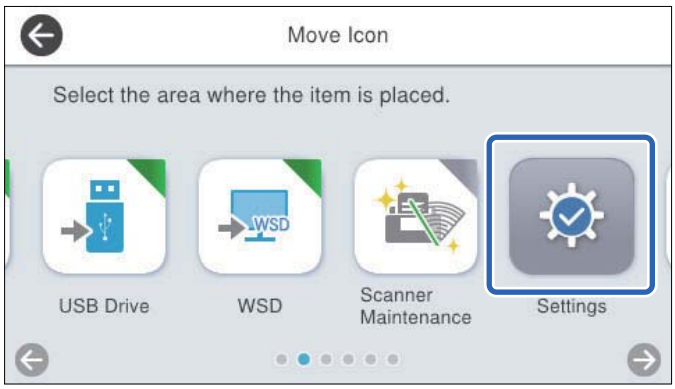
3. Välj **Ja** för att slutföra.

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

4. Välj för att återgå och kontrollera startskärmen.

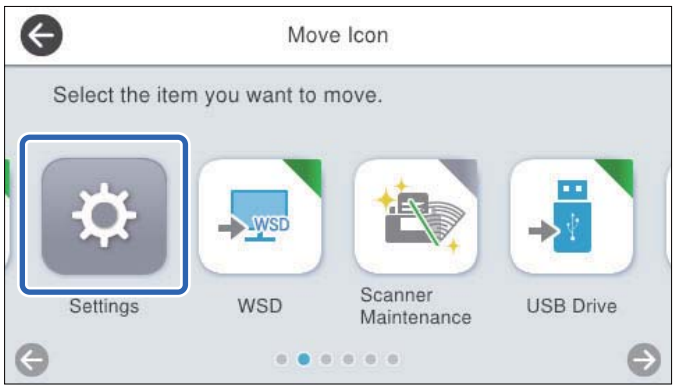
Flytta ikon

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 av produktsäkerhetsfunktioner

Det här avsnittet introducerar säkerhetsfunktionen för Epson-enheterna.

Funktionsnamn	Funktionstyp	Vad man ska ställa in	Vad man ska förhindra
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.
Inställningar för åtkomstkontroll	Om du loggar in på enheten med ett användarkonto som är registrerat i förväg får du använda enheten.	Registrera ett användarkonto. Du kan registrera upp till 10 användarkonton.	Begränsa användare för att förhindra obehörig användning av enheten.
Inställning för externt 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 administratörslösenordet” på sidan 74
➡ ”Inaktivera externt gränssnitt” på sidan 82

Administratörsinställningar

Konfigurera administratörslösenordet

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 endast för Web Config): Ingen (blank)*
- ❏ *·Lösenord: Beroende på den etikett som sitter på produkten.*

  Om det finns en ”PASSWORD”-etikett fäst på baksidan anger du numret med 8 siffror som visas på etiketten. Om det inte finns någon ”PASSWORD”-etikett påklistrad anger du serienumret på etiketten som finns på produktens baksida för det initiala administratörslösenordet.

Du kan 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 igen 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**.

   Det nya lösenordet måste vara 8 till 20 tecken långt och endast innehålla enkla alfanumeriska tecken och symboler.

   Anmärkning:
   Följande ger standardvärden för administratörsinformationen.

   - ❏ *Användarnamn: inget (blank)*
   - ❏ *·Lösenord: Beroende på den etikett som sitter på produkten.*

     Om det finns en "PASSWORD"-etikett fäst på baksidan anger du numret med 8 siffror som visas på etiketten. Om det inte finns någon "PASSWORD"-etikett påklistrad anger du serienumret på etiketten som finns på produktens baksida för det initiala administratörslösenordet.

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

3. Välj **OK**.

Relaterad information

➡ "Hur du kör Web Config i en webbläsare" på sidan 37

Ändra administratörslösenordet från skannerns kontrollpanel

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:
   Det initiala lösenordet för administratören (standard) vid tiden för inköpet beror på den etikett som sitter på produktens baksida. Om det finns en "PASSWORD"-etikett fäst på baksidan anger du numret med 8 siffror som visas på etiketten. Om det inte finns någon "PASSWORD"-etikett påklistrad anger du serienumret på etiketten som finns på produktens baksida för det initiala administratörslösenordet.

5. Ange det nya lösenordet.

   Det nya lösenordet måste vara 8 till 20 tecken långt och endast innehålla enkla alfanumeriska tecken och symboler.

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

6. Ange det nya lösenordet 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.

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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

Låsinställning-objekt på menyn Inst.

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

✓ : Som ska låsas.

- : Som inte ska låsas.

Menyn Inst.		**Låsinställning**
Grundl. inställn.		-
	LCD-ljusstyrka	-
	Ljud	-
	Sömntimer	✓
	Avstängningstimer	✓
	Snabbstart	✓
	Datum-/tidsinställningar	✓
	Språk/Language	✓/-*
	Tangentbord (Den här funktionen är kanske inte tillgänglig beroende på din region.)	-
	Åtgärden avbröts	✓
	PC Anslutning via USB	✓
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	✓
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	✓
	Åtkomstkontroll	✓
	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		-
	Autentisera enhetsstatus		-
	Information om Epson Open Platform		-
	Menu (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

När **Låsinställning** är aktiverat kan du använda följande metoder för att logga in som administratör från skannerns kontrollpanel.

1. Tryck på uppe till höger på skärmen.

2. Om skärmen **Välj användare** visas väljer du **Administratör**.
3. Ange lösenordet för att logga in.

   Ett komplett inloggningsmeddelande visas och sedan visas hemskärmen på kontrollpanelen.

För att logga ut trycker du på  längst upp till höger på skärmen eller så trycker du på knappen  .

Begränsa tillgängliga funktioner (Åtkomstkontroll)

Du kan begränsa användare genom att registrera användarkonton på skannern.

När Åtkomstkontroll är aktiverad kan användaren använda skanningfunktioner genom att ange lösenordet på skannerns kontrollpanel och logga in. Du kan inte skanna om du inte loggar in.

Du kan skanna från en dator genom att registrera din Användarnamn och Lösenord i skannerdrivrutinen (Epson Scan 2). Se Epson Scan 2 hjälp för produkter *Användarhandbok* för mer information kring hur du gör inställningar.

Skapa användarkontot

Du kan skapa ett Åtkomstkontroll-konto.

1. Öppna Web Config, och välj sedan fliken **Produktsäkerhet** > **Inställningar för åtkomstkontroll** > **Användarinställningar**.
2. Klicka på **Lägg till** för det nummer du vill registrera.

   > ***Viktigt:***
   >
   > *Vid användning av skanner med ett autentiseringssystem från Epson eller ett annat företag, registrera Användarnamn in Inställningar för åtkomstkontroll i fack nummer 2 till 10.*
   >
   > *Programvara som autentiseringssystemet använder nummer ett, så att användarnamnet inte visas på skannerns kontrollpanel.*

3. Ställ in varje objekt.

   ❏ Användarnamn:

   Ange namnet som visas på användarnamnslistan med mellan 1 och 14 tecken med alfanumeriska tecken.

   ❏ Lösenord:

   Ange ett lösenord mellan 0 och 20 tecken i ASCII (0x20–0x7E). Lämna lösenordet tomt när du initierar lösenordet.

   ❏ Markera kryssrutan för att aktivera eller inaktivera varje funktion.

   Välj **Skanna** om du vill spara de skannade funktionerna.

4. Klicka på **Tillämpa**.

Redigera användarkontot

Du kan redigera det registrerade Åtkomstkontroll-kontot.

1. Öppna Web Config, och välj sedan fliken **Produktsäkerhet** > **Inställningar för åtkomstkontroll** > **Användarinställningar**.
2. Klicka på **Redigera** för det nummer du vill redigera.
3. Ändra varje alternativ.
4. Klicka på **Tillämpa**.

Ta bort användarkontot

Du kan radera det registrerade Åtkomstkontroll-kontot.

1. Öppna Web Config, och välj sedan fliken **Produktsäkerhet** > **Inställningar för åtkomstkontroll** > **Användarinställningar**.
2. Klicka på **Redigera** för det nummer du vill ta bort.
3. Klicka på **Radera**.

> ***Viktigt:***
> *När du klickar på **Radera** tas användarkontot bort utan att ett bekräftelsemeddelande visas. Var försiktig när du tar bort kontot.*

Aktivera Åtkomstkontroll

När du aktiverar Åtkomstkontroll kan endast den registrerade användaren använda skannern.

Anmärkning:
När Inställningar för åtkomstkontroll är aktiverade måste du meddela användaren om dennes kontoinformation.

1. Öppna Web Config, och välj sedan fliken **Produktsäkerhet** > **Inställningar för åtkomstkontroll** > **Grundläggande**.
2. Välj **Aktivera åtkomstkontroll**.

   Om du aktiverar Inställningar för åtkomstkontroll och vill skriva ut från en dator som inte har autentiseringsinformation väljer du **Tillåt utskrift och skanning utan autentiseringsinformation från en dator**.
3. Klicka på **OK**.

Logga in på en skanner där Åtkomstkontroll är aktiverat

När **Åtkomstkontroll** är aktiverat kan du använda följande metoder för att logga in som administratör från skannerns kontrollpanel.

1. Tryck på  uppe till höger på skärmen.
2. Om skärmen **Välj användare** visas väljer du användaren.

3. Ange lösenordet för att logga in.

   Ett komplett inloggningsmeddelande visas och sedan visas hemskärmen på kontrollpanelen.

För att logga ut trycker du på  längst upp till höger på skärmen eller så trycker du på knappen  .

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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

Aktivera programverifiering vid uppstart

Om du aktiverar funktionen för programverifiering utför skannern verifiering vid start för att kontrollera om obehöriga tredje parter har manipulerat programmet. Om några problem upptäcks startar inte skannern.

Anmärkning:
Genom att aktivera den här funktionen ökar skannerns starttid.

1. Öppna Web Config, och välj sedan fliken **Produktsäkerhet** > **Programverifikation vid start**.

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

   Inst. > ***Systemadministration*** > ***Programverifikation vid start***

2. Välj **På** för att aktivera **Programverifikation vid start**.

3. Klicka på **OK**.

Inaktivera nätverksskanning från din dator

Du kan göra följande inställningar i Web Config för att inaktivera nätverksskanning med Epson Scan 2 från datorn.

1. Öppna Web Config, och välj sedan fliken **Skanna** > **Nätverksskanning**.

2. Rensa kryssrutan för **Epson Scan 2**, och kryssrutan **Aktivera skanning**.

3. Klicka på **Nästa**.

   Bekräftelseskärmen för inställningar visas.

4. Klicka på **OK**.

Aktivera eller inaktivera WSD-skanning

Anmärkning:
Du kan också utföra inställningar för begränsning via skannerns kontrollpanel. Välj ***Inst.*** *>****Systemadministration*** *>* ***WSD-inställningar****.*

Du kan aktivera eller inaktivera WSD-funktionen.

Om du inte vill att din dator ska konfigurera skannern som en WSD-skanningenhet, följer du stegen nedan för att inaktivera WSD-inställningar.

1. Öppna Web Config, och välj sedan fliken **Nätverkssäkerhet** > **Protokoll**.

2. In **WSD-inställningar**, rensa kryssrutan **Aktivera WSD**.

3. Klicka på **Nästa**.

   Bekräftelseskärmen för inställningar visas.

4. Klicka på **OK**.

Anmärkning:
Om din dator fortfarande konfigurerar skannern som en WSD-skanningenhet, väljer du fliken ***Skanna*** *>* ***Nätverksskanning****, och markerar sedan kryssrutan* ***Aktivera skanning*** *i* ***AirPrint****.*

Om AirPrint inaktiverats kommer också, Mopria-skanning från Chromebooks, Windows, och Mopria Scan-appen inaktiveras.

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

➡ ”Registrera en e-postserver” på sidan 44

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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

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.

Använda Web Config för att styra skannerns strömtillförsel

Om din dator fjärrstyrs från skannern kan du fortfarande använda Web Config för att stänga av eller starta om skannern.

1. Öppna Web Config, och välj sedan fliken **Enhetshantering** > **Ström**.

2. Välj **Stäng av** eller **Starta om**.

3. Klicka på **Kör**.

Återställa standardinställningarna

Du kan välja de nätverksinställningar eller andra inställningar som lagras i skannern och återställa dessa inställningar till standardinställningarna.

1. Öppna Web Config, och välj sedan fliken **Enhetshantering** > **Återställ inställningarna**.

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

   Inst. > ***Systemadministration*** > ***Återställ inställningarna***

2. Välj de alternativ som du vill återställa.

3. Klicka på **Kör**.

   Följ sedan instruktionerna på skärmen.

Epson Remote Services-information

Epson Remote Services är en tjänst som med jämna mellanrum samlar in skannerinformation via Internet. Detta kan användas för att förutsäga när förbrukningsvaror och reservdelar behöver bytas ut eller fyllas på, och för att snabbt lösa eventuella fel eller problem.

Kontakta din återförsäljare för mer information om Epson Remote Services.

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: Beroende på den etikett som sitter på produkten.*

  Om det finns en ”PASSWORD”-etikett fäst på baksidan anger du numret med 8 siffror som visas på etiketten.

  Om det inte finns någon ”PASSWORD”-etikett påklistrad anger du serienumret på etiketten som finns på produktens baksida för det initiala administratörslösenordet.

Om du återställer administratörslösenordet återställs det till det initila värdet vid tiden för inköpet.

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 89

➡ ”SSL-/TLS-kommunikation med skannern” på sidan 97

➡ ”Krypterad kommunikation med IPsec/IP-filtrering” på sidan 98

➡ ”Ansluta skannern till ett IEEE802.1X-nätverk” på sidan 109

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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

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 92
➡ ”Uppdatera ett självsignerat certifikat” på sidan 95
➡ ”Konfigurera ett CA-certifikat” på sidan 96

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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

Inställningsalternativ för CSR

Alternativ	Inställningar och förklaringar
Nyckellängd	Välj nyckellängd för CSR.
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

Alternativ	Inställningar och förklaringar
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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37
➡ ”Konfigurera ett CA-signerat Certifikat” på sidan 92
➡ ”Konfigurera ett CA-certifikat” på sidan 96

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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37
➡ ”Konfigurera ett CA-signerat Certifikat” på sidan 92
➡ ”Konfigurera ett CA-certifikat” på sidan 96

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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

IEEE 802.1X Inställningsalternativ för nätverket

Alternativ	Inställningar och förklaringar	
IEEE802.1X (trådbundet LAN)	Du kan aktivera eller inaktivera sidans inställningar (**IEEE802.1X** > **Grundläggande**) för IEEE802.1X (Trådbunden LAN).	
IEEE802.1X (Wi-Fi)	Anslutningsstatusen för IEEE802.1X (Wi-Fi) visas.	
Anslutningsmetod	Anslutningsmetoden för ett aktuellt nätverk visas.	
EAP-typ	Välj ett alternativ för en autentiseringsmetod mellan skannern och en RADIUS-server.	
	EAP-TLS	Du måste skaffa 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 en 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 finns i fältet subject/subjectAltName i ett servercertifikat som skickas från en RADIUS-server eller inte. Ange 0 till 128 1-byte ASCII (0x20 till 0x7E)-tecken.	
Certifikatverifiering (LAN med kabel)	Om du vill utföra **Certifikatverifiering** using **IEEE802.1X (trådbundet LAN)**, välj **Aktivera**. Om du väljer Aktivera, se relaterad information och importera **CA-certifikat**. Observera att Certifikatverifiering alltid är aktiverad i IEEE802.1X (Wi-Fi). Se till att importera CA-certifikat.	
Anonymt namn	Om du väljer **PEAP-TLS** eller **PEAP/MSCHAPv2** som **EAP-typ**, kan du konfigurera ett anonymt namn istället för ett användar-ID för fas 1 i en 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

Relaterad information

➡ ”Konfigurera ett CA-certifikat” på sidan 96

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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

➡ ”Krypterad kommunikation med IPsec/IP-filtrering” på sidan 98

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 98

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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

➡ ”Krypterad kommunikation med IPsec/IP-filtrering” på sidan 98

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 98

Kan inte öppna enheten 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.

Relaterad information

➡ ”Konfigurera ett IEEE 802.1X-nätverk” på sidan 109

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 94

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 95

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 92

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 92

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 94
➡ ”Radera ett CA-signerat certifikat” på sidan 95

Använda Epson Open Platform

Epson Open Platform Översikt

Epson Open Platform är en plattofrm som gör det möjligt för dig att använda autentiseringssystem med den här skannern.

Det kan användas med Epson Print Admin (Epson Authentication System) eller ett autentiseringssystem från tredje part. Du kan hämta loggar via enhet och användare, konfigurera enheter som användare och grupper kan använda, konfigurera gränser öfr funktioner och så vidare.

Om du ansluter en autentiseringsenhet kan du även utföra användarautentisering med ID-kort.

Konfigurera Epson Open Platform

Aktivera Epson Open Platform så att du kan använda enheten från autentiseringssystemet.

1. Hämta en produktnyckel från webbsidan.

   Se mnaualen Epson Open Platform för information om hur du får produktnyckeln.

2. Öppna Web Config, och välj sedan fliken **Epson Open Platform** > **Produktnyckel eller Licensnyckel**.

3. Kontrollera och konfigurera varje objekt.

   ❏ Serienummer

   Enhetens serienummer visas.

   ❏ Version av Epson Open Platform

   Välj version av Epson Open Platform. Motsvarande version varierar beroende på autentiseringssystemet.

   ❏ Produktnyckel eller Licensnyckel

   Ange produktnyckeln du hämtat.

4. Klicka på **Nästa**.

   Bekräftelseskärmen för inställningar visas.

5. Klicka på **OK**.

   Inställningarna tillämpas på skannern.

   Anmärkning:
   Du kan inte använda Epson Print Admin Serverless när systemet är synkroniserat med Epson Open Platform.

Validera Epson Open Platform

Du kan kontrollera giltigheten för Epson Open Platform med någon av följande metoder.

❏ Web Config

En produktnyckel har angetts på fliken **Epson Open Platform** > **Produktnyckel eller Licensnyckel** > **Produktnyckel eller Licensnyckel** och fliken **Epson Open Platform** > **Autentiseringssystem** visas till vänster om menyträdet.

❏ Skannerns kontrollpanel

Kontrollera att produktnyckeln visas i **Inst.** > **Enhetsinformation** > **Information om Epson Open Platform**.

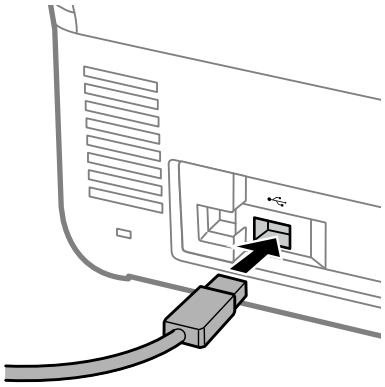
Montera en autentiseringsenhet

Ansluta autentiseringsenheten

Anmärkning:
En autentiseringsenhet används i kombination av användning av ett autentiseringssystem.

> ***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**.

Bekräfta att autentiseringskortet känns igen

Du kan kontrollera att autentiseringskort kan kännas igen genom att använda Web Config.

1. Öppna Web Config, och välj sedan fliken **Enhetshantering** > **Kortläsare**.
2. Håll autentiseringskortet över autentiseringskortläsaren.
3. Klicka på **Kontroll**.
   Resultatet visas.

Felsökning av autentiseringsenheten

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 är certifierade.
Kontakta din återförsäljare för information om autentiseringsenheter- och kort som 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 skannern orsaka problem vid pappersmatning och kvalitetsförsämringar vid skanning. Rengör skannern invändigt i intervaller om 5,000 skanningar.

Du kan kontrollera det senaste antalet skanningar på kontrollenalen eller i Epson Scan 2 Utility.

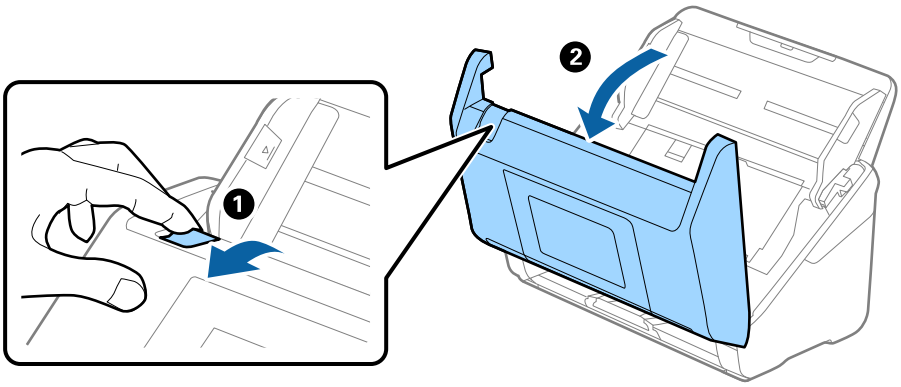
Om en yta får fläckar som är svåra att få bort ska du använda ett Epson-rengöringskit för att ta bort fläckar. Använd en liten mängd rengöringsmedel för rengöringstrasan för att ta bort fläckar.

Viktigt:

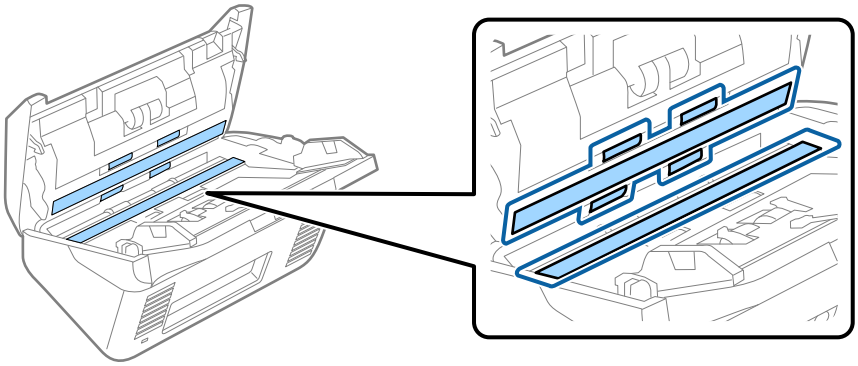
- ❏ *Använd aldrig alkohol, thinner eller något frätande lösningsmedel för att rengöra skannern. Deformering eller missfärgning kan uppstå.*
- ❏ *Spraya aldrig några vätskor eller smörjmedel på skannern. Skada på utrustning eller kretsar kan orsaka onormal drift.*
- ❏ *Öppna aldrig skannerns hölje.*

1. Tryck på knappen ⏻ för att stänga av skannern.
2. Koppla ur AC-adaptern från skannern.

3. Dra i spaken för att öppna skannerluckan.



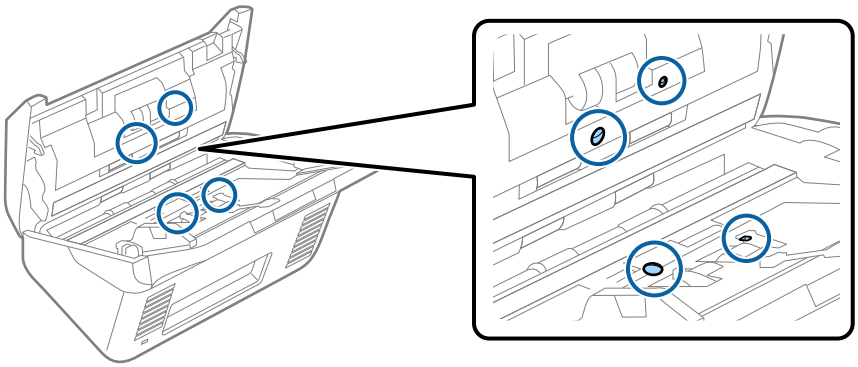
4. Torka bort fläckar på plastrullen (4 ställen) och glaset på undersidan av skannerlocket med en mjuk trasa. Torka av med en mjuk, luddfri trasa som fuktats med en liten mängd rengöringsmedel eller vatten.



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.*

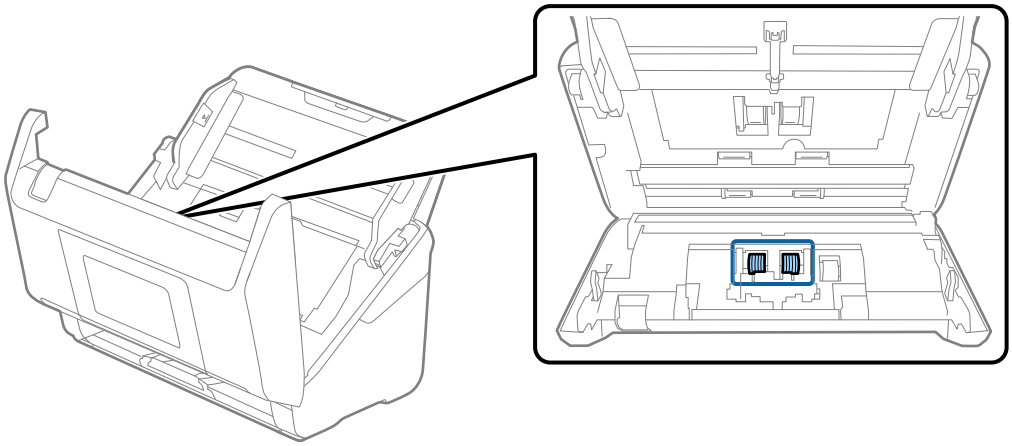
5. Torka bort fläckar på sensorerna med en bomullspad.



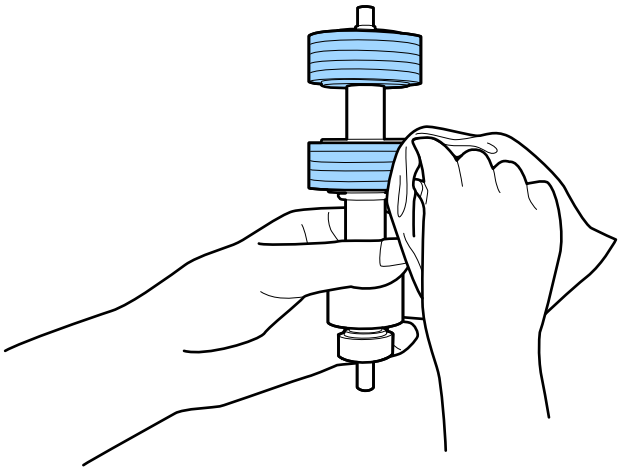
> ***Viktigt:***
> *Använd inte vätskor, såsom rengöringsmedel på en bomullspad.*

6. Öppna luckan och ta sedan bort separationsrullen.

   Se ”Byta valsenhetskit” för mer information.



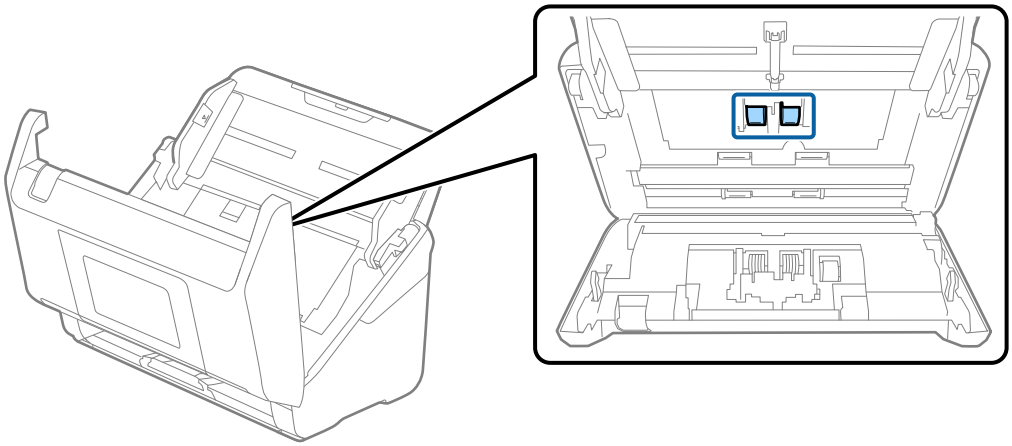
7. Torka av separationsrullen. Torka av med en mjuk, luddfri trasa som fuktats med en liten mängd rengöringsmedel eller vatten.



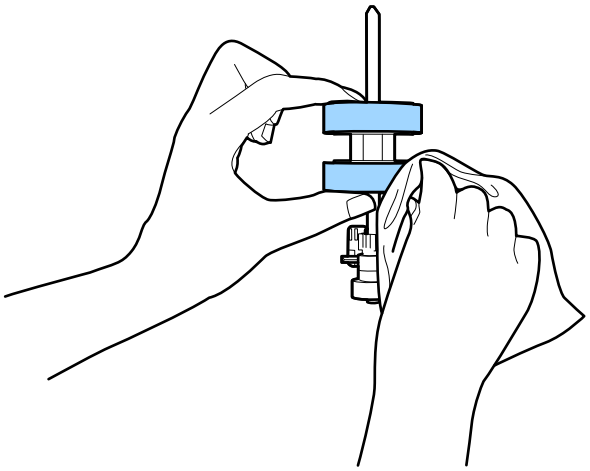
> ***Viktigt:***
> *Använd bara Epson-rengöringskit eller en mjuk, fuktig trasa för att rengöra valsen. Om du använder en torr trasa kan det skada rullens yta.*

8. Öppna luckan och ta sedan bort pickup-valsen.

   Se ”Byta valsenhetskit” för mer information.



9. Torka av pickup-rullen. Torka av med en mjuk, luddfri trasa som fuktats med en liten mängd rengöringsmedel eller vatten.

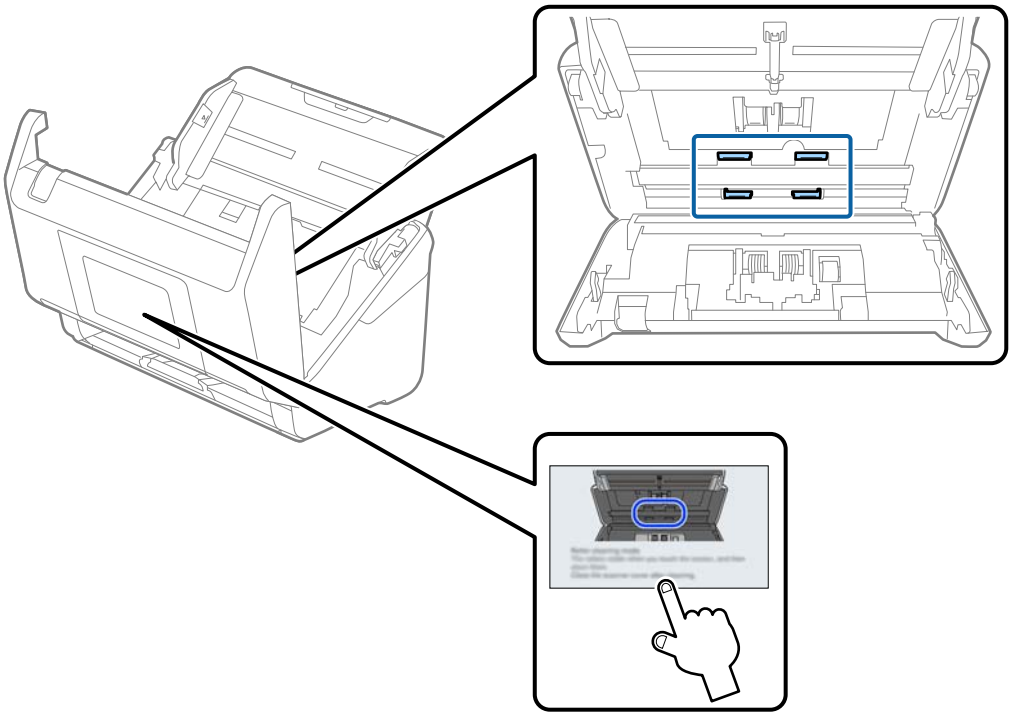


> ***Viktigt:***
>
> *Använd bara Epson-rengöringskit eller en mjuk, fuktig trasa för att rengöra valsen. Om du använder en torr trasa kan det skada rullens yta.*

10. Stäng skannerlocket.
11. Koppla in nätadaptern 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.

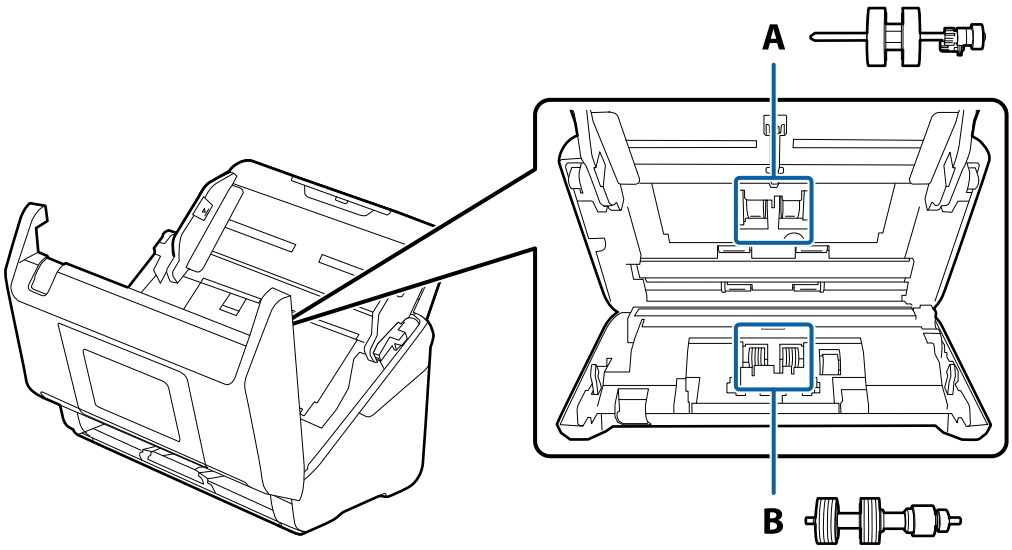
    Skannern stänger rengöringsläget för rullen.

Relaterad information

➡ ”Byta rullmonteringskit” på sidan 129

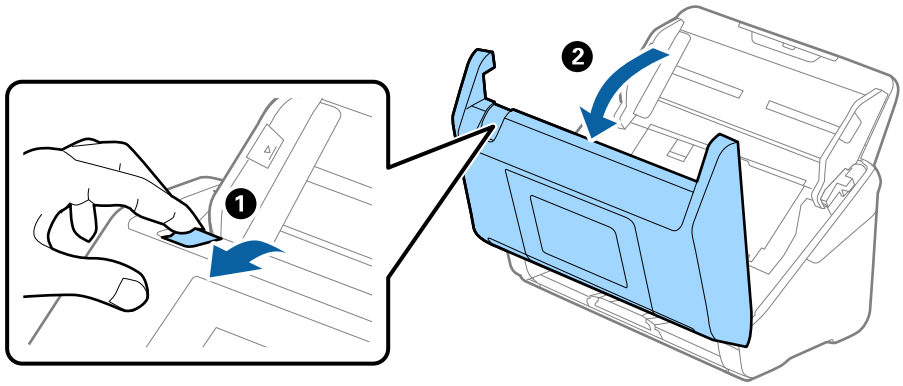
Byta rullmonteringskit

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.

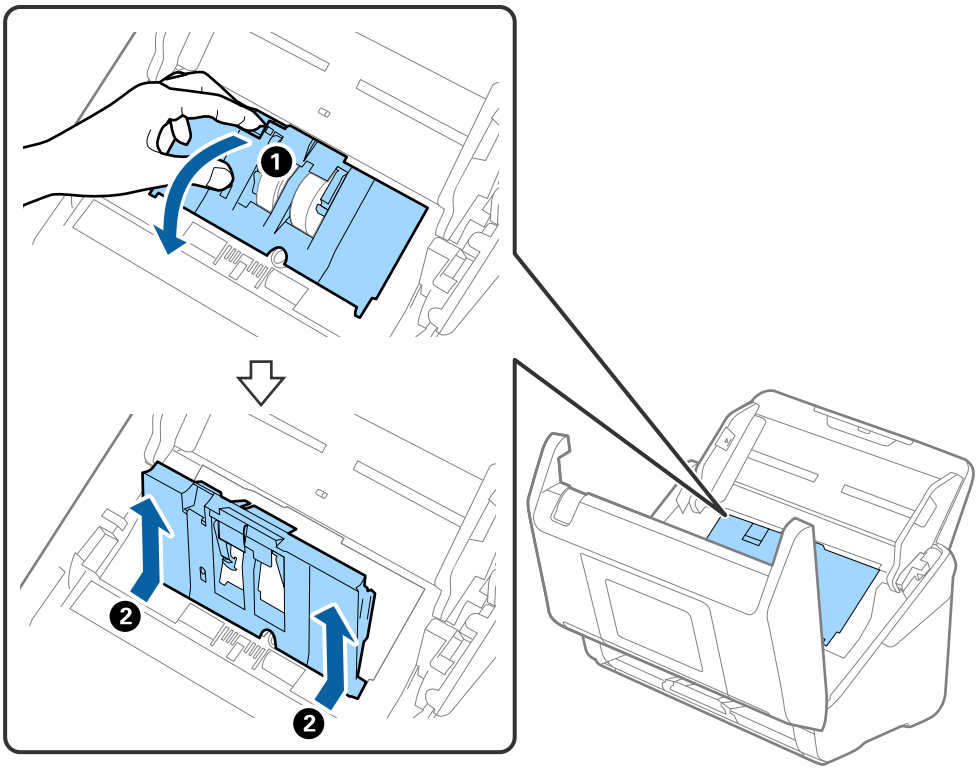


A: pickup-rulle, B: separationsrulle

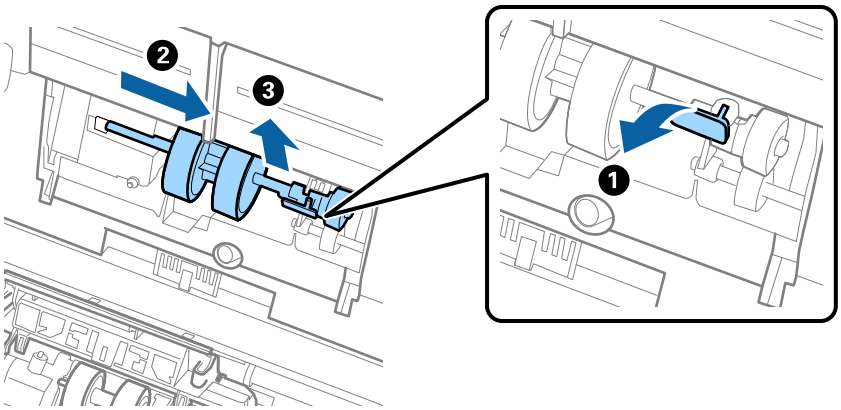
1. Tryck på knappen ⏻ för att stänga av skannern.
2. Koppla ur AC-adaptern från skannern.
3. Dra i spaken för att öppna skannerlocket.



4. Öppna luckan på pickup-rullen och skjut den sedan åt sidan för att ta bort den.

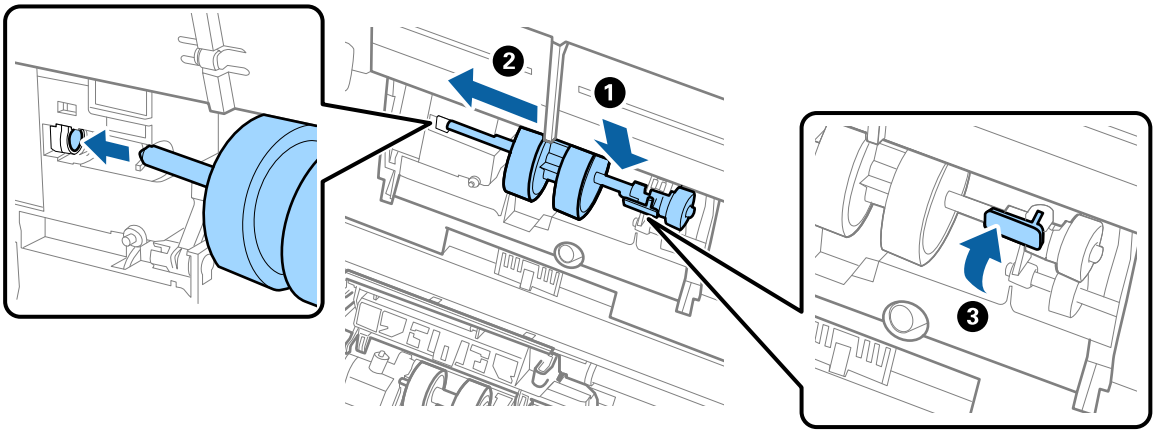


5. Dra fixturen nedåt för rullaxeln och skjut sedan på den och ta bort de installerade pickup-rullarna.

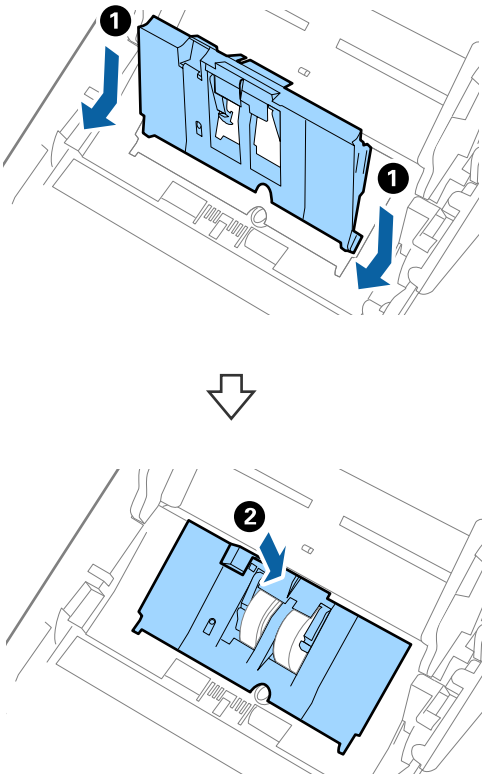


> ***Viktigt:***
>
> *Dra inte ut pickup-rullen med tvång. Detta kan påverka skdan invändigt i skannern.*

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.

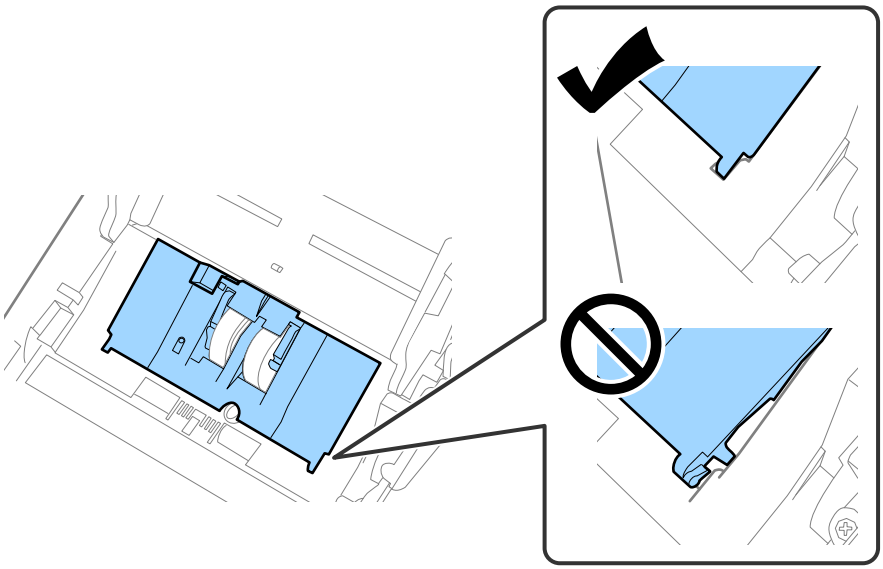


7. Sätt kanten på luckan över pickup-rullen i skåran och skjut på den. Stäng luckan ordentligt.

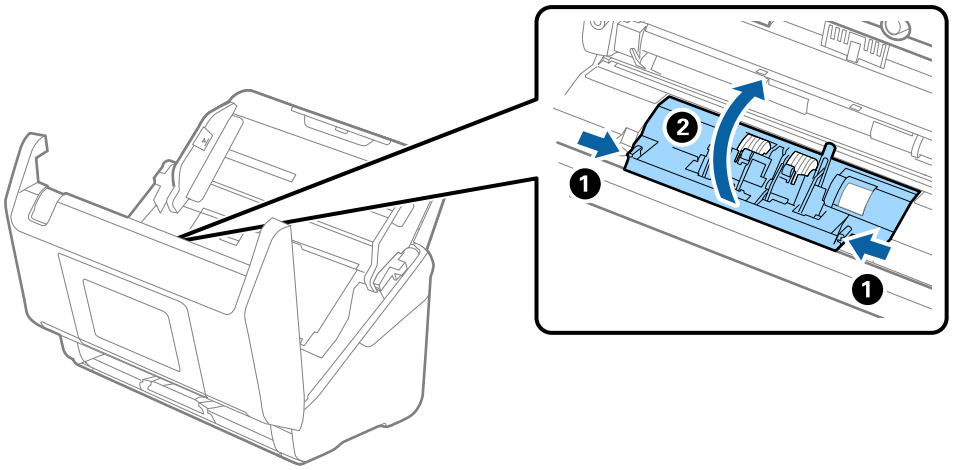


Viktigt:

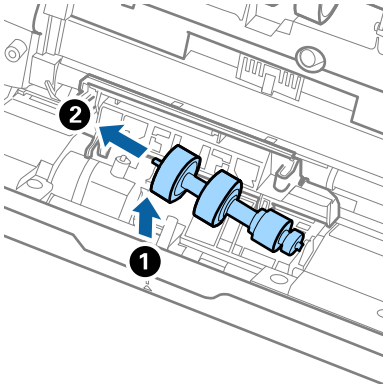
- ❏ *Kontrollera att pickup-locket är stängt.*
- ❏ *Se till att matarvalsarna installerats korrekt om luckan är svår att stänga.*
- ❏ *Installera inte luckan när den är uppställd.*



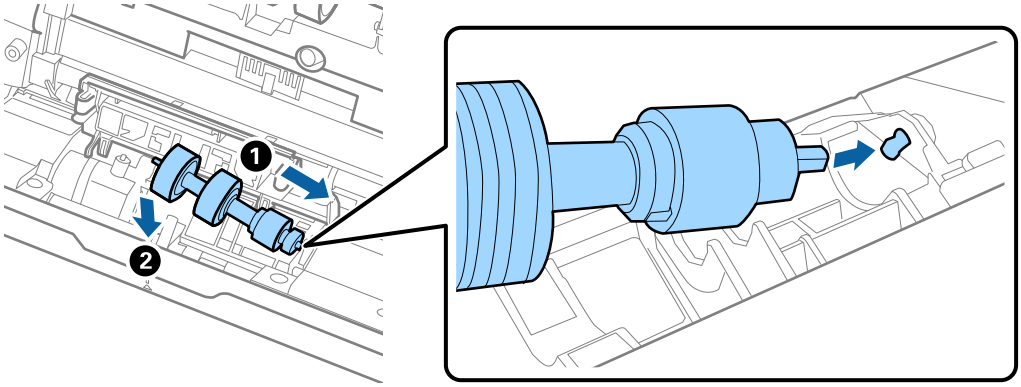
8. Tryck på krokarna på båda ändar av separationsrullslocket för att öppna luckan.



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.

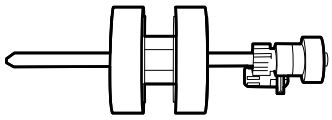
14. Återställ skanningsantalet på kontrollpanelen.

Anmärkning:
Kassera pickup-rullen och separationsrullen i enlighet med de regler och föreskrifter som gäller hos din lokala myndighet. Ta inte isär dem.

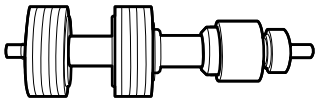
Koder för rullmonteringskit

Delar (pickup-rulle och separationsrulle) 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: separationsrulle

Delens namn	Koder	Livscykel
Valsmonteringskit 2	B12B819711 B12B819721 (endast Indien)	200,000*

* Detta nummer uppnåddes genom konsekvent skanning med Epsons testoriginalpapper, 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 efter att ha bytt ut valsarna

Återställ antalet skanningar med kontrollpanelen Epson Scan 2 Utility efter byte av valsenhetskitet.

Det här avsnittet beskriver hur du återställer via kontrollpanelen.

1. Tryck på **Underhåll av skanner** från hemskärmen.
2. Tryck på **Byte av underhållsvals**.
3. Tryck på **Återställ antal skanningar**.
4. Välj **Antalet skan. efter byte av underhållsvals**, och tryck sedan på **Ja**.

Anmärkning:
*För att återställa från Epson Scan 2 Utility, startar du Epson Scan 2 Utility, klickar på fliken **Räknare**, och klickar sedan på **Återställ** i **Valsmonteringspaketet**.*

Relaterad information

➡ ”Byta rullmonteringskit” på sidan 129

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 tillämpar ändringar.

1. Välj **Inst.** på startskärmen.
2. Välj **Grundl. inställn.**.
3. Välj **Sömntimer** eller **Avstängningsinst.** och gör sedan inställningarna.

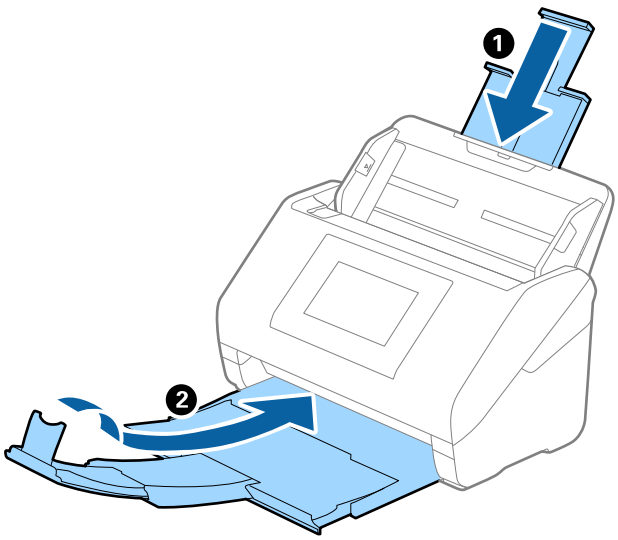
   Anmärkning:
   Tillgängliga funktioner kan variera beroende på köpplatsen.

Transportera skannern

Om du måste transportera skannern en längre sträcka, följ stegen nedan för hur man packar ner skannern.

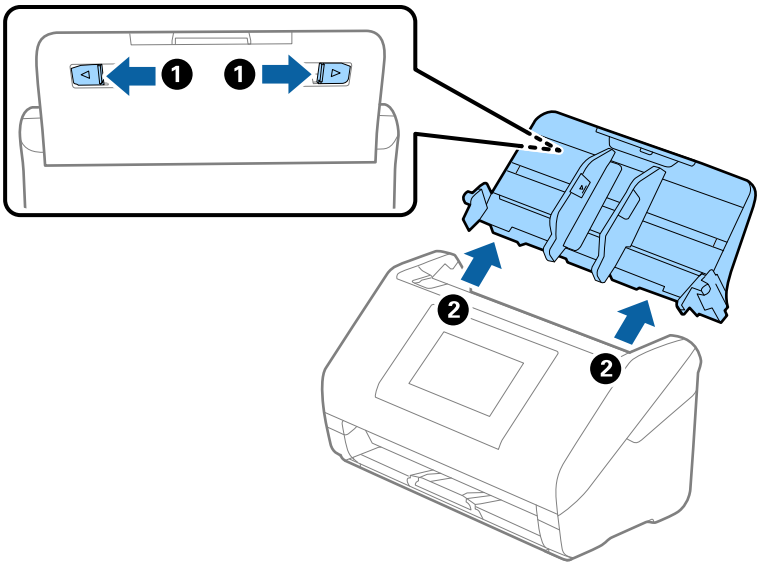
1. Tryck på knappen ⏻ för att stänga av skannern.
2. Koppla ur nätadaptern.
3. Ta bort inmatningsförlängningen och utmatningsfacket.

   Ta bort valfri eller medföljande Paper Alignment Plate om bifogad.
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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

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 att raderas. Raderade inställningar kan inte återställas.*

Anmärkning:
Du kan också göra inställningarna på Web Config.

*Fliken **Enhetshantering** > **Återställ inställningarna***

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 11

   Klicka på startknappen och välj sedan **Alla appar** > **Epson Software** > **EPSON Software Updater**.

   ❏ 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

➡ ”Hur du kör Web Config i en webbläsare” på sidan 37

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. If you cannot update over the network, try this method.

Anmärkning:
Före uppdateringen ska du se till att skannerdrivrutinen Epson Scan 2 installeras på din dator. Om Epson Scan 2 inte är installerat ska du installera det på nytt.

1. Kontrollera webbplatsen för Epson för senaste firmwareuppdateringar.

   http://www.epson.com

   - ❏ Om det finns firmware för din skanner hämtar du den och går till nästa steg.
   - ❏ Om det inte finns någon firmware-information 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.