EPSON
EXCEED YOUR VISION

DS-790WN

Administratorhåndbok

NPD6726-00 NO

Opphavsrett

Varemerker

- ❏ EPSON, EPSON EXCEED YOUR VISION, EXCEED YOUR VISION og deres logoer er registrerte varemerker eller varemerker for Seiko Epson.
- ❏ Microsoft®, Windows®, and Windows Server® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- ❏ Chrome is a trademark of Google LLC.
- ❏ The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- ❏ Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- ❏ FeliCa og PaSoRi er registrerte varemerker som tilhører Sony Corporation.
- ❏ MIFARE er et registrert varemerke som tilhører NXP Semiconductor Corporation.
- ❏ Generell merknad: andre produktnavn som brukes i denne publikasjonen, brukes bare i identifikasjonsøyemed, og kan være varemerker for sine respektive eiere. Epson fraskriver seg alle rettigheter til slike merker.

Innholdsfortegnelse

Avanserte sikkerhetsinnstillinger

Godkjenningsinnstillinger

Vedlikehold

Innledning

Innholdet i dette dokumentet

Dette dokumentet oppgir følgende informasjon for skanneradministratorer.

❏ Nettverksinnstillinger

❏ Forberede skannefunksjonen

❏ Aktivere og administrere sikkerhetsinnstillinger

❏ Aktivere og administrere Godkjenningsinnstillinger

❏ Utføre daglig vedlikehold

For standardmetodene for å bruke skanneren, kan du se *Brukerhåndbok*.

Merknad:
Dette dokumentet beskriver Godkjenningsinnstillinger som leverer selvstendig godkjenning uten å måtte bruke en godkjenningsserver. I tillegg til disse Godkjenningsinnstillinger som ble introdusert i denne bruksanvisningen, kan du også bygge et godkjenningssystem med en godkjenningsserver. For å bygge et system bruker du Document Capture Pro Server Authentication Edition (det forkortede navnet er Document Capture Pro Server AE).

Kontakt ditt lokale Epson kontor for ytterligere informasjon.

Bruk av denne guiden

Merker og symboler

> ***Forsiktig:***
> *Instruksjoner som må følges nøye for å unngå personskade.*

> ***Forsiktighetsregel:***
> *Instruksjoner som må overholdes for å unngå skade på utstyret.*

Merknad:
Gir supplerende og referanseinformasjon.

Relatert informasjon

➡ Lenker til relaterte avsnitt.

Beskrivelser brukt i denne bruksanvisningen

❏ Skjermbilder for programmene er fra Windows 10 eller macOS High Sierra. Innholdet vist på skjermene varierer avhengig av modell og situasjon.

❏ Illustrasjonene som er brukt i denne bruksanvisningen er kun for referanse. Selv om de kan avvike noe fra det faktiske produktet, er driftsmetodene de samme.

Referanser for operativsystem

Windows

I denne håndboken refererer termer som «Windows 10», «Windows 8.1», «Windows 8», «Windows 7», «Windows Server 2019», «Windows Server 2016», «Windows Server 2012 R2», «Windows Server 2012» og «Windows Server 2008 R2» til følgende operativsystemer. I tillegg henviser «Windows» til alle versjoner og «Windows Server» henviser til «Windows Server 2019», «Windows Server 2016», «Windows Server 2012 R2», «Windows Server 2012» og «Windows Server 2008 R2».

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

Mac OS

I denne bruksanvisningen brukes «Mac OS» for å referere til macOS Big Sur, macOS Catalina, macOS Mojave, macOS High Sierra, macOS Sierra, OS X El Capitan, og OS X Yosemite.

Nødvendige innstillinger som passer til ditt formål

Nødvendige innstillinger som passer til ditt formål

Se det følgende for å gjøre nødvendige endringer for å passe formålet ditt.

Koble skanneren til nettverket

Formål	Nødvendige innstillinger
Jeg vil koble skanneren til nettverket.	Sett opp skanneren din for nettverksskanning. "Koble skanneren til nettverket" på side 13
Jeg vil koble skanneren til en ny datamaskin.	Konfigurer nettverksinnstillingene for skanneren på den nye datamaskinen. "Legge til eller skifte ut datamaskinen eller enheter" på side 19

Innstillinger for skanning

Formål	Nødvendige innstillinger
Jeg vil sende skannede bilder via e-post. (Skann til e-post)	1. Konfigurer e-postserveren du vil koble til. "Konfigurere en e-postserver" på side 40 2. Registrer mottakerens e-postadresse i **Kontakter** (valgfritt). Ved å registrere e-postadressen trenger du ikke å skrive den inn hver gang du vil sende noe, du kan bare velge den fra kontaktene dine. "Gjøre kontakter tilgjengelig" på side 59
Jeg vil lagre skannede bilder til en mappe på et nettverk. (Skann til nettverksmappe /FTP)	1. Lag en mappe i nettverket der du vil lagre bildene. "Konfigurere en delt nettverksmappe" på side 43 2. Registrer banen til mappen i **Kontakter** (valgfritt). Ved å registrere mappebanen trenger du ikke å skrive den inn hver gang du vil sende noe, du kan bare velge den fra kontaktene dine. "Gjøre kontakter tilgjengelig" på side 59
Jeg vil lagre skannede bilder i en skytjeneste. (Skann til nettsky)	Konfigurer Epson Connect. Se nettsiden til Epson Connect-portalen for mer informasjon om oppsettet. Du trenger en brukerkonto for den nettbaserte lagringstjenesten du vil koble til når du stiller dette inn. https://www.epsonconnect.com/ http://www.epsonconnect.eu (kun Europa)

Tilpasse kontrollpanelskjermen

Formål	Nødvendige innstillinger
Jeg vil endre det som vises på skannerens kontrollpanel.	Angi **Forhåndsinns** eller **Rediger Startskjerm**. Du kan registrere favoritt-skanneinnstillinger på kontrollpanelet og redigere elementene som vises. "Tilpasse kontrollpanelskjermen" på side 72

Angi grunnleggende sikkerhetsfunksjoner

Formål	Nødvendige innstillinger
Jeg vil unngå at andre enn administratoren kan endre skanneinnstillingene.	Angi et administratorpassord for skanneren. "Administratorinnstillinger" på side 81
Jeg vil deaktivere bruk av skannere med USB-tilkobling.	Deaktiver det eksterne grensesnittet. "Deaktivere eksternt grensesnitt" på side 87

Angi avanserte sikkerhetsfunksjoner

Formål	Nødvendige innstillinger
Jeg vil kontrollere hvilke protokoller som brukes.	Aktiverer eller deaktiver protokollene. "Kontrollere med protokoller" på side 92
Jeg vil kryptere kommunikasjonsbanen.	1. Konfigurer et digitalt sertifikat. "Bruke et digitalt sertifikat" på side 95 2. Konfigurer SSL/TLS-kommunikasjon. "SSL/TLS-kommunikasjon med skanneren" på side 100
Jeg vil bruke kryptert kommunikasjon (IPsec). Jeg vil kunne bruke programvaren kun fra én bestemt datamaskin (IP-filtrering).	Konfigurere policyer for å filtrere trafikk. "Kryptert kommunikasjon ved bruk av IPsec/IP-filtrering" på side 102
Jeg vil bruke en skanner i et IEEE802.1X-nettverk.	Konfigurer IEEE802.1X for skanneren. "Koble skanneren til et IEEE802.1X-nettverk" på side 113

Konfigurere funksjoner som skal godkjennes av skanneren

Formål	Nødvendige innstillinger
Jeg vil aktivere Godkjenningsinnstillinger.	Se følgende for mer informasjon om de tilgjengelige Godkjenningsinnstillinger og Godkjenningsmetode. "Om Godkjenningsinnstillinger" på side 123 "Om Godkjenningsmetode" på side 124

Bruke en server godkjenningssystem

Med Document Capture Pro Server Authentication Edition (forkortet til Document Capture Pro Server AE), kan du bygge et godkjenningssystem som bruker en server til godkjenning.

Kontakt ditt lokale Epson kontor for ytterligere informasjon.

Nettverksinnstillinger

Koble skanneren til nettverket

Denne delen forklarer hvordan du kobler skanneren til nettverket ved hjelp av skannerens kontrollpanel.

Merknad:
Hvis skanneren og datamaskinen er i samme segment, kan du også koble til med installasjonsprogrammet.

❏ *Konfigurere fra nettstedet*

Åpne den følgende nettsiden og tast inn produktnavnet. Gå til ***Oppsett****, og start konfigurasjonen.*

http://epson.sn

❏ *Konfigurering med programvaredisken (kun for modeller som har medfølgende programvaredisk og brukere med Windows-datamaskiner med diskstasjon).*

Sett programvaredisken inn i datamaskinen og følg så instruksjonene på skjermen.

Før tilkobling til nettverket

For å koble til nettverket må du kontrollere tilkoblingsmetoden og informasjonen om innstilling for tilkoblingen på forhånd.

Informasjonssamling i tilkoblingsinnstilling

Klargjør nødvendig konfigureringsinformasjon for å koble til. Kontroller følgende informasjon på forhånd.

Divisjoner	Artikler	Merk
Enhetens tilkoblingsmetode	❏ Ethernet ❏ Wi-Fi	Fastslå hvordan skanneren skal kobles til nettverket. Koble til LAN-bryteren for kablet LAN. Koble til tilgangspunktets nettverk (SSID) for Wi-Fi.
LAN-tilkoblingsinformasjon	❏ IP-adresse ❏ Nettverksmaske ❏ Standard gateway	Fastslå IP-adressen som skal tilordnes til skanneren. Når du tilordner IP-adressen statisk, er alle verdier nødvendige. Når du tilordner IP-adressen automatisk ved hjelp av DHCP-funksjonen, er ikke denne informasjonen nødvendig fordi den angis automatisk.
Wi-Fi-tilkoblingsinformasjon	❏ SSID ❏ Passord	Dette er SSID-en (nettverksnavnet) og passordet til tilgangspunktet som skanneren kobler seg til. Hvis filtrering av MAC-adresse har blitt angitt, må skannerens MAC-adresse registreres på forhånd for å registrere skanneren. Se følgende for støttede standarder. "Nettverksspesifikasjoner" på side 26
DNS-serverinformasjon	❏ IP-adresse for primær DNS ❏ IP-adresse for sekundær DNS	Disse kreves når du spesifiserer DNS-servere. Den sekundære DNS-en angis når systemet har overflødig konfigurasjon og det finnes en sekundær DNS-server. Hvis du er i en liten organisasjon og ikke angir DNS-serveren, angis routerens IP-adresse.

Divisjoner	Artikler	Merk
Proxy-serverinformasjon	❏ Proxy-servernavn	Angi dette når nettverksmiljøet bruker proxyserveren til å få tilgang til Internett fra intranettet og du bruker funksjonen som kobler skanneren direkte til Internett. For følgende funksjoner kobles skanneren direkte til Internett. ❏ Epson Connect-tjenester ❏ Skytjenester fra andre selskaper ❏ Fastvareoppdatering ❏ Sende skannede bilde til SharePoint(WebDAV)
Portnummerinformasjon	❏ Frigjøring av portnummer	Kontroller portnummeret som brukes av skanneren og datamaskinen, og frigjør porten som er blokkert av en brannmur hvis nødvendig. Se følgende for portnummeret som brukes av skanneren. "Bruke porten for skanneren" på side 29

Tildeling av IP-adresse

Dette er de følgende typer IP-adressetildeling.

Statisk IP-adresse:

Tildel forhåndsbestemt IP-adresse til skanneren (vert) manuelt.

Informasjonen om å koble til nettverket (delmettmaske, standard gateway, DNS-server og så videre) må angis automatisk.

IP-adressen endres ikke når enheten slås av, noe som er nyttig når du ønsker å administrere enheter med et miljø hvor du ikke kan endre IP-adresse, eller du ønsker å administrere enheter ved hjelp av IP-adressen. Vi anbefaler innstillinger for skanneren, serveren, osv., som mange datamaskiner bruker. Når sikkerhetsfunksjoner som IPsec/IP-filtrering brukes, må du tildele en fast IP-adresse slik at IP-adressen ikke endres.

Automatisk tildeling ved hjelp av DHCP-funksjonen (dynamisk IP-adresse):

Tildel IP-adressen automatisk til skanneren (vert) ved hjelp av DHCP-funksjonen til DHCP-serveren eller -routeren.

Informasjonen om å koble til nettverket (delnettmaske, standard gateway, DNS-server og så videre) angis automatisk, så du kan enkelt koble enheten til nettverket.

Hvis enheten eller routeren er slått av, eller avhengig av DHCP-serverens innstillinger, kan IP-adressen endres ved ny tilkobling.

Vi anbefaler å administrere enheter med annet enn IP-adressen og kommunisere med protokoller som kan følge IP-adressen.

Merknad:
Når du bruker DHCP-ens reservasjonsfunksjon for IP-adresse, kan du når som helst tildele samme IP-adresse til enhetene.

DNS-server og proxy-server

DNS-serveren har et vertsnavn, domenenavn for e-postadressen osv., i forbindelse med IP-adresseinformasjonen.

Kommunikasjon er ikke mulig hvis den andre parten beskrives av vertsnavnet, domenenavnet osv., når datamaskinen eller skanneren utfører IP-kommunikasjon.

Spør DNS-serveren om den informasjonen og får IP-adressen til den andre parten. Denne prosessen kalles navneløsing.

Derfor kan enheter som datamaskiner og skannere kommunisere ved hjelp av IP-adressen.

Navneløsing er nødvendig for at skanneren skal kunne kommunisere ved hjelp av e-postfunksjonen eller funksjonen for Internet-tilkobling.

Når du bruker disse funksjonene, må innstillingene for DNS-server angis.

Når du tilordner skannerens IP-adresse ved hjelp av DHCP-funksjonen til DHCP-serveren eller -routeren, angis dette automatisk.

Proxy-serveren er plassert på gateway mellom nettverket og Internett, og kommuniserer til datamaskinen, skanner og Internett (motsatt server) på vegne av hver av dem. Den motsatte serveren kommuniserer bare til proxy-serveren. Derfor vil skannerinformasjon som IP-adresse og portnummer kanskje ikke leses, noe som er forbundet med økt sikkerhet.

Når du kobler til Internett via proxyserver, må proxyserveren konfigureres på skanneren.

Koble til nettverket fra kontrollpanelet

Koble skanneren til nettverket ved å bruke kontrollpanelet på skanneren.

Tilordne IP-adressen

Still inn de grunnleggende elementene, for eksempel vertsadresse, Nettverksmaske eller Standard gateway.

Denne seksjonen forklarer prosedyren for hvordan du angir en statisk IP-adresse.

1. Slå på skanneren.

2. Velg **Innst.** på startskjermen til skannerens kontrollpanel.

3. Velg **Nettverksinnstillinger** > **Avansert** > **TCP/IP**.

4. Velg **Manuell** ved **Skaff IP-adresse**.

   Når du stiller inn IP-adresse automatisk ved å bruke DHCP-funksjonen på ruteren, velger du **Auto**. I slikt tilfelle stilles også **IP-adresse**, **Nettverksmaske** og **Standard gateway** i trinn 5 til 6 inn automatisk. Gå derfor til trinn 7.

5. Skriv inn IP-adressen.

   Fokus flyttes til fremste eller bakerste segment separert med punktum hvis du velger ◀ og ▶.

   Bekreft verdien som ble vist på forrige skjerm.

6. Konfigurer **Nettverksmaske** og **Standard gateway**.

   Bekreft verdien som ble vist på forrige skjerm.

   > ***Forsiktighetsregel:***
   >
   > *Hvis kombinasjonen av IP-adresse, Nettverksmaske og Standard gateway er feil, blir* ***Start oppsett*** *inaktiv og vil ikke kunne fortsette med innstillingene. Kontroller at alt som er skrevet inn er riktig.*

7. Skriv inn IP-adressen for den primære DNS-serveren.

   Bekreft verdien som ble vist på forrige skjerm.

   Merknad:
   *Når du velger **Auto** i innstillingene for tilordning av IP-adresse, kan du velge DNS-serverinnstillinger fra **Manuell** eller **Auto**. Hvis du ikke kan hente DNS-server automatisk, velger du **Manuell** og angir DNS-serveradresse. Deretter skriver du sekundær DNS-serveradresse direkte inn. Hvis du velger **Auto**, går du til trinn 9.*

8. Skriv inn IP-adressen for den sekundære DNS-serveren.

   Bekreft verdien som ble vist på forrige skjerm.

9. Trykk **Start oppsett**.

Angi proxy-server

Konfigurer proxyserveren hvis begge av følgende er sant.

❏ Proxyserveren er bygget for Internett-tilkobling.

❏ Ved bruk av en funksjon hvor en skanner kobler direkte til Internett, som Epson Connect-tjenester eller andre selskapers skytjenester.

1. Velg **Innst.** på startskjermen.

   Når du angir innstillinger etter innstilling av IP-adresse, vises **Avansert**-skjermen. Gå til trinn 3.

2. Velg **Nettverksinnstillinger** > **Avansert**.

3. Velg **Proxyserver**.

4. Velg **Bruk** ved **Proxyserver-innst.**.

5. Skriv inn adressen for proxy-serveren med IPv4- eller FQDN-format.

   Bekreft verdien som ble vist på forrige skjerm.

6. Skriv inn portnummeret for proxy-serveren.

   Bekreft verdien som ble vist på forrige skjerm.

7. Trykk **Start oppsett**.

Koble til Ethernet

Koble skanneren til nettverket ved å bruke en LAN-kabel, og kontroller tilkoblingen.

1. Koble sammen skanneren og huben (LAN-bryter) med en LAN-kabel.

2. Velg  på Hjem-skjermen.

3. Velg **Ruter**.

4. Sørg for at innstillingene for Tilkobling og IP-adresse stemmer.

5. Trykk **Lukk**.

Koble til trådløst LAN (Wi-Fi)

Du kan koble skanneren til trådløst LAN (Wi-Fi) på flere måter. Velg en tilkoblingsmetode som passer med miljøet og forholdene du bruker enheten i.

Hvis du kjenner informasjonen til den trådløse ruteren, som SSID og passord, kan du angi innstillingene manuelt.

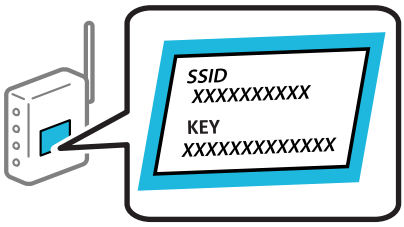
Hvis den trådløse ruteren støtter WPS, kan du angi innstillinger ved hjelp av konfigurering med trykknapp.

Etter du har koblet skanneren til nettverket, kobler til skanneren fra enheten du vil bruke (datamaskin, smartenhet, nettbrett og så videre.)

Angi Wi-Fi-innstillinger ved å angi SSID og passord

Du kan konfigurere et Wi-Fi-nettverk ved å angi nødvendig informasjon for å koble til en trådløs ruter fra skannerens kontrollpanel. Hvis du vil konfigurere ved hjelp av denne metoden, trenger du SSID og passord til en trådløs ruter.

Merknad:
Hvis du bruker en trådløs ruter med standard innstillinger, er SSID og passord angitt på etiketten. Hvis du ikke kjenner SSID-en og passordet, tar du kontakt med personen som konfigurerte trådløs-ruteren, eller så kan du se i dokumentasjonen som fulgte med trådløs-ruteren.



1. Trykk  på startskjermen.

2. Velg **Ruter**.

3. Trykk **Start oppsett**.

   Tilkoblingsdetaljene vises hvis nettverkstilkoblingen allerede er satt opp. Trykk **Bytt til Wi-Fi-tilkobling.** eller **Endre innstillinger** for å endre innstillingene.

4. Velg **Konfigurasjonveiledning for Wi-Fi**.

5. Følg instruksjonene på skjermen for å velge SSID-en, skrive inn passordet for den trådløse ruteren og starte oppsettet.

   Hvis du vil sjekke skannerens tilkoblingsstatus til nettverket etter oppsett er fullført, kan du se lenken til relatert informasjon nedenfor hvis du vil ha mer informasjon.

Merknad:

❏ *Hvis du ikke vet SSID-en, kan du se om det står skrevet på etiketten til trådløs-ruteren. Hvis du bruker trådløs-ruterens standardinnstillinger, bruker du SSID-en angitt på etiketten. Hvis du ikke finner noen informasjon, kan du se dokumentasjonen som fulgte med den trådløse ruteren.*

❏ *Passordet skiller mellom små og store bokstaver.*

❏ *Hvis du ikke vet passordet, kan du se om informasjonen står skrevet på etiketten til den trådløse ruteren. På etiketten er passordet gjerne oppgitt som «Network Key», «Wireless Password» eller lignende. Hvis du bruker standardinnstillingene til den trådløse ruteren, bruker du passordet som er skrevet på etiketten.*

Relatert informasjon

➡ "Kontrollere statusen for nettverkstilkoblingen" på side 25

Utføre Wi-Fi-innstillinger med konfigurasjon med trykknapp (WPS)

Du kan konfigurere Wi-Fi-nettverk automatisk ved å trykke på en knapp på den trådløse ruteren. Du kan konfigurere med denne metoden hvis følgende betingelser er oppfylt.

❏ Den trådløse ruteren er kompatibel med WPS (Wi-Fi Protected Setup).

❏ Den gjeldende Wi-Fi-tilkoblingen har blitt etablert ved å trykke på en knapp på den trådløse ruteren.

Merknad:
Hvis du ikke finner knappen eller du konfigurere med programvaren, må du se dokumentasjonen som følger med den trådløse ruteren.

1. Trykk  på startskjermen.
2. Velg **Ruter**.
3. Trykk **Start oppsett**.

   Tilkoblingsdetaljene vises hvis nettverkstilkoblingen allerede er satt opp. Trykk **Bytt til Wi-Fi-tilkobling.** eller **Endre innstillinger** for å endre innstillingene.
4. Velg **Trykknapp-oppsett (WPS)**.
5. Følg instruksjonene på skjermen.

   Hvis du vil sjekke skannerens tilkoblingsstatus til nettverket etter oppsett er fullført, kan du se lenken til relatert informasjon nedenfor hvis du vil ha mer informasjon.

   Merknad:
   Hvis tilkoblingen mislykkes, starter du den trådløse ruteren på nytt, flytter den nærmere skanneren og prøver igjen.

Relatert informasjon

➡ "Kontrollere statusen for nettverkstilkoblingen" på side 25

Utføre Wi-Fi-innstillinger med konfigurasjon med PIN-kode (WPS)

Du kan automatisk koble til en trådløs ruter ved hjelp av en PIN-kode. Du kan bruke denne metoden til å konfigurere en trådløs ruter hvis den er kompatibel med WPS (Wi-Fi-beskyttet konfigurering). Bruk en datamaskin til å angi PIN-kode til den trådløse ruteren.

1. Trykk  på startskjermen.
2. Velg **Ruter**.
3. Trykk **Start oppsett**.

   Tilkoblingsdetaljene vises hvis nettverkstilkoblingen allerede er satt opp. Trykk **Bytt til Wi-Fi-tilkobling.** eller **Endre innstillinger** for å endre innstillingene.
4. Velg **Annet** > **Oppsett av PIN (WPS)**
5. Følg instruksjonene på skjermen.

   Hvis du vil sjekke skannerens tilkoblingsstatus til nettverket etter oppsett er fullført, kan du se lenken til relatert informasjon nedenfor hvis du vil ha mer informasjon.

   Merknad:
   Se dokumentasjonen som følger med den trådløse ruteren for å få mer informasjon om hvordan du angir PIN-kode.

Relatert informasjon

➡ "Kontrollere statusen for nettverkstilkoblingen" på side 25

Legge til eller skifte ut datamaskinen eller enheter

Koble til en skanner som er koblet til nettverket

Når skanneren allerede er koblet til nettverket, kan du koble en datamaskin eller en smartenhet til skanneren over nettverket.

Bruke en nettverksskanner fra en annen datamaskin

Vi anbefaler å bruke installasjonsprogrammet for å koble skanneren til en datamaskin. Du kan kjøre installasjonsprogrammet med en av følgende metoder.

❏ Konfigurere fra nettstedet

Åpne den følgende nettsiden og tast inn produktnavnet. Gå til **Oppsett**, og start konfigurasjonen.

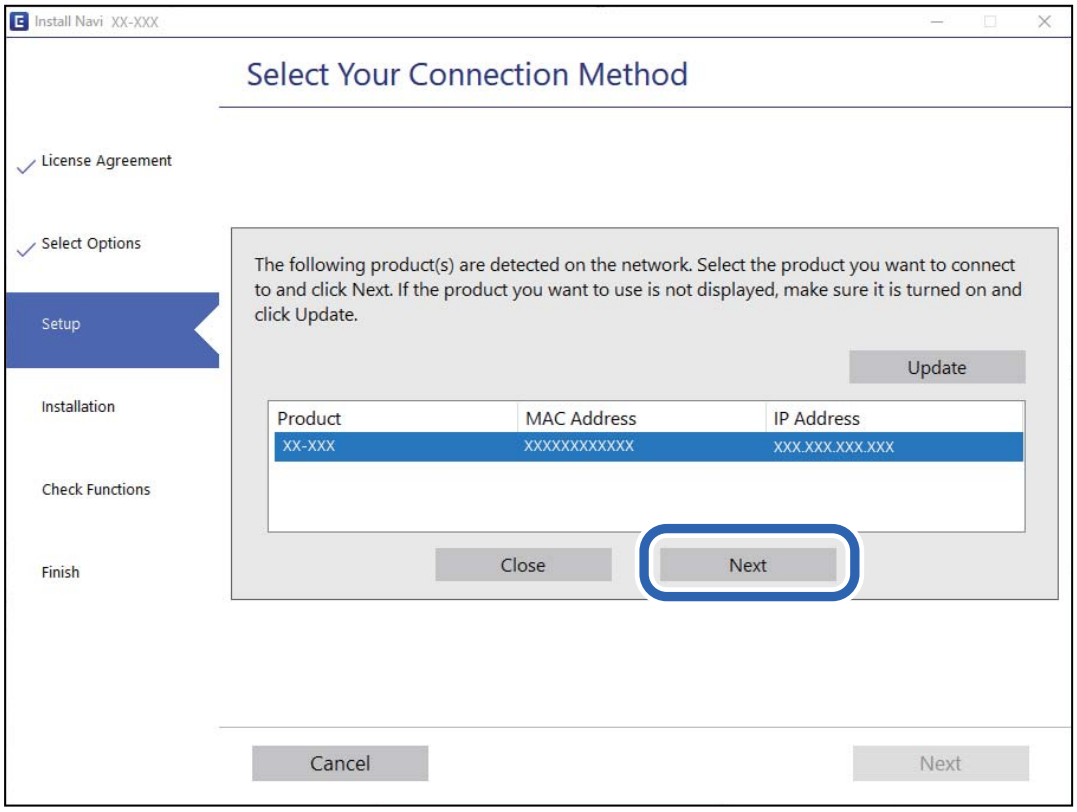
http://epson.sn

❏ Konfigurering med programvaredisken (kun for modeller som har medfølgende programvaredisk og brukere med Windows-datamaskin med diskstasjon).

Sett programvaredisken inn i datamaskinen og følg så instruksjonene på skjermen.

Velge skanneren

Følg instruksjonene på skjermen helt til følgende skjerm vises, velg skannernavnet du vil koble til, og klikk deretter på **Neste**.



Følg instruksjonene på skjermen.

Bruke en nettverksskanner fra en smartenhet

Du kan koble en smartenhet til skanneren ved å bruke en av metodene nedenfor.

Koble til over en trådløs ruter

Koble smartenheten til samme Wi-Fi-nettverk (SSID) som skanneren.

Se følgende for mer informasjon.

"Angi innstillinger for tilkobling til smartenheten" på side 24

Koble til via Wi-Fi Direct

Koble smartenheten til skanneren direkte, uten en trådløs ruter.

Se følgende for mer informasjon.

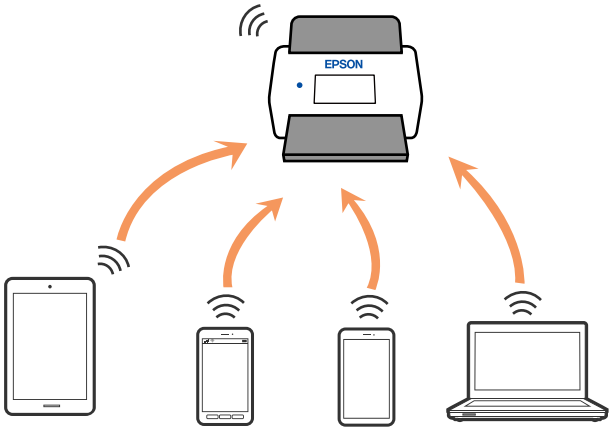
"Koble til en smartenhet og skanner direkte (Wi-Fi Direct)" på side 21

Koble til en smartenhet og skanner direkte (Wi-Fi Direct)

Wi-Fi Direct (Enkel AP) lar deg koble en smartenhet direkte til skanneren uten en trådløs ruter og skanne fra smartenheten.

Om Wi-Fi Direct

Bruk denne tilkoblingsmetoden når du ikke bruker Wi-Fi hjemme eller på kontoret, eller når du vil koble en datamaskin eller smartenhet direkte til skanneren. I denne modusen fungerer skanneren som en trådløs-ruter, og du kan koble enhetene til skanneren uten å bruke en vanlig trådløs-ruter. Enheter som er koblet direkte til skanneren kan imidlertid ikke kommunisere med hverandre gjennom skanneren.



Skanneren kan kobles til med Wi-Fi eller Ethernet og Wi-Fi Direct-modus (Enkel AP) samtidig. Hvis du starter en nettverkstilkobling i Wi-Fi Direct (Enkel AP)-modus mens skanneren er koblet til via Wi-Fi, blir imidlertid Wi-Fi midlertidig frakoblet.

Koble til en smartenhet med Wi-Fi Direct

Denne metoden gir deg mulighet til å koble skanneren direkte til smartenheter uten bruk av trådløs ruter.

1. Velg  på startskjermen.
2. Velg **Wi-Fi Direct**.
3. Velg **Start oppsett**.
4. Start Epson Smart Panel på smartenheten.
5. Følg instruksene som vises på Epson Smart Panel for å koble til skanneren din.

   Når smartenheten din er koblet til skanneren kan du gå til neste trinn.
6. Velg **Ferdig** på skannerens kontrollpanel.

Koble fra Wi-Fi Direct (Enkel AP)-tilkobling

Det finnes to metoder for å deaktivere en Wi-Fi Direct (Enkel AP)-tilkobling: du kan deaktivere alle tilkoblinger ved hjelp av skannerens kontrollpanel eller deaktivere hver tilkobling fra datamaskinen eller smartenheten.

Når du vil deaktivere alle forbindelser, velger du  > **Wi-Fi Direct** > **Start oppsett** > **Endre** > **Deaktiver Wi-Fi Direct**.

> ***Forsiktighetsregel:***
> *Når Wi-Fi Direct (Enkel AP)-tilkobling deaktiveres, blir alle datamaskiner og smartenheter som er koblet til skanneren med Wi-Fi Direct (Enkel AP)-tilkobling frakoblet.*

Merknad:
Hvis du vil koble fra en bestemt enhet, skal du koble den fra via enheten i stedet for via skanneren. Bruk en av følgende metoder til å koble Wi-Fi Direct (Enkel AP)-tilkoblingen fra enheten.

❏ *Koble fra Wi-Fi-tilkoblingen til skannerens nettverksnavn (SSID).*

❏ *Koble til et annet nettverksnavn (SSID).*

Endre innstillinger for Wi-Fi Direct (Enkel AP), som SSID

Når Wi-Fi Direct-tilkobling (Enkel AP) er aktivert, kan du endre innstillingene fra  > **Wi-Fi Direct** > **Start oppsett** > **Endre**, og så vil de følgende menyelementene vises.

Endre nettverksnavn

Endre Wi-Fi Direct (Enkel AP)-nettverksnavnet (SSID) brukt for å koble skanneren til ditt vilkårlige navn. Du kan angi nettverksnavnet (SSID) i ASCII-tegn som vises på programvaretastaturet på kontrollpanelet. Du kan skrive inn opptil 22 tegn.

Når nettverksnavnet (SSID) endres er alle tilkoblede enheter frakoblet. Bruk det nye nettverksnavnet (SSID) hvis du ønsker å koble til enheten igjen.

Endre passord

Endre Wi-Fi Direct-passordet (Enkel AP) for tilkobling til skanneren til din vilkårlige verdi. Du kan angi ASCII-tegn som vises på programvaretastaturet på kontrollpanelet. Du kan skrive inn 8 til 22 tegn.

Når passordet endres er alle tilkoblede enheter frakoblet. Bruk det nye passordet hvis du ønsker å koble til enheten igjen.

Endre frekvensområde

Endre frekvensområdet for Wi-Fi Direct som brukes til å koble til skanneren. Du kan velge 2,4 GHz eller 5 GHz.

Når frekvensområdet endres, blir alle tilkoblede enheter frakoblet. Koble til enheten på nytt.

Merk at når du endrer til 5 GHz, kan du ikke koble til enheter på nytt hvis enheten ikke støtter 5 GHz-frekvensområdet.

Innstillingen vises kanskje ikke, avhengige av området.

Deaktiver Wi-Fi Direct

Deaktiver Wi-Fi Direct-innstillingene for skanneren (Enkel AP). Når det deaktiveres, blir alle enheter koblet til skanneren i Wi-Fi Direct-tilkobling (Enkel AP), frakoblet.

Gjenopprett standardinnst.

Tilbakestill alle Wi-Fi Direct-innstillinger (Enkel AP) til standard.

Tilkoblingsinformasjonen for Wi-Fi Direct (Enkel AP) til smartenheten du lagret til skanneren er slettet.

Merknad:
*Du kan også konfigurere fra **Nettverk**-fanen > **Wi-Fi Direct** på Web Config for følgende innstillinger.*

- ❏ *Aktivere eller deaktivere Wi-Fi Direct (Enkel AP)*
- ❏ *Endre nettverksnavn (SSID)*
- ❏ *Endre passord*
- ❏ *Endre frekvensområdet*

  Innstillingen vises kanskje ikke, avhengige av området.
- ❏ *Tilbakestille Wi-Fi Direct-innstillinger (Enkel AP)*

Tilbakestille nettverkstilkoblingen

Dette avsnittet forklarer hvordan du foretar innstillingene for nettverkstilkobling og endrer tilkoblingsmetoden når du erstatter den trådløse ruteren eller datamaskinen.

Når du skifter ut den trådløse ruteren

Når du skifter ut den trådløse ruteren, angir du innstillinger for tilkoblingen mellom datamaskinen eller smartenheten og skanneren.

Du må angi disse innstillingene hvis du endrer Internett-leverandøren din og så videre.

Angi innstillinger for tilkobling til datamaskinen

Vi anbefaler å bruke installasjonsprogrammet for å koble skanneren til en datamaskin. Du kan kjøre installasjonsprogrammet med en av følgende metoder.

- ❏ Konfigurere fra nettstedet

  Åpne den følgende nettsiden og tast inn produktnavnet. Gå til **Oppsett**, og start konfigurasjonen.

  http://epson.sn
- ❏ Konfigurering med programvaredisken (kun for modeller som har medfølgende programvaredisk og brukere med Windows-datamaskin med diskstasjon).

  Sett programvaredisken inn i datamaskinen og følg så instruksjonene på skjermen.

Velge tilkoblingsmetodene

Følg instruksjonene på skjermen. På skjermbildet **Velg operasjon** velger du **Sett opp Skriver-tilkobling på nytt (for ny nettverksruter eller endring av USB til nettverk osv.)**, og klikker deretter på **Neste**.

Følg instruksjonene på skjermen for å fullføre oppsettet.

Hvis du ikke kan koble til, kan du se følgende for å prøve å løse problemet.

"Kan ikke koble til et nettverk" på side 30

Angi innstillinger for tilkobling til smartenheten

Du kan bruke skanneren fra en smartenhet når du kobler skanneren til samme Wi-Fi-nettverk (SSID) som smartenheten. Gå til følgende nettsted og skriv inn produktnavnet for å bruke skanneren fra en smartenhet. Gå til **Oppsett**, og start konfigurasjonen.

http://epson.sn

Åpne nettstedet fra smartenheten som du ønsker å koble til skanneren.

Når du endrer datamaskinen

Når du endrer datamaskinen, må du angi tilkoblingsinnstillinger mellom datamaskinen og skanneren.

Angi innstillinger for tilkobling til datamaskinen

Vi anbefaler å bruke installasjonsprogrammet for å koble skanneren til en datamaskin. Du kan kjøre installasjonsprogrammet med følgende metode.

❏ Konfigurere fra nettstedet

Åpne den følgende nettsiden og tast inn produktnavnet. Gå til **Oppsett**, og start konfigurasjonen.

http://epson.sn

❏ Konfigurering med programvaredisken (kun for modeller som har medfølgende programvaredisk og brukere med Windows-datamaskin med diskstasjon).

Sett programvaredisken inn i datamaskinen og følg så instruksjonene på skjermen.

Følg instruksjonene på skjermen.

Endre tilkoblingsmetoden til datamaskinen

Dette avsnittet forklarer hvordan du endrer tilkoblingsmetoden når datamaskinen og skanneren er koblet til.

Endre nettverkstilkoblingen fra Ethernet til Wi-Fi

Endre Ethernet-tilkobling til Wi-Fi-tilkobling fra skannerens kontrollpanel. Metoden for å endre tilkoblingsmetode er essensielt den samme som metoden for endring av Wi-Fi-innstillinger.

Relatert informasjon

➡ "Koble til trådløst LAN (Wi-Fi)" på side 17

Endre nettverkstilkoblingen fra Wi-Fi til Ethernet

Følg trinnene nedenfor hvis du vil endre fra en Wi-Fi-tilkobling til en Ethernet-tilkobling.

1. Velg **Innst.** på startskjermen.
2. Velg **Nettverksinnstillinger** > **Oppsett av kablet LAN**.

3. Følg instruksjonene på skjermen.

Endre fra USB til en nettverkstilkobling

Bruke installasjonsprogrammet og konfigurere igjen med en annen tilkoblingsmetode.

❏ Konfigurere fra nettstedet

Åpne den følgende nettsiden og tast inn produktnavnet. Gå til **Oppsett**, og start konfigurasjonen.

http://epson.sn

❏ Konfigurering med programvaredisken (kun for modeller som har medfølgende programvaredisk og brukere med Windows-datamaskin med diskstasjon).

Sett programvaredisken inn i datamaskinen og følg så instruksjonene på skjermen.

Velge Endre tilkoblingsmetodene

Følg instruksjonene på skjermen. På skjermbildet **Velg operasjon** velger du **Sett opp Skriver-tilkobling på nytt (for ny nettverksruter eller endring av USB til nettverk osv.)**, og klikker deretter på **Neste**.

Velg nettverkstilkoblingen du vil bruke, **Koble via trådløst nettverk (Wi-Fi)** eller **Koble til via kablet LAN (Ethernet)**, og klikk deretter på **Neste**.

Følg instruksjonene på skjermen for å fullføre oppsettet.

Kontrollere statusen for nettverkstilkoblingen

Du kan sjekke tilkoblingsstatus for nettverket på følgende vis.

Kontrollere status for nettverkstilkoblingen fra kontrollpanelet

Du kan sjekke status for nettverkstilkobling med nettverksikonet eller nettverksinformasjonen på skannerens kontrollpanel.

Kontrollere status for nettverkstilkoblingen med nettverksikonet

Du kan kontrollere tilkoblingsstatus og styrken på radiobølgene ved hjelp av nettverksikonet på skannerens startskjerm.

	Viser status for nettverkstilkobling. Velg ikonet for å kontrollere og endre gjeldende innstillinger. Dette er snarveien for følgende meny. **Innst.** > **Nettverksinnstillinger** > **Wi-Fi-oppsett**	
		Skanneren er ikke tilkoblet et trådløst (Wi-Fi) nettverk.
		Skanneren søker etter SSID, IP-adresse med fjernet angivelse eller har problemer med et trådløst (Wi-Fi)-nettverk.
		Indikerer at skanneren er koblet til et trådløst nettverk (Wi-Fi). Antall streker indikerer signalstyrken på tilkoblingen. Jo flere streker det er, jo sterkere tilkobling.
		Skanneren er ikke koblet til et trådløst (Wi-Fi) nettverk i Wi-Fi Direct-modus (Enkel AP).
		Skanneren er koblet til et trådløst (Wi-Fi) nettverk i Wi-Fi Direct-modus (Enkel AP).
		Skanneren er ikke tilkoblet et kablet (Ethernet) nettverk eller fjernet angivelse av denne.
		Skanneren er tilkoblet et kablet (Ethernet) nettverk.

Vise detaljert nettverksinformasjon på kontrollpanelet

Når skanneren er koblet til nettverket, kan du også vise annen nettverksrelatert informasjon ved å trykke nettverksmenyene du vil kontrollere.

1. Velg **Innst.** på startskjermen.
2. Velg **Nettverksinnstillinger** > **Nettverkstatus**.
3. For å kontrelle informasjonen, kan du velge menyene du vil kontrollere.
   - ❏ Status for kablet LAN/Wi-Fi

     Viser nettverksinformasjon (enhetsnavn, tilkobling, signalstyrke, også videre) for Ethernet eller Wi-Fi-tilkobling.
   - ❏ Wi-Fi Direct-status

     Viser hvorvidt Wi-Fi Direct er aktivert eller deaktivert, og SSID, passord også videre for Wi-Fi Direct-tilkoblinger.
   - ❏ E-postserverstatus

     Viser nettverksinformasjonen til e-postserveren.

Nettverksspesifikasjoner

Wi-Fi-spesifikasjoner

Se følgende tabell for Wi-Fi-spesifikasjonene.

Land eller regioner utenom de som er oppført nedenfor	Tabell A
Australia New Zealand Taiwan Sør-Korea	Tabell B

Tabell A

Standarder	IEEE 802.11b/g/n*1
Frekvensområde	2,4 GHz
Maksimal transmittert radiofrekvenseffekt	2400–2483,5 MHz: 20 dBm (EIRP)
Kanaler	1/2/3/4/5/6/7/8/9/10/11/12/13
Tilkoblingsmoduser	Infrastruktur, Wi-Fi Direct (Enkel AP)*2*3
Sikkerhetsprotokoller*4	WEP (64/128bit), WPA2-PSK (AES)*5, WPA3-SAE (AES), WPA2/WPA3-Enterprise

*1 Bare tilgjengelig for HT20.

*2 Støttes ikke for IEEE 802.11b.

*3 Infrastruktur- og Wi-Fi Direct-modus eller en Ethernet-tilkobling kan brukes samtidig.

*4 Wi-Fi Direct støtter kun WPA2-PSK (AES).

*5 Overholder WPA2-standarder med støtte for WPA/WPA2 Personal.

Tabell B

Standarder	IEEE 802.11a/b/g/n*1/ac		
Frekvensområder	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)
Tilkoblingsmoduser	Infrastruktur, Wi-Fi Direct (Enkel AP)*4, *5		
Sikkerhetsprotokoller*6	WEP (64/128bit), WPA2-PSK (AES)*7, WPA3-SAE (AES), WPA2/WPA3-Enterprise		

*1 Bare tilgjengelig for HT20.

*2 Ikke tilgjengelig i Taiwan.

*3 Tilgjengeligheten til disse kanalene og bruken av produktene utendørs med disse kanalene varierer etter sted. Les http://support.epson.net/wifi5ghz/ for å få mer informasjon.

*4 Støttes ikke for IEEE 802.11b.

*5 Infrastruktur- og Wi-Fi Direct-modus eller en Ethernet-tilkobling kan brukes samtidig.

*6 Wi-Fi Direct støtter bare WPA2-PSK (AES).

*7 Overholder WPA2-standarder med støtte for WPA/WPA2 Personal.

Ethernet-spesifikasjoner

Standarder	IEEE802.3i (10BASE-T)*1 IEEE802.3u (100BASE-TX)*1 IEEE802.3ab (1000BASE-T)*1 IEEE802.3az (Energi Effektivt Ethernet)*2
Kommunikasjonsmodus	Auto, 10 Mbps Fullduplekss, 10 Mbps Halvdupleks, 100 Mbps Fullduplekss, 100 Mbps Halvdupleks
Kontakt	RJ-45

*1 Bruk en kategori 5e eller høyere STP (skjermet tvunnet par) kabel for å forhindre fare for radioforstyrrelser.

*2 Den tilkoblede enheten skal oppfylle IEEE802.3az standarder.

Nettverksfunksjoner og IPv4/IPv6

Funksjoner	Støttes
Epson Scan 2	IPv4, IPv6
Document Capture Pro/Document Capture	IPv4
Document Capture Pro Server	IPv4, IPv6

Sikkerhetsprotokoll

IEEE802.1X*	
IPsec/IP Filtering	
SSL/TLS	HTTPS Server/Client
SMTPS (STARTTLS, SSL/TLS)	
SNMPv3	

* Du må bruke en tilkoblingsenhet som oppfyller IEEE802.1X.

Bruke porten for skanneren

Skanneren bruker følgende port. Disse portene bør tillates å bli gjort tilgjengelig av nettverksadministrator etter behov.

Når senderen (klienten) er skanneren

Bruk	Destinasjon (server)	Protokoll	Portnummer
Filsending (når skann til nettverksmappe brukes fra skanneren)	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
E-postsending (når skann til e-post-funksjonen brukes fra skanneren)	SMTP-server	SMTP (TCP)	25
		SMTP SSL/TLS (TCP)	465
		SMTP STARTTLS (TCP)	587
POP før SMTP-tilkobling (når skann til e-post-funksjonen brukes fra skanneren)	POP-server	POP3 (TCP)	110
Når Epson Connect er brukt	Epson Connect-server	HTTPS	443
		XMPP	5222
Samler brukerinformasjon (bruk kontaktene fra skanneren)	LDAP-server	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389
Brukergodkjenning når brukerinformasjon samles inn (når kontaktene fra skanneren brukes) Brukergodkjenning når du bruker skann til nettverksmappe (SMB) fra skanneren	KDC-server	Kerberos	88
Control WSD	Klientdatamaskin	WSD (TCP)	5357
Søk på datamaskinen ved push-skanning fra en applikasjon	Klientdatamaskin	Registrering av nettverkspush-skann	2968

Når senderen (klienten) er klientdatamaskinen

Bruk	Destinasjon (server)	Protokoll	Portnummer
Registrer skanneren fra et program som EpsonNet Config og skannerdriveren.	Skanner	ENPC (UDP)	3289
Samle og konfigurer MIB-informasjon fra et program som EpsonNet Config og skannerdriver.	Skanner	SNMP (UDP)	161
Søker WSD-skanner	Skanner	WS-Discovery (UDP)	3702
Videreseng skannedataene fra en applikasjon	Skanner	Nettverksskann (TCP)	1865
Henter jobbinformasjon ved push-skanning fra en applikasjon	Skanner	Nettverkspush-skann	2968
Web Config	Skanner	HTTP (TCP)	80
		HTTPS (TCP)	443

Problemløsning

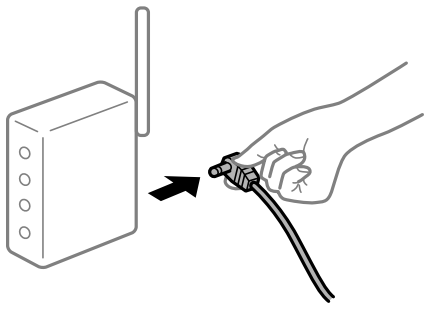
Kan ikke koble til et nettverk

Problemet kan være ett av følgende problemer.

Noe gikk galt med nettverksenheten for Wi-Fi-tilkobling.

Løsninger

Slå av enhetene du vil koble til nettverket. Vent i omtrent 10 sekunder og slå deretter på enhetene i følgende rekkefølge: trådløs ruter, datamaskin eller smartenhet og deretter skanneren. Flytt skanneren og datamaskinen eller smartenheten nærmere den trådløse ruteren for å bedre radiobølgekommunikasjonen og prøv å angi nettverksinnstillinger på nytt.



Enhetene kan ikke motta signaler fra den trådløse ruteren fordi de er for langt fra hverandre.

Løsninger

Når du har flyttet datamaskinen eller smartenheten og skanneren nærmere den trådløse ruteren, slår du av den trådløse ruteren, og slår den deretter på igjen.

Når du endrer den trådløse ruteren, stemmer ikke innstillingene med den nye ruteren.

Løsninger

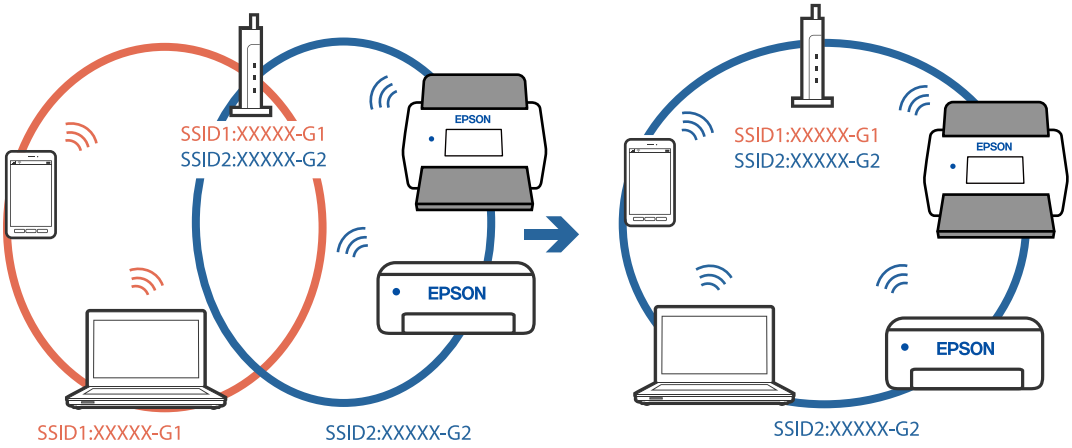
Gjør tilkoblingsinnstillingene på nytt slik at de samsvarer med den nye trådløse ruteren.

SSID-ene som er koblet fra datamaskinen eller smartenhet og datamaskin, er forskjellige.

Løsninger

Når du bruker flere trådløse rutere samtidig, eller den trådløse ruteren har flere SSID-er, og enhetene er koblet til forskjellige SSID-er, kan du ikke koble til den trådløse ruteren.

Koble datamaskinen eller smartenheten til samme SSID som skanneren.



En skillefunksjon for personvern er tilgjengelig på den trådløse ruteren.

Løsninger

De fleste trådløse rutere har en skillefunksjon for personvern som blokkerer kommunikasjon mellom enhetene. Hvis du ikke kan kommunisere mellom skanneren og datamaskinen eller smartenheten, selv om de er koblet til samme nettverk, kan du deaktivere skillefunksjonen for personvern på den trådløse ruteren. Se bruksanvisningen som følger med den trådløse ruteren for mer informasjon.

IP-adressen er ikke tilordnet på riktig måte.

Løsninger

Hvis IP-adressen som er tilordnet til skanneren er 169.254.XXX.XXX, og nettverksmasken er 255.255.0.0, kan ikke IP-adressen tilordnes på riktig måte.

Velg **Innst.** > **Nettverksinnstillinger** > **Avansert** > **TCP/IP-oppsett** på skannerens kontrollpanel, og kontroller deretter IP-adressen og nettmasken tilordnet skanneren.

Start den trådløse ruteren på nytt eller tilbakestill skannerens nettverksinnstillinger.

Det er et problem med nettverksinnstillingene på datamaskinen.

Løsninger

Prøv å åpne hvilken som helst nettside fra datamaskinen for å sørge for at datamaskinens nettverksinnstillinger er riktige. Hvis du ikke kan åpne noen nettsider, er det et problem på datamaskinen.

Kontroller nettverkstilkoblingen på datamaskinen. Se i dokumentasjonen som fulgte med datamaskinen for nærmere informasjon.

Skanneren er koblet til Ethernet ved hjelp av enheter som støtter IEEE 802.3az (energieffektivt Ethernet).

Løsninger

Når du kobler til skanneren med Ethernet ved hjelp av enheter som støtter IEEE 802.3az (energieffektivt Ethernet), kan følgende problemer oppstå avhengig av huben eller ruteren du bruker.

- ❏ Tilkoblingen blir ustabil, skanneren kobler seg til og fra igjen og igjen.
- ❏ Kan ikke koble til skanneren.
- ❏ Kommunikasjonshastigheten blir sakte.

Følg trinnene under for å deaktivere IEEE 802.3az for skanneren og deretter koble til.

1. Ta ut Ethernet-kabelen som er koblet til datamaskinen og skanneren.
2. Når IEEE 802.3az for datamaskinen er aktivert, deaktiverer du det.

   Se i dokumentasjonen som fulgte med datamaskinen for nærmere informasjon.
3. Koble sammen datamaskinen og skanneren direkte med en Ethernet-kabel.
4. Sjekk nettverksinnstillingene på skanneren.

   Velg **Innst.** > **Nettverksinnstillinger** > **Nettverkstatus** > **Status for kablet LAN/Wi-Fi**.
5. Kontroller skannerens IP-adresse.
6. Åpne Web Config på datamaskinen.

   Start en nettleser og angi skannerens IP-adresse.

   "Kjøre web-konfigurasjon på en nettleser" på side 34
7. Velg **Nettverk**-fanen > **Kablet lokalnett**.
8. Velg **Av** ved **IEEE 802.3az**.
9. Klikk på **Neste**.
10. Klikk på **OK**.
11. Ta ut Ethernet-kabelen som er koblet til datamaskinen og skanneren.
12. Hvis du deaktiverte IEEE 802.3az for datamaskinen i trinn 2, aktiverer du det.
13. Koble Ethernet-kablene som du fjernet i trinn 1 til datamaskinen og skanneren.

Hvis problemet vedvarer, kan det hende at andre enheter enn skanneren forårsaker problemet.

Skanneren er slått av.

Løsninger

Pass på at skanneren er slått på.

Du må også vente til statuslampen slutter å blinke, noe som indikerer at skanneren er klar til å skanne.

Programvare for å konfigurere skanneren

Web Config

Web Config er et program som kjører på nettlesere som Internet Explorer og Safari på en datamaskin. Du kan bekrefte skannerens status eller endre nettverkstjenesten og skanneinnstillingene. Siden du får tilgang til og styrer skannerne direkte fra nettverket, egnes det til å konfigurere én skanner om gangen. Koble datamaskinen til samme nettverk som skanneren for å bruke Web Config.

Følgende nettlesere støttes.

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

* Bruk kun den siste versjonen.

Kjøre web-konfigurasjon på en nettleser

1. Kontroller skannerens IP-adresse.

   Velg **Innst.** > **Nettverksinnstillinger** > **Nettverkstatus** på skannerens kontrollpanel. Velg deretter statusen til den aktive tilkoblingsmetoden (**Status for kablet LAN/Wi-Fi** eller **Wi-Fi Direct-status**) for å bekrefte skannerens IP-adresse.

2. Start en nettleser fra en datamaskin eller en smartenhet, og skriv deretter inn skannerens IP-adresse.

   Format:

   IPv4: http://skannerens IP-adresse/

   IPv6: http://[skannerens IP-adresse]/

   Eksempler:

   IPv4: http://192.168.100.201/

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

   Merknad:
   Siden skanneren bruker et selvsignert sertifikat når HTTPS åpnes, vises en advarsel i nettleseren når du starter Web Config. Dette indikerer ikke noe problem og kan trygt ignoreres.

3. Logg inn som administrator for å endre skanneinnstillingene.

   Klikk på **Pålogging for administrator** øverst til høyre på skjermen. Skriv inn **Brukernavn** og **Nåværende passord**, og klikk deretter på **OK**.

   Merknad:
   - *Følgende gir opprinnelige verdier for Web Config-administratorinformasjon.*

     ·Brukernavn: ingen (tomt)

     ·Passord: serienummeret til skanneren

     Du finner serienummeret på etiketten på baksiden av skanneren.
   - *Hvis **Avlogging for administrator** vises øverst til høyre på skjermen er du allerede logget inn som administrator.*

Kjøre Web Config i Windows

Når du skal koble en datamaskin til skanneren med WSD, følger du trinnene nedenfor for å kjøre Web Config.

1. Åpne skannerlisten på datamaskinen.
   - ❏ Windows 10

     Klikk på startknappen og velg **Windows-system** > **Kontrollpanel** > **Vis enheter og skrivere** i **Maskinvare og lyd**.
   - ❏ Windows 8.1/Windows 8

     Velg **Skrivebord** > **Innstillinger** > **Kontrollpanel** > **Vis enheter og skrivere** i **Maskinvare og lyd** (eller **Maskinvare**).
   - ❏ Windows 7

     Klikk på startknappen og velg **Kontrollpanel** > **Vis enheter og skrivere** i **Maskinvare og lyd**.
2. Høyreklikk på skanneren og velg **Egenskaper**.
3. Velg kategorien **Web Service** og klikk på URL.

   Siden skanneren bruker et selvsignert sertifikat når HTTPS åpnes, vises en advarsel i nettleseren når du starter Web Config. Dette indikerer ikke noe problem og kan trygt ignoreres.

   Merknad:
   - ❏ *Følgende gir opprinnelige verdier for Web Config-administratorinformasjon.*

     ·Brukernavn: ingen (tomt)

     ·Passord: serienummeret til skanneren

     Du finner serienummeret på etiketten på baksiden av skanneren.
   - ❏ *Hvis **Avlogging for administrator** vises øverst til høyre på skjermen er du allerede logget inn som administrator.*

Epson Device Admin

Epson Device Admin er et flerfunksjonelt program som lar deg administrere enhetene på et nettverk.

Du kan bruke konfigurasjonsmaler til å bruke forente innstillinger på flere skannere på et nettverk. Dette gjør at det egner seg til å installere og administrere flere skannere.

Du kan laste ned Epson Device Admin fra Epsons nettsted for kundestøtte. For mer informasjon om hvordan du bruker dette programmet, kan du se hjelpedokumentasjonen for Epson Device Admin.

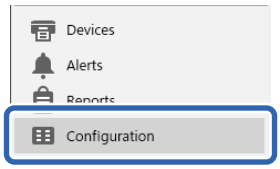
Konfigurasjonsmal

Opprette konfigurasjonsmal

Opprette ny konfigurasjonsmal.

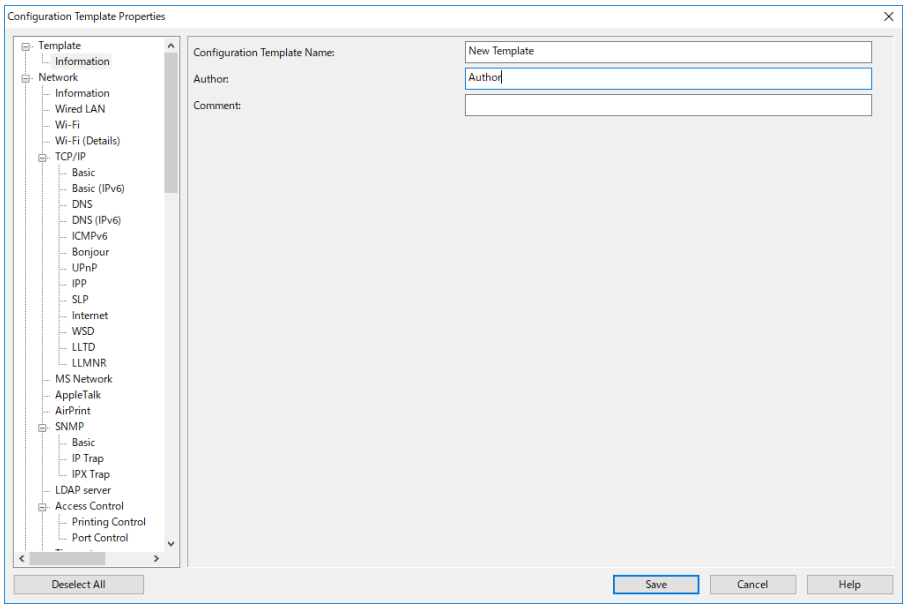
1. Start Epson Device Admin.

2. Velg **Configuration** på sidestolpen med oppgavemeny.



3. Velg **New** på båndmenyen.

4. Angi alle elementene.



Artikkel	Forklaring
Configuration Template Name	Navn på konfigurasjonsmal. Skriv inn opptil 1024 tegn i Unicode (UTF-8).
Author	Informasjon om skaperen av malen. Skriv inn opptil 1024 tegn i Unicode (UTF-8).
Comment	Angi valgfri informasjon. Skriv inn opptil 1024 tegn i Unicode (UTF-8).

5. Velg elementene du ønsker å angi til venstre.

Merknad:
Klikk på menyelementene til venstre for å bytte til hvert skjermbilde. Angitt verdi beholdes dersom du bytter skjermbilde, men ikke hvis du avbryter det. Når du er ferdig med alle innstillingene, klikk ***Save****.*

Bruke konfigurasjonsmal

Bruke den lagrede konfigurasjonsmalen på skanneren. Det valgte elementet på malen brukes. Hvis målskanneren ikke har en egnet funksjon, brukes ikke dette.

Merknad:
Når et administratorpassord er angitt for skanneren, må passordet konfigureres på forhånd.

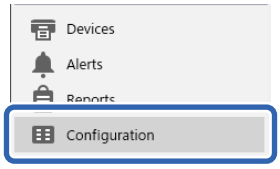
*1. Velg **Options** > **Password manager** fra båndmenyen på Enhetsliste-skjermbildet.*

*2. Velg **Enable automatic password management** og klikk så **Password manager**.*

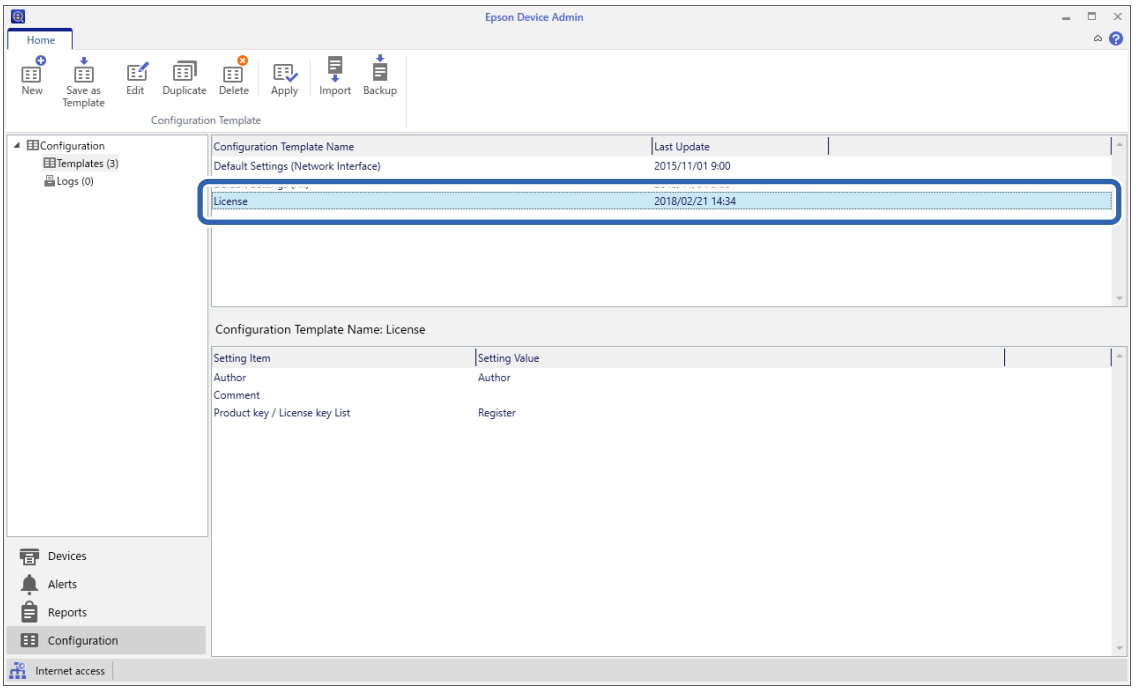
*3. Velg riktig skanner, og klikk på **Edit**.*

*4. Angi passordet og klikk **OK**.*

1. Velg **Configuration** på sidestolpen med oppgavemeny.



2. Velg konfigurasjonsmalen du ønsker å bruke **Configuration Template Name**.



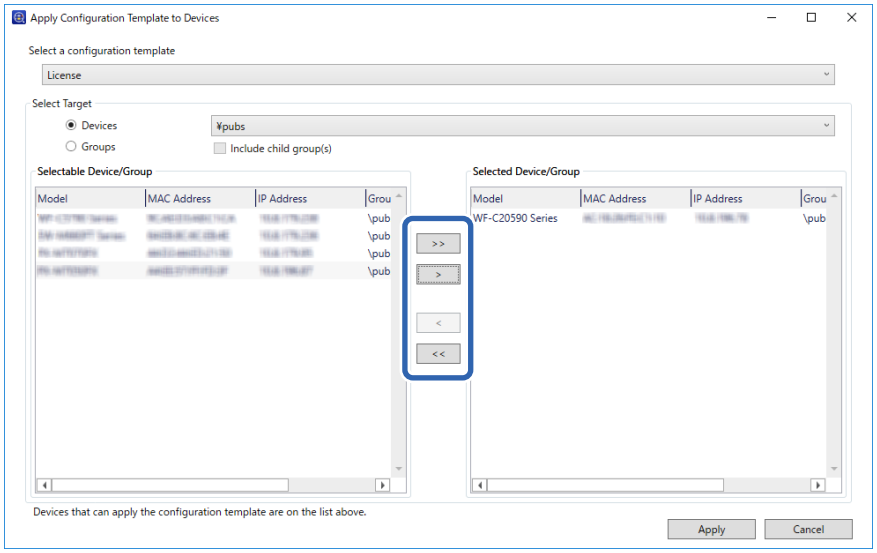
3. Klikk **Apply** på båndmenyen.

   Skjermbildet for enhetsvalg vises.

4. Velg konfigurasjonsmalen du vil bruke.

   Merknad:
   - ❏ *Når du velger **Devices** og grupper som inneholder enheter fra rullegardinmenyen, vises hver enkelt enhet.*
   - ❏ *Grupper vises når du velger **Groups**. Velg **Include child group(s)** hvis du ønsker å automatisk velge barnegrupper i den valgte gruppen.*

5. Flytt skanneren eller gruppene du vil bruke malen for, til **Selected Device/Group**.



6. Klikk på **Apply**.

   Det vises et bekreftelsesskjermbilde for konfigurasjonsmalen som skal brukes.

7. Klikk på **OK** for å bruke konfigurasjonsmalen.

8. Når det vises en melding om at prosedyren er fullført, kan du klikke på **OK**.

9. Klikk **Details** og kontroller informasjonen.

   Når vises på elementene du har brukt, har anvendelsen blitt utført.

10. Klikk på **Close**.

Nødvendige innstillinger for skanning

Konfigurere en e-postserver

Konfigurer e-postserveren fra Web Config.

Når skanneren kan sende e-posten ved å konfigurere e-postserveren, er følgende mulig.

❏ Overfører skanneresultatene ved hjelp av e-post

❏ Mottar e-postvarsling fra skanneren

Kontroller under før du konfigurerer.

❏ Skanneren er koblet til nettverket som har tilgang til e-postserveren.

❏ Informasjon om e-postkonfigurering for datamaskinen som bruker samme e-postserver som skanneren.

Merknad:

❏ *Når du bruker e-postserveren på Internett, må du bekrefte konfigureringsinformasjonen fra leverandøren eller webområdet.*

❏ *Du kan også konfigurere e-postserveren fra kontrollpanelet. Se under for å få tilgang.*

Innst.* > *Nettverksinnstillinger* > *Avansert* > *E-postserver* > *Serverinnstillinger

1. Gå inn på Web Config og velg **Nettverk**-fanen > **E-postserver** > **Grunnleggende**.
2. Angi en verdi for hvert element.
3. Velg **OK**.

   Innstillingene du har valgt, vises.

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34

Innstillingselementer for e-postserver

Artikler	Innstillinger og forklaring	
Godkjenningsmetode	Angi godkjenningsmetoden for skanneren som skal få tilgang til e-postserveren.	
	Av	Autentifisering er deaktivert under kommunikasjon med en e-postserver.
	SMTP-autentisering	Krever at en e-postserver støtter SMTP-autentifisering.
	POP før SMTP	Konfigurer POP3-serveren når du velger denne metoden.
Godkjent konto	Hvis du velger **SMTP-autentisering** eller **POP før SMTP** som **Godkjenningsmetode**, skriver du inn det autentiserte kontonavnet på mellom 0 og 255 tegn i ASCII (0x20 til 0x7E).	
Godkjent passord	Hvis du velger **SMTP-autentisering** eller **POP før SMTP** som **Godkjenningsmetode**, skriver du inn det autentiserte passordet på mellom 0 og 20 tegn i ASCII (0 × 20 til 0 × 7E).	
Avsenderens e-postadresse	Skriv inn avsenderens e-postadresse. Skriv inn opptil 255 tegn i ASCII (0x20 til 0x7E), bortsett fra : ( ) < > [ ] ; ¥. Det første tegnet kan ikke være et punktum «.».	

Artikler	Innstillinger og forklaring	
SMTP-server adresse	Skriv inn mellom 0 og 255 tegn ved hjelp av A–Z a–z 0–9 . -. Du kan bruke IPv4- eller FQDN-format.	
SMTP-server portnummer	Skriv inn et tall mellom 1 og 65 535.	
Sikker forbindelse	Spesifiser sikker tilkobling metode for e-postserveren.	
	Ingen	Hvis du velger **POP før SMTP** i **Godkjenningsmetode**, blir tilkoblingsmetoden satt til **Ingen**.
	SSL/TLS	Dette er tilgjengelig når **Godkjenningsmetode** er satt til **Av** eller **SMTP-autentisering**.
	STARTTLS	Dette er tilgjengelig når **Godkjenningsmetode** er satt til **Av** eller **SMTP-autentisering**.
Sertifikatvalidering	Sertifikatet er validert når dette er aktivert. Vi anbefaler at dette settes til **Aktiver**.	
POP3-server adresse	Hvis du velger **POP før SMTP** som **Godkjenningsmetode**, fyll inn POP3-serveradresse mellom 0 og 255 tegn, med A–Z a–z 0–9 . -. Du kan bruke IPv4- eller FQDN-format.	
POP3-server portnummer	Hvis du velger **POP før SMTP** som **Godkjenningsmetode**, skriver du inn et nummer mellom 1 og 65 535 tegn.	

Kontrollere e-postservertilkoblingen

Du kan kontrollere tilkoblingen til e-postserveren ved å utføre tilkoblingskontrollen.

1. Gå inn på Web Config og velg **Nettverk**-fanen > **E-postserver** > **Tilkoblingstest**.
2. Velg **Start**.

   Tilkoblingstesten til e-postserveren startes. Etter testen vil kontrollrapporten vises.

   Merknad:
   Du kan også kontrollere tilkoblingen til e-postserveren fra kontrollpanelet. Se under for å få tilgang.

   Innst. > ***Nettverksinnstillinger*** > ***Avansert*** > ***E-postserver*** > ***Tilkoblingskontroll***

Testreferanser for e-postservertilkobling

Meldinger	Årsak
Tilkoblingstesten var vellykket.	Denne meldingen vises når tilkoblingen til serveren er vellykket.
SMTP-serverkommunikasjonsfeil. Kontroller følgende. - Nettverksinnstillinger	Denne meldingen vises når ❏ Skanneren er ikke koblet til et nettverk ❏ SMTP-serveren er nede ❏ Nettverkstilkobling er frakoblet under kommunikasjon ❏ Mottok ufullstendige data

Meldinger	Årsak
POP3-serverkommunikasjonsfeil. Kontroller følgende. - Nettverksinnstillinger	Denne meldingen vises når ❏ Skanneren er ikke koblet til et nettverk ❏ POP3-serveren er nede ❏ Nettverkstilkobling er frakoblet under kommunikasjon ❏ Mottok ufullstendige data
Det oppstod en feil under tilkobling til SMTP-serveren. Kontroller følgende. - SMTP-serveradresse - DNS-server	Denne meldingen vises når ❏ Tilkobling til en DNS-server mislyktes ❏ Navnløsning for en SMTP-server mislyktes
Det oppstod en feil under tilkobling til POP3-serveren. Kontroller følgende. - POP3-serveradresse - DNS-server	Denne meldingen vises når ❏ Tilkobling til en DNS-server mislyktes ❏ Navnløsning for en POP3-server mislyktes
SMTP-serverautentiseringfeil. Kontroller følgende. - Autentiseringsmetode - Autentisert konto - Autentisert passord	Denne meldingen vises når SMTP-serverautentisering mislyktes.
POP3-serverautentiseringfeil. Kontroller følgende. - Autentiseringsmetode - Autentisert konto - Autentisert passord	Denne meldingen vises når POP3-serverautentisering mislyktes.
Kommunikasjonsmetode støttes ikke. Kontroller følgende. - SMTP-serveradresse - SMTP-serverportnummer	Denne meldingen vises når du prøver å kommunisere med ikke-støttede protokoller.
Tilkobling til SMTP-serveren mislyktes. Endre Sikker forbindelse til Ingen.	Denne meldingen vises når det oppstår en SMTP uoverensstemmelse mellom en server og en klient, eller når serveren ikke støtter SMTP sikker tilkobling (SSL-tilkobling).
Tilkobling til SMTP-serveren mislyktes. Endre Sikker forbindelse til SSL/TLS.	Denne meldingen vises når det oppstår en SMTP uoverensstemmelse mellom en server og en klient, eller når serveren forespør om å bruke en SSL/TLS tilkobling for en SMTP sikker forbindelse.
Tilkobling til SMTP-serveren mislyktes. Endre Sikker forbindelse til STARTTLS.	Denne meldingen vises når det oppstår en SMTP uoverensstemmelse mellom en server og en klient, eller når serveren forespør om å bruke en STARTTLS tilkobling for en SMTP sikker forbindelse.
Tilkoblingen er ikke klarert. Kontroller følgende. - Dato og klokkeslett	Denne meldingen vises når skannerens dato og klokkeslett er feil eller sertifikatet er utløpt.
Tilkoblingen er ikke klarert. Kontroller følgende. - CA-sertifikat	Denne meldingen vises når skanneren ikke har et rotsertifikat som tilsvarer serveren eller en CA-sertifikat ikke har blitt importert.
Tilkoblingen er ikke sikret.	Denne meldingen vises når det fremstilte sertifikatet er skadet.
SMTP-serverautentisering mislyktes. Endre autentiseringsmetode til SMTP-AUTH.	Denne meldingen vises når en uoverensstemmelser for autentiseringsmetode oppstår mellom en server og en klient. Serveren støtter SMTP-autentisering.
SMTP-serverautentisering mislyktes. Endre autentiseringsmetode til POP før SMTP.	Denne meldingen vises når en uoverensstemmelser for autentiseringsmetode oppstår mellom en server og en klient. Serveren støtter ikke SMTP-autentisering.

Meldinger	Årsak
Avsenderens e-postadresse er feil. Endre til e-postadressen for e-posttjenesten.	Denne meldingen vises når den angitte avsenderens e-postadresse er feil.
Får ikke tilgang til produktet før behandlingen er fullført.	Denne meldingen vises når skanneren er opptatt.

Konfigurere en delt nettverksmappe

Angi en nettverksmappe for å lagre det skannede bildet.

Når du lagrer en fil i en mappe, logger skanneren seg på som brukeren av datamaskinen som mappen ble skapt på.

Opprette den delte mappen

Relatert informasjon

➡ "Før den delte mappen opprettes" på side 43

➡ "Kontrollere nettverksprofilen" på side 43

➡ "Plasseringen hvor den delte mappen opprettes og et eksempel på sikkerheten" på side 44

➡ "Legge til gruppe eller bruker som gir tilgang" på side 55

Før den delte mappen opprettes

Kontroller følgende før den delte mappen opprettes.

❏ Skanneren er koblet til nettverket hvor den kan få tilgang til datamaskinen hvor den delte mappen vil bli opprettet.

❏ Et tegn på flere byte er ikke inkludert i navnet til datamaskinen hvor den delte mappen vil bli opprettet.

Forsiktighetsregel:

Når et tegn på flere byte er inkludert i navnet til datamaskinen, kan lagring av en fil til den delte mappen mislykkes.

I så fall må du bytte til datamaskinen som ikke har et tegn på flere byte i navnet eller endre navnet på datamaskinen.

Når navnet på datamaskinen endres, må du bekrefte med administratoren på forhånd ettersom det kan påvirke enkelte innstillinger som datamaskinbehandling, ressurstilgang, osv.

Kontrollere nettverksprofilen

Kontroller om mappedeling er tilgjengelig på datamaskinen hvor den delte mappen vil bli opprettet.

1. Logg på datamaskinen hvor den delte mappen vil bli opprettet av brukerkontoen med administratorrettigheter.

2. Velg **Kontrollpanel** > **Nettverk og Internett** > **Nettverks- og delingssenter**.

3. Klikk **Endre de avanserte innstillingene for deling** og klikk deretter for profilen med **(gjeldende profil)** i nettverksprofilene som vises.

4. Kontroller om **Aktiver fil- og skriverdeling** er valgt under **Fil- og skriverdeling**.

   Hvis dette allerede er valgt, klikker du **Avbryt** og lukker vinduet.

   Når du endrer innstillingene, klikk **Lagre endringer** og lukk vinduet.

Plasseringen hvor den delte mappen opprettes og et eksempel på sikkerheten

Avhengig av plasseringen hvor den delte mappen opprettes, varierer sikkerhet og beleilighet.

For å betjene den delte mappen fra skannerne eller andre datamaskiner, kreves følgende lese- og endretillatelser for mappen.

❏ **Deling**-fanen > **Avansert deling** > **Tillatelser**

Dette kontrollerer den delte mappens tillatelser til nettverkstilgang.

❏ Åpne tillatelser for **Sikkerhet**-fanen

Dette kontrollerer den delte mappens tillatelser til nettverkstilgang og lokal tilgang.

Når du angir **Alle** for den delte mappen som opprettes på skrivebordet, som et eksempel på oppretting av delt mappe, vil alle brukere med tilgang på datamaskinen ha tilgang.

Brukeren som ikke har autoritet har imidlertid ikke tilgang til dem, fordi skriverbordet (mappen) kontrolleres av brukermappen, og dermed overføres brukermappens sikkerhetsinnstillinger til den. Brukeren som har tilgang til **Sikkerhet**-fanen (pålogget bruker og administrator i dette tilfellet) kan betjene mappen.

Se under for oppretting av riktig plassering.

Dette eksempelet gjelder for oppretting av mappen «scan_folder».

Relatert informasjon

➡ “Eksempel på konfigurasjon for filservere” på side 44

➡ “Eksempel på konfigurasjon for datamaskiner” på side 50

Eksempel på konfigurasjon for filservere

Denne forklaringen er et eksempel på oppretting av delt mappe på driverens rot på den delte datamaskinen, som filserveren under følgende forhold.

Brukere med tilgangskontroll, for eksempel noen som har samme domene for en datamaskin for å opprette en delt mappe, kan åpne den delte mappen.

Angi denne konfigurasjonen når du tillatter en bruker å lese og skrive til datamaskinens delte mappe, som filserveren og den delte datamaskinen.

❏ Plass for oppretting av delt mappe: driverens rot

❏ Mappebane: C:\scan_folder

❏ Åpne tillatelser via nettverk (Del tillatelser): alle

❏ Åpne tillatelser på filsysten (Sikkerhet): Godkjente brukere

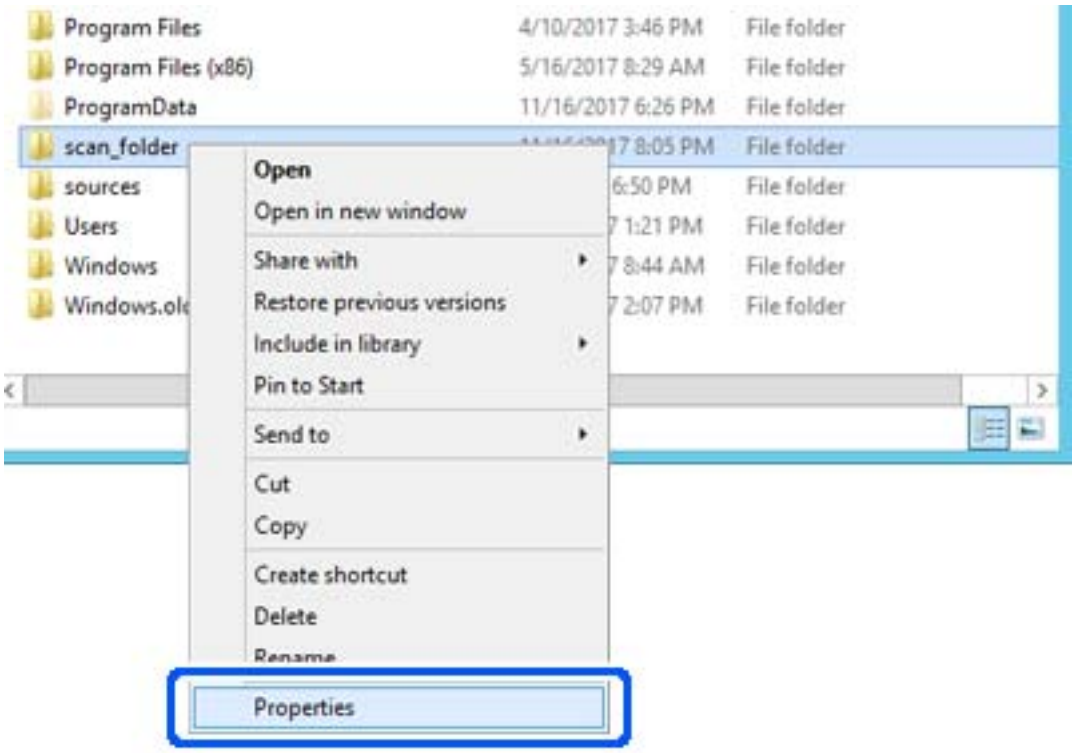
1. Logg på datamaskinen hvor den delte mappen vil bli opprettet av brukerkontoen med administratorrettigheter.

2. Start utforskeren.

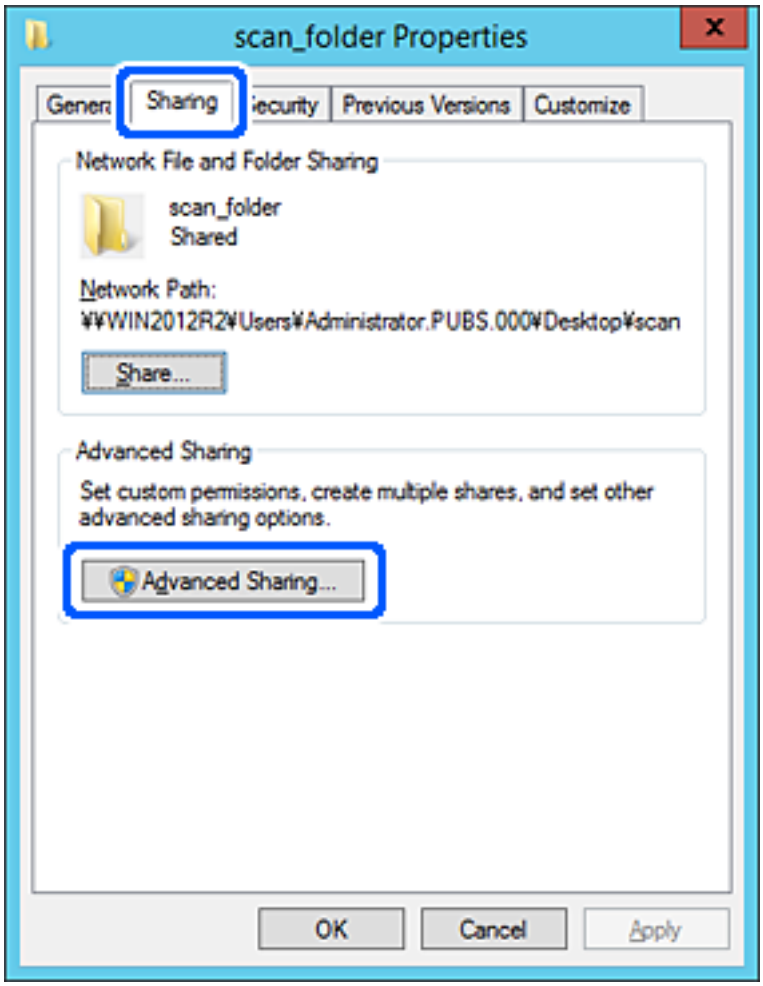
3. Opprett mappen på driverens rot og gi den navnet «scan_folder».

   Skriv mellom 1 og 12 alfanumeriske tegn for mappenavnet. Hvis mappenavnets tegnbegrensning overskrides, kan det være at du ikke vil kunne åpne den normalt ved ulike omgivelser.

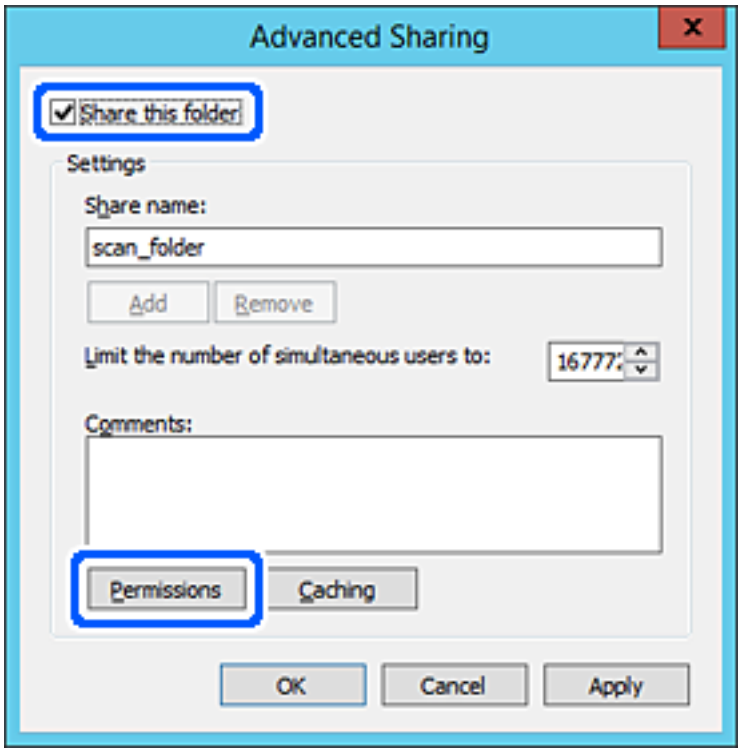
4. Høyreklikk på mappen og velg deretter **Egenskaper**.



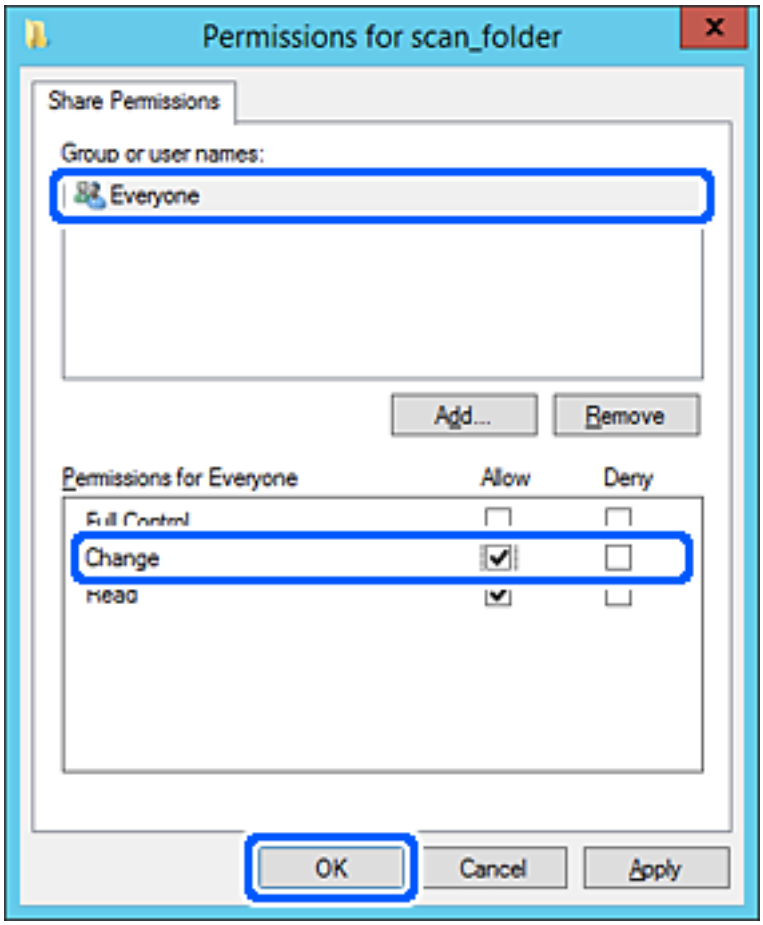
5. Klikk på **Avansert deling** på **Deling**-fanen.



6. Velg **Del denne mappen** og klikk deretter **Tillatelser**.

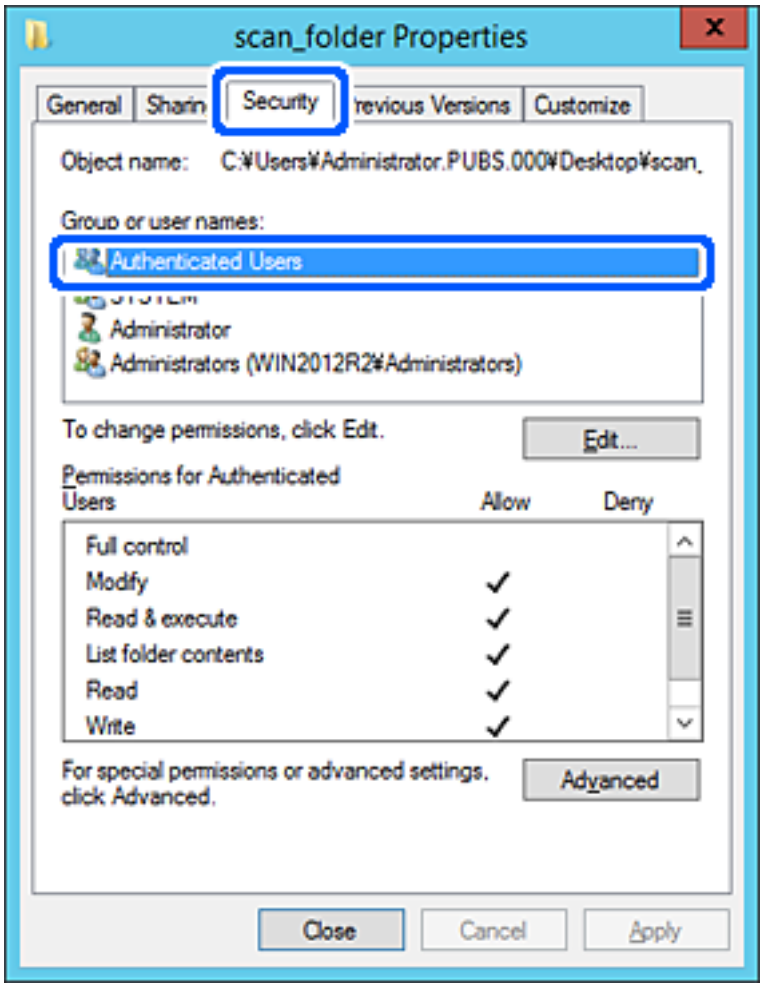


7. Velg **Alle**-gruppen for **Gruppe- eller brukernavn**, velg **Tillat** på **Endre** og klikk deretter **OK**.



8. Klikk **OK**.

9. Velg **Sikkerhet**-fanen og velg deretter **Godkjente brukere** på **Gruppe- eller brukernavn**.

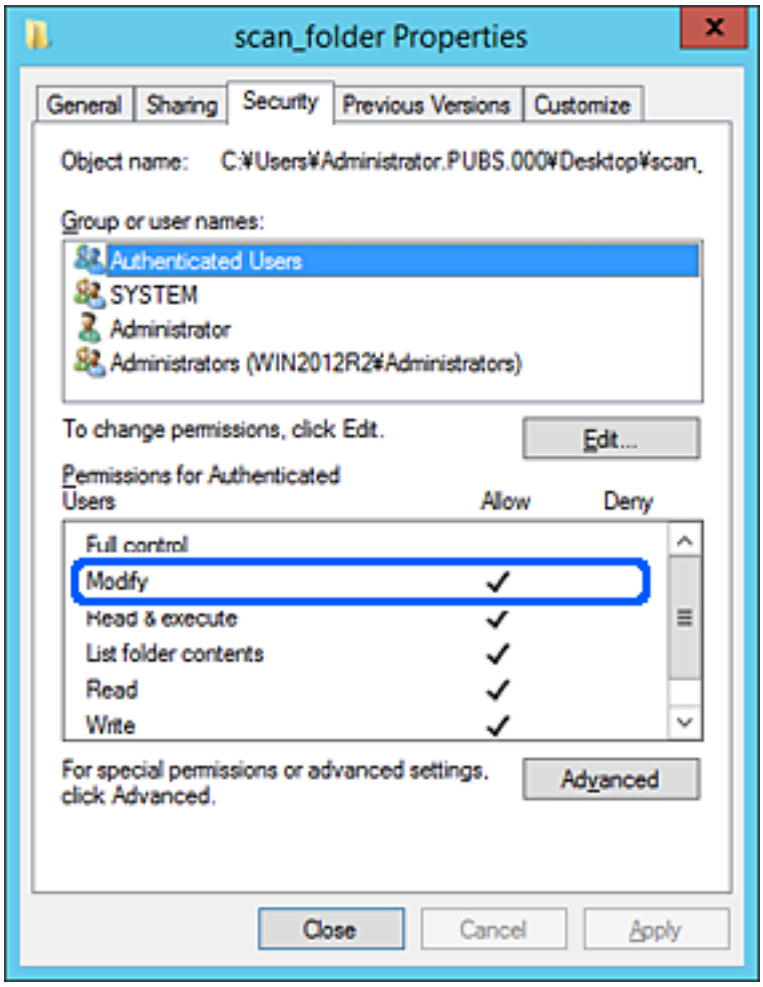


«Godkjente brukere» er den bestemte gruppen som inneholder alle brukere som kan logge på domenet eller datamaskinen. Denne gruppen vises kun når mappen er opprettet rett under rotmappen.

Hvis den ikke vises, kan du legge den til ved å klikke **Rediger**. Se relatert informasjon for mer informasjon.

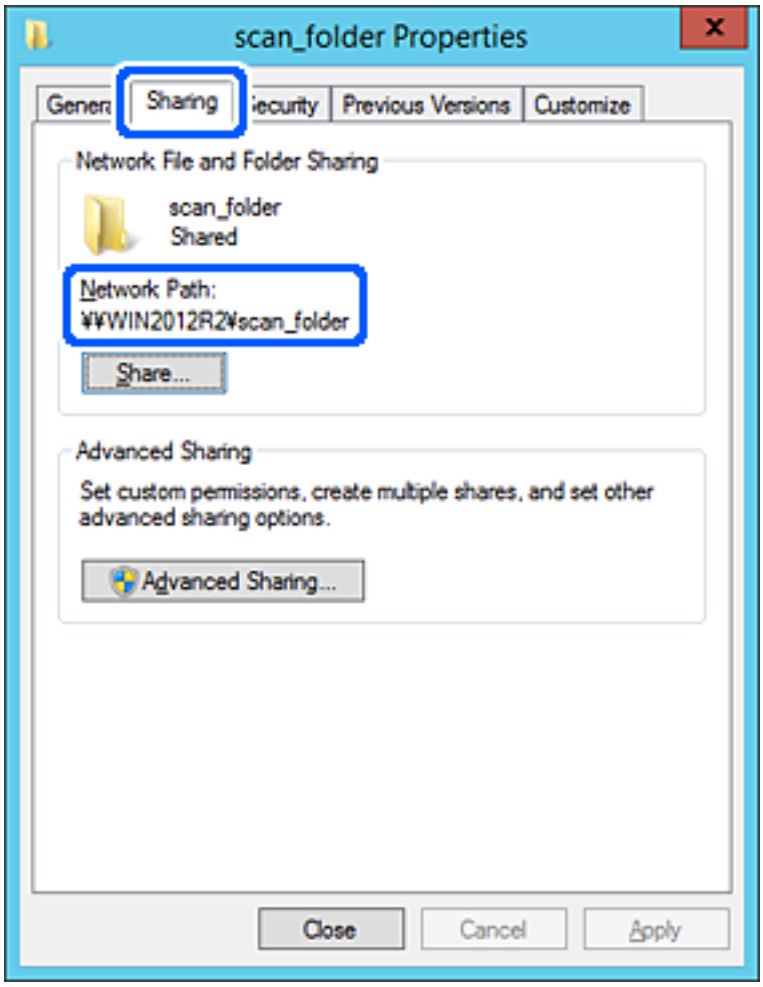
10. Kontroller at **Tillat** på **Modifiser** er valgt i **Tillatelser for godkjente brukere**.

    Hvis det ikke er valgt, velg **Godkjente brukere**, klikk **Rediger**, velg **Tillat** på **Modifiser** i **Tillatelser for godkjente brukere** og klikk deretter **OK**.



11. Velg **Deling**-fanen.

    Nettverksbanen til den delte mappen vises. Den brukes ved registrering til skannerens kontakter. Skriv den ned.



12. Klikk på **OK** eller **Lukk** for å lukke skjermbildet.

    Kontroller om filen kan skrives eller leses på den delte mappen fra datamaskinene med samme domene.

Relatert informasjon

➡ "Legge til gruppe eller bruker som gir tilgang" på side 55
➡ "Registrere et mål for kontakter ved hjelp av Web Config" på side 60

Eksempel på konfigurasjon for datamaskiner

Denne forklaringen er et eksempel på oppretting av delt mappe på skrivebordet til brukeren som nå logger inne på datamaskinen.

Brukeren med administratorrettigheter som logger inn på datamaskinen kan åpne skrivebordsmappen og dokumentmappen som finnes under brukermappen.

Angi denne konfigurasjonen når du IKKE tillater lesing og skriving til en annen bruker til den delte mappen på en datamaskin.

❏ Plass for oppretting av delt mappe: skrivebord

❏ Mappebane: C:\Users\xxxx\Desktop\scan_folder

❏ Åpne tillatelser via nettverk (Del tillatelser): alle

❏ Åpne tillatelse på filsystemet (Sikkerhet): legg ikke til eller legg til bruker-/gruppenavn for å gi tilgang

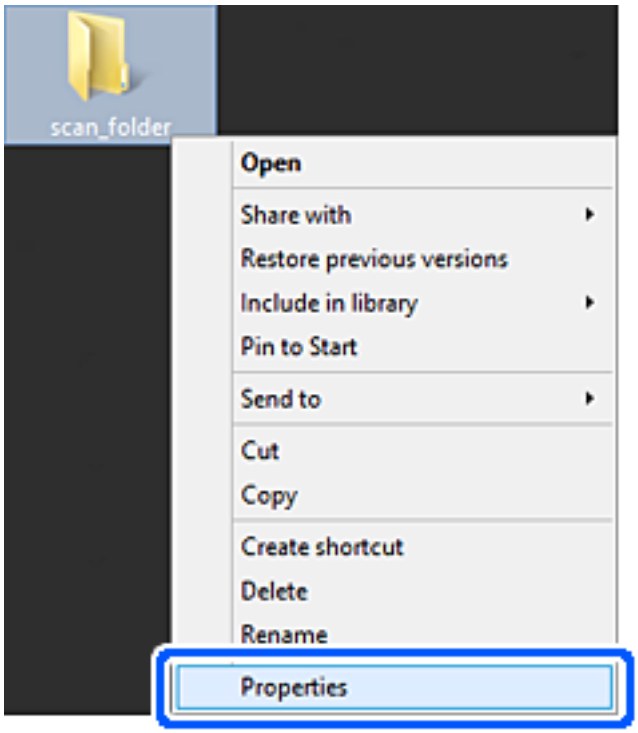
1. Logg på datamaskinen hvor den delte mappen vil bli opprettet av brukerkontoen med administratorrettigheter.

2. Start utforskeren.

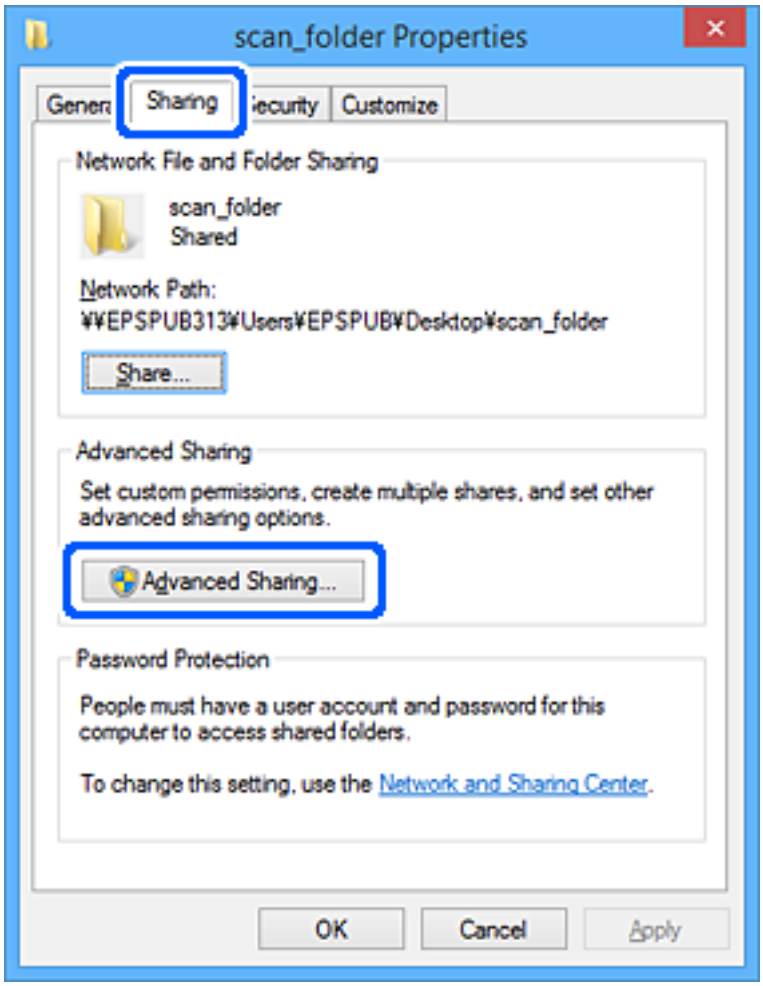
3. Opprett mappen på skrivebordet og gi den navnet «scan_folder».

   Skriv mellom 1 og 12 alfanumeriske tegn for mappenavnet. Hvis mappenavnets tegnbegrensning overskrides, kan det være at du ikke vil kunne åpne den normalt ved ulike omgivelser.

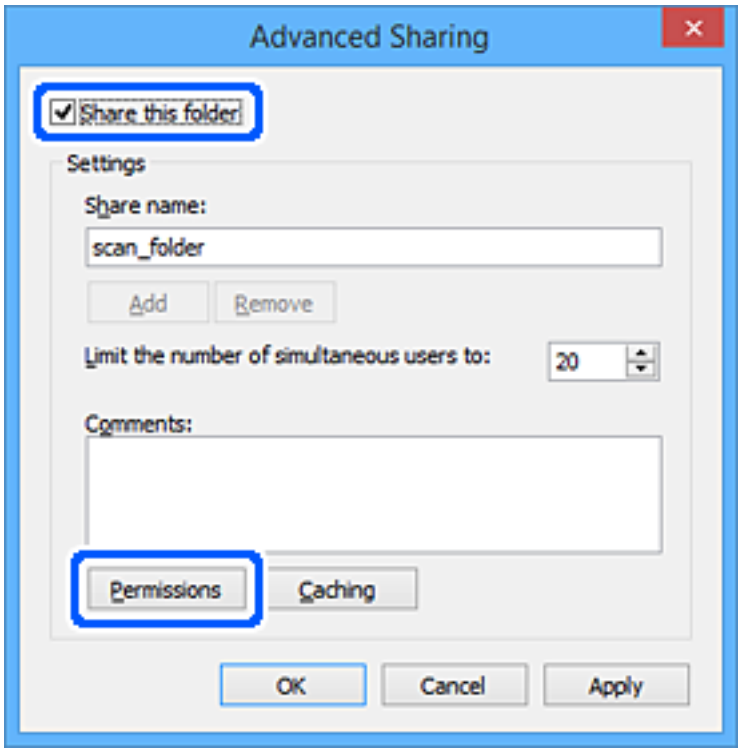
4. Høyreklikk på mappen og velg deretter **Egenskaper**.



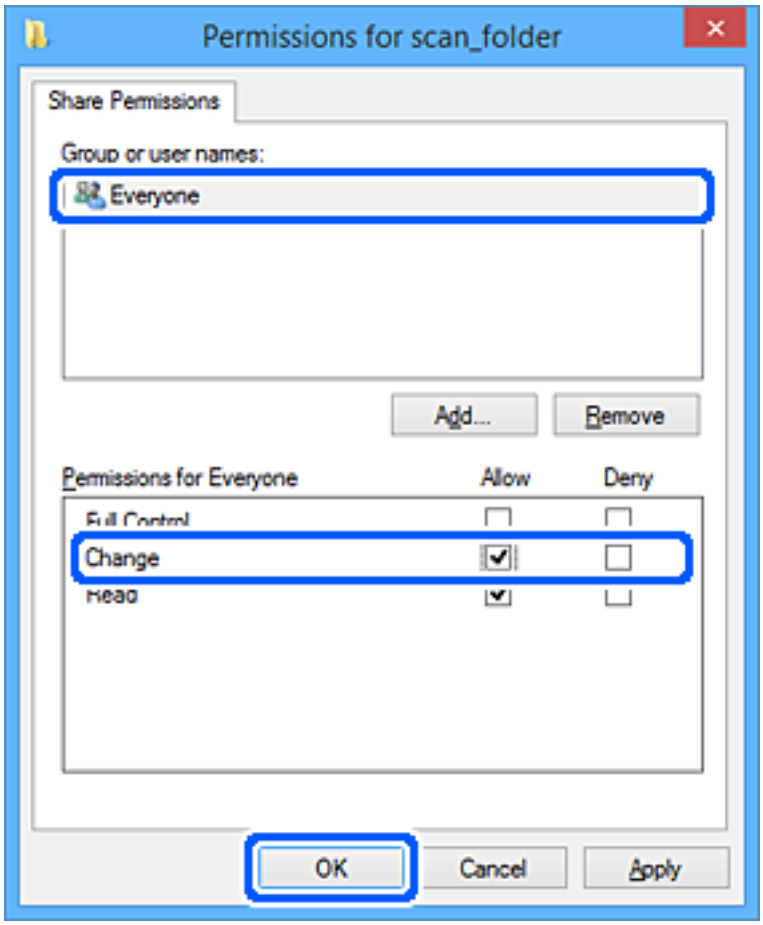
5. Klikk på **Avansert deling** på **Deling**-fanen.



6. Velg **Del denne mappen** og klikk deretter **Tillatelser**.



7. Velg **Alle**-gruppen for **Gruppe- eller brukernavn**, velg **Tillat** på **Endre** og klikk deretter **OK**.



8. Klikk **OK**.

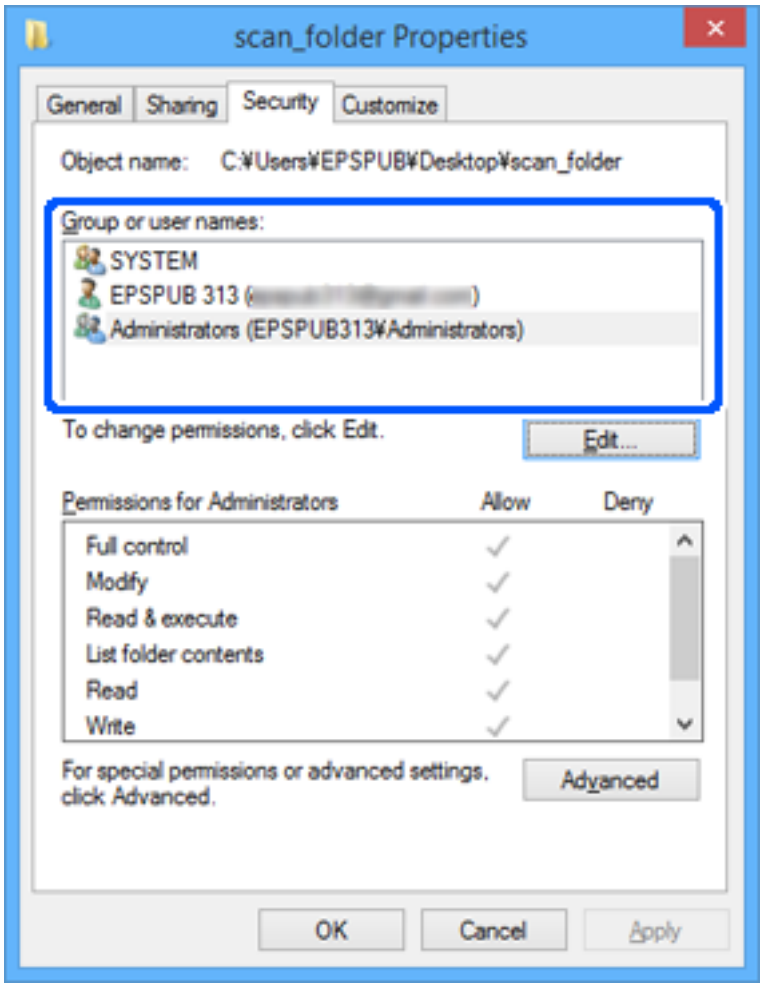
9. Velg **Sikkerhet**-fanen.

10. Kontroller gruppen eller brukeren i **Gruppe- eller brukernavn**.

    Gruppen eller brukeren som vises her kan åpne den delte mappen.

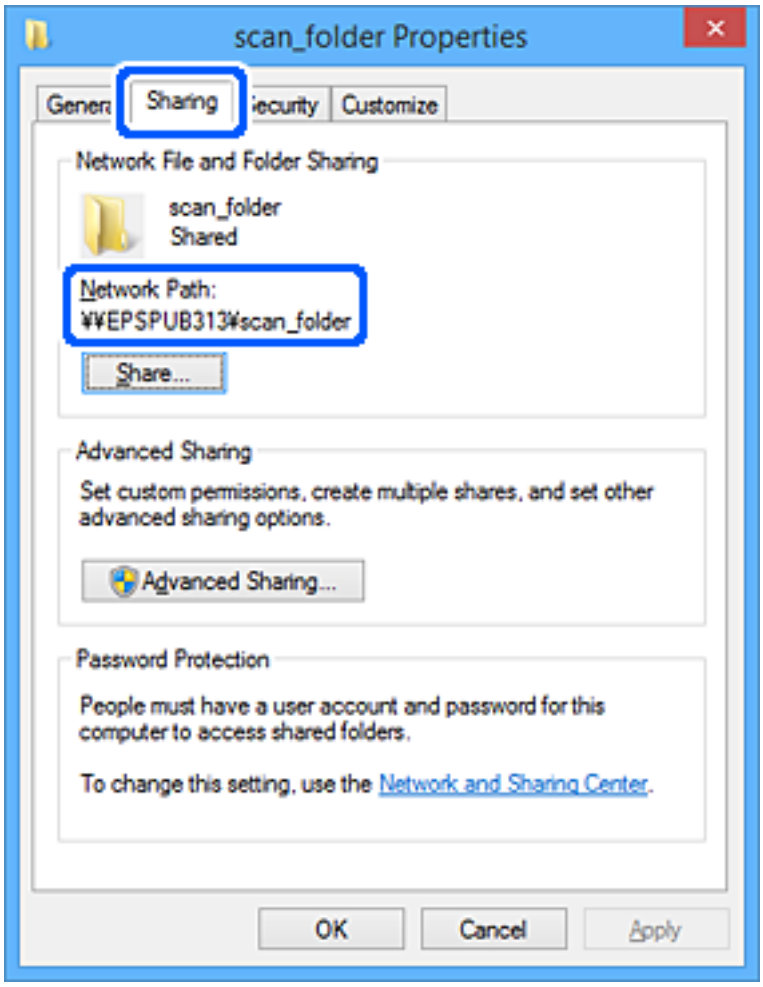
    I dette tilfellet kan brukeren som logger på denne datamaskinen og administratoren åpne den delta mappen.

    Gi tillatelse for tilgang ved behov. Du kan legge den til ved å klikke **Rediger**. Se relatert informasjon for mer informasjon.



11. Velg **Deling**-fanen.

    Nettverksbanen til den delte mappen vises. Den brukes ved registrering til skannerens kontakter. Skriv den ned.



12. Klikk på **OK** eller **Lukk** for å lukke skjermbildet.

    Kontroller om filen kan skrives eller leses på den delte mappen fra datamaskinene til brukere eller grupper med tilgangstillatelse.

Relatert informasjon

➡ "Legge til gruppe eller bruker som gir tilgang" på side 55
➡ "Registrere et mål for kontakter ved hjelp av Web Config" på side 60

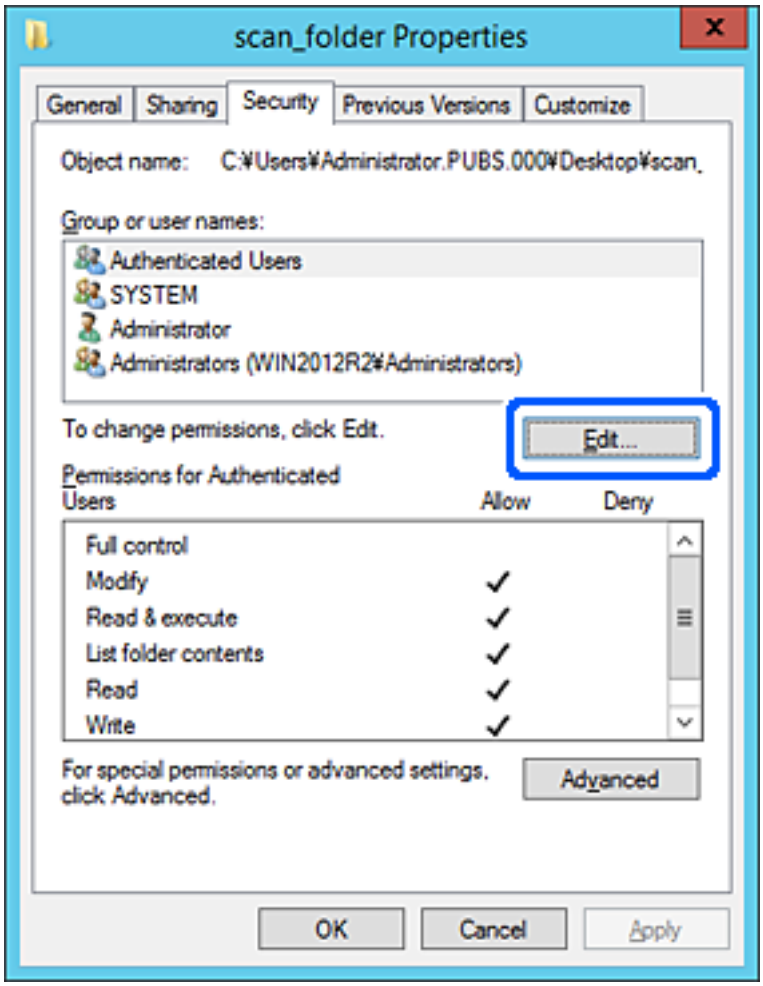
Legge til gruppe eller bruker som gir tilgang

Du kan legge til gruppen eller brukeren som gir tilgang.

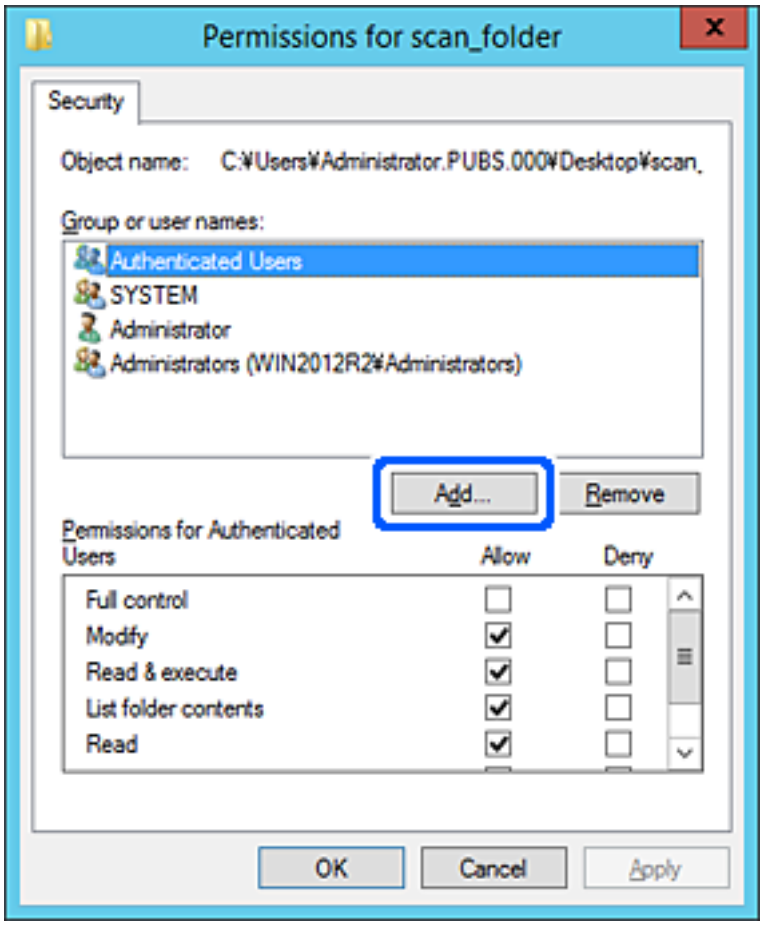
1. Høyreklikk på mappen og velg **Egenskaper**.

2. Velg **Sikkerhet**-fanen.

3. Klikk **Rediger**.



4. Klikk på **Legg til** under **Gruppe- eller brukernavn**.

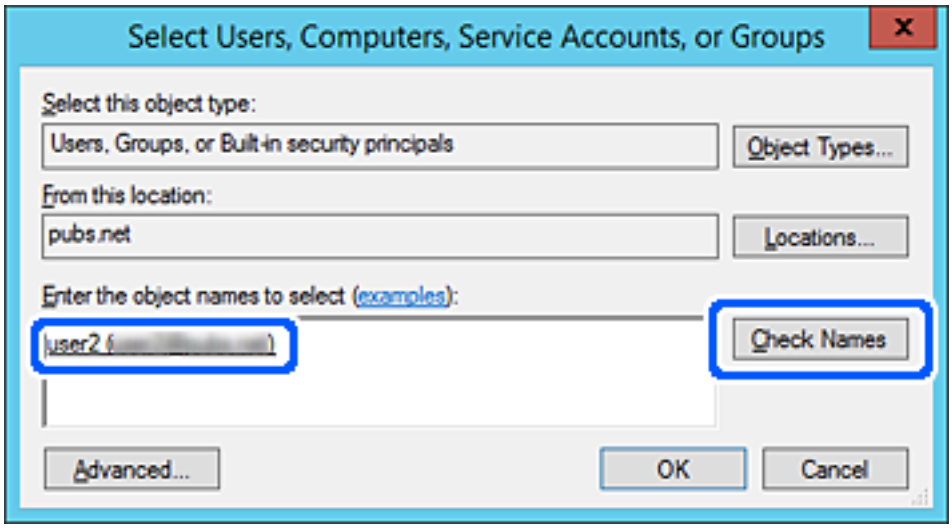


5. Skriv inn gruppe- eller brukernavnet du ønsker å gi tilgang til, og klikk **Kontroller navn**.

   Navnet får en understrek.

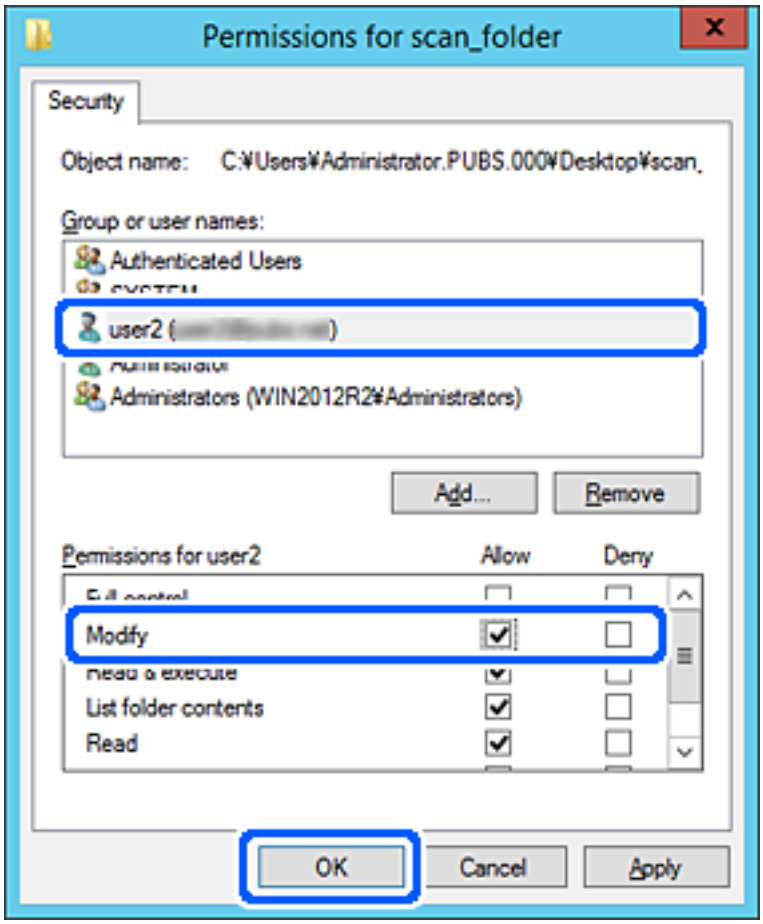
Merknad:
Hvis du ikke kjenner det fullstendige gruppe- eller brukernavnet, skriv inn deler av navnet og klikk ***Kontroller navn****. Gruppe- eller brukernavnene som samsvarer deler av navnet føres opp, og deretter kan du velge det fullstendige navnet fra listen.*

Hvis bare ett navn samsvarer, vises det fullstendige navnet med understrek i ***Skriv inn objektnavnene som skal velges****.*



6. Klikk **OK**.

7. I skjermbildet Tillatelser velger du brukernavnet som er fylt inn i **Gruppe- eller brukernavn**, velger tilgangstillatelse på **Modifiser** og klikker deretter på **OK**.



8. Klikk på **OK** eller **Lukk** for å lukke skjermbildet.

   Kontroller om filen kan skrives eller leses på den delte mappen fra datamaskinene til brukere eller grupper med tilgangstillatelse.

Gjøre kontakter tilgjengelig

Registrering av destinasjoner i skannerens kontaktliste gjør det enkelt å skrive inn destinasjonen når du skanner.

Du kan registrere følgende destinasjonstyper i kontaktlisten. Du kan registrere opptil 300 oppføringer.

Merknad:
Du kan også bruke LDAP-serveren (LDAP-søk) for å skrive inn destinasjonen.

E-post	Destinasjon for e-post. Du må konfigurere innstillingene for e-postserveren på forhånd.
Nettverksmappe	Destinasjon for skannedata. Du må forberede nettverksmappen på forhånd.

Relatert informasjon

➡ "Samarbeid mellom LDAP-server og brukere" på side 66

Sammenlikning av kontaktkonfigurasjon

Det finnes tre verktøy for å konfigurere skannerens kontakter: Web Config, Epson Device Admin og skannerens kontrollpanel. Forskjellene mellom de tre verktøyene vises i tabellen nedenfor.

Funksjoner	Web Config*	Epson Device Admin	Skannerens kontrollpanel
Registrere et mål	✓	✓	✓
Redigere et mål	✓	✓	✓
Legge til en gruppe	✓	✓	✓
Redigere en gruppe	✓	✓	✓
Slette et mål eller grupper	✓	✓	✓
Slette alle mål	✓	✓	–
Importere en fil	✓	✓	–
Eksportere til en fil	✓	✓	–

* Logg på som administrator for å angi innstillinger.

Registrere et mål for kontakter ved hjelp av Web Config

Merknad:
Du kan også registrere kontakter på skannerens kontrollpanel.

1. Gå inn på Web Config og velg **Skann**-fanen > **Kontakter**.
2. Velg et tall som du vil registrere og klikk deretter **Rediger**.
3. Skriv inn **Navn** og **Indeksord**.
4. Velg destinasjonstype som **Type**-alternativet.

   Merknad:
   *Du kan ikke endre **Type**-alternativet etter at registreringen er fullført. Hvis du ønsker å endre type, slett destinasjonen og registrer deg på nytt.*
5. Angi en verdi for hvert element, og klikk deretter **Bruk**.

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34

Destinasjonens innstillingspunkter

Artikler	Innstillinger og forklaring
Vanlige innstillinger	
Navn	Skriv inn et navn til visning i kontakter, med maksimalt 30 tegn i Unicode (UTF-8). Hvis du ikke angir dette, la det stå tomt.
Indeksord	Angi et navn på 30 tegn eller mindre i Unicode (UTF-8) for å søke etter kontaktene på skannerens kontrollpanel. Hvis du ikke angir dette, la det stå tomt.
Type	Velg adressetypen som du vil registrere.
Tilordne hyppig bruk	Velg for å angi den registrerte adressen som en hyppig brukt adresse. Når du angir som en hyppig brukt adresse, vil det vises på den øverste skjermen av skanning, og du kan angi destinasjonen uten å vise kontaktene.
E-post	
E-postadresse	Skriv inn mellom 1 og 255 tegn ved hjelp av A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.
Nettverksmappe (SMB)	
Lagre til	\\«Mappebane» Angi plassering for målmappen, mellom 1 og 253 tegn i Unicode (UTF-8), uten «\ \». Angi nettverksbanen som vises på mappens skjermbilde for egenskaper. Se følgende for mer informasjon om hvordan du angir nettverksbanen. "Eksempel på konfigurasjon for datamaskiner" på side 50
Brukernavn	Skriv inn et brukernavn på maksimalt 30 tegn (UTF-8) for å få tilgang til en nettverksmappe. Unngå å bruke kontrolltegn (0x00 til 0x1F, 0x7F).
Passord	Skriv inn et passord på maksimalt 20 tegn (UTF-8) for å få tilgang til en nettverksmappe. Unngå å bruke kontrolltegn (0x00 til 0x1F, 0x7F).
FTP	
Sikker forbindelse	Velg FTP eller FTPS avhengig av filoverføringsprotokollen FTP-serveren støtter. Velg **FTPS** for å la skanneren kommunisere med sikkerhetstiltak.
Lagre til	Skriv inn servernavnet mellom 1 og 253 tegn i ASCII (0x20–0x7E), utelat «ftp://» eller «ftps://».
Brukernavn	Skriv inn et brukernavn på maksimalt 30 tegn (UTF-8) for å få tilgang til en FTP-server. Unngå å bruke kontrolltegn (0x00 til 0x1F, 0x7F). Hvis serveren tillater anonyme tilkoblinger, skriver du inn et brukernavn som Anonymous og FTP. Hvis du ikke angir dette, la det stå tomt.
Passord	Skriv inn et passord på maksimalt 20 tegn i Unicode (UTF-8) for å få tilgang til en FTP-server. Unngå å bruke kontrolltegn (0x00 til 0x1F, 0x7F). Hvis du ikke angir dette, la det stå tomt.
Tilkoblingsmodus	Velg tilkoblingsmodus fra menyen. Hvis det er angitt en brannmur mellom skanneren og FTP-serveren, velger du **Passivt modus**.
Portnummer	Skriv inn FTP-serverens portnummer (mellom 1 og 65535).

Artikler	Innstillinger og forklaring
Sertifikatvalidering	Sertifikatet for FTP-serveren valideres når dette er aktivert. Dette er tilgjengelig når **FTPS** er valgt for **Sikker forbindelse**. For å konfigurere må du importere CA-sertifikat til skanneren.
SharePoint(WebDAV)	
Sikker forbindelse	Velg HTTP eller HTTPS avhengig av filoverføringsprotokollen serveren støtter. Velg **HTTPS** for å la skanneren kommunisere med sikkerhetstiltak.
Lagre til	Skriv inn servernavnet mellom 1 og 253 tegn i ASCII (0x20–0x7e), utelat «http://» eller «https://».
Brukernavn	Skriv inn et brukernavn på maksimalt 30 tegn (UTF-8) for å få tilgang til en server. Unngå å bruke kontrolltegn (0x00 til 0x1F, 0x7F). Hvis du ikke angir dette, la det stå tomt.
Passord	Skriv inn et passord på maksimalt 20 tegn i Unicode (UTF-8) for å få tilgang til en server. Unngå å bruke kontrolltegn (0x00 til 0x1F, 0x7F). Hvis du ikke angir dette, la det stå tomt.
Sertifikatvalidering	Sertifikatet for serveren valideres når dette er aktivert. Dette er tilgjengelig når **HTTPS** er valgt for **Sikker forbindelse**. For å konfigurere må du importere CA-sertifikat til skanneren.
Proxy-server	Velg om du skal bruke en proxy-server.

Registrere mål som en gruppe med Web Config

Hvis destinasjonstypen er satt til **E-post**, kan du registrere destinasjonen som en gruppe.

1. Gå inn på Web Config og velg **Skann**-fanen > **Kontakter**.
2. Velg et tall som du vil registrere og klikk deretter **Rediger**.
3. Velg en gruppe fra **Type**.
4. Klikk **Velg** for **Kontakt(er) for Gruppe**.
   De tilgjengelige destinasjonene vises.
5. Velg den destinasjonen du vil registrere i gruppen, og klikk deretter **Velg**.
6. Skriv inn et **Navn** og **Indeksord**.
7. Velg om du tilordne den registrerte gruppen til ofte brukte gruppen.
   Merknad:
   Destinasjoner kan registreres til flere grupper.
8. Klikk på **Bruk**.

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34

Sikkerhetskopiere og importere kontakter

Ved hjelp av Web Config eller andre vektøy kan du sikkerhetskopiere og importere kontakter.

For Web Config kan du sikkerhetskopiere kontakter ved å eksportere skanneinnstillingene som inkluderer kontakter. Den eksporterte filen kan redigeres fordi den eksporteres som en binær fil.

Kontaktene overskrives når skanneinnstillingene importeres til skanneren.

For Epson Device Admin kan kun kontakter eksporteres fra enhetens skjermbilde for egenskaper. Hvis du ikke eksporterer sikkerhetsrelaterte elementer, kan du også redigere de eksporterte kontaktene og importere dem, ettersom dette kan lagres som en SYLK- eller CSV-fil.

Importere kontakter med Web Config

Hvis du har en skanner som gir deg mulighet til å sikkerhetskopiere kontakter og som er kompatibel med denne skanneren, kan du enkelt registrere kontakter ved å importere sikkerhetskopifilen.

Merknad:
Hvis du vil ha instruksjoner for hvordan du sikkerhetskopierer skannerens kontakter, kan du se bruksanvisninger som følger med skanneren.

Følg trinnene under for å importere kontakter til denne skanneren.

1. Åpne Web Config og velg **Enhetsadministrasjon**-fanen > **Innstillingsverdi for eksportering og importering** > **Importer**.
2. Velg sikkerhetskopifilen du opprettet i **Fil**, angi passordet og klikk på **Neste**.
3. Velg avmerkingsboksen **Kontakter** og klikk på **Neste**.

Sikkerhetskopiere kontakter med Web Config

Data for kontakter kan gå tapt på grunn av feilfunksjon i skanneren. Vi anbefaler at du tar en sikkerhetskopi av dataen når du oppdaterer den. Epson skal ikke holdes ansvarlig for eventuelle tap av data, for sikkerhetskopiering eller gjenoppretting av data og/eller innstillinger, selv i løpet av en garantiperiode.

Med Web Config, kan du sikkerhetskopiere kontaktdata som er lagret på skanneren til datamaskinen.

1. Gå inn på Web Config, og velg deretter **Enhetsadministrasjon**-fanen > **Innstillingsverdi for eksportering og importering** > **Eksporter**.
2. Velg avmerkingsboksen **Kontakter** under kategorien **Skann**.
3. Skriv inn et passord for å kryptere den eksporterte filen.

   Du trenger passordet for å importere filen. La dette stå tomt hvis du ikke ønsker å kryptere filen.
4. Klikk på **Eksporter**.

Eksportering og grupperegistrering av kontakter med verktøyet

Hvis du bruker Epson Device Admin, kan du velge å kun sikkerhetskopiere kontaktene og redigere de eksporterte filene, og deretter registrere alle samtidig.

Dette er nyttig hvis du ønsker å kun sikkerhetskopiere kontaktene, eller når du bytter ut skanneren og ønsker å overføre kontaktene fra den gamle skanneren til den nye.

Eksportere kontakter

Lagre kontaktinformasjonen til filen.

Du kan redigere filer lagret i SYLK- eller csv-format ved bruk av en regnearksapplikasjon eller et tekstbehandlingsprogram. Du kan registrere alle på en gang etter at informasjonen er slettet eller lagt til.

Informasjonen som inkluderer sikkerhetselementer som passord og personlig informasjon, kan lagres i binærformat med passord. Du kan ikke endre filen. Dette kan brukes som sikkerhetskopifil av informasjonen, inkludert sikkerhetselementene.

1. Start Epson Device Admin.
2. Velg **Devices** på sidestolpen med oppgavemeny.
3. Velg enheten du vil konfigurere fra enhetslisten.
4. Klikk **Device Configuration** på **Home**-fanen på båndmenyen.

   Når et passord har blitt angitt for administratoren, skriver du inn passordet og klikker **OK**.
5. Klikk **Common** > **Contacts**.
6. Velg eksportformat fra **Export** > **Export items**.
   - ❏ All Items

     Eksporter den krypterte binærfilen. Velg når du ønsker å inkludere sikkerhetselementer som passord og personlig informasjon. Du kan ikke endre filen. Hvis du velger den, må du angi passordet. Klikk **Configuration** og angi et passord mellom 8 og 63 tegn i ASCII. Dette passordet kreves når binærfilen importeres.
   - ❏ Items except Security Information

     Eksporter filene i SYLK- eller csv-format. Velg når du ønsker å redigere informasjonen til den eksporterte filen.
7. Klikk på **Export**.
8. Spesifiser stedet hvor filen skal lagres, velg filtype og klikk **Save**.

   Fullføringsmeldingen vises.
9. Klikk på **OK**.

   Kontroller at filen er lagret til det spesifiserte stedet.

Importere kontakter

Importer kontaktinformasjonen fra filen.

Du kan importere filene lagret i SYLK- eller CSV-format, eller den sikkerhetskopierte binærfilen som er inkludert i sikkerhetselementene.

1. Start Epson Device Admin.
2. Velg **Devices** på sidestolpen med oppgavemeny.
3. Velg enheten du vil konfigurere fra enhetslisten.
4. Klikk **Device Configuration** på **Home**-fanen på båndmenyen.

   Når et passord har blitt angitt for administratoren, skriver du inn passordet og klikker **OK**.
5. Klikk **Common** > **Contacts**.
6. Klikk **Browse** på **Import**.
7. Velg filen du vil importere og klikk deretter **Open**.

   Når du velger binærfilen, skal du skrive inn passordet du skrev inn da du eksporterte filen **Password**.
8. Klikk på **Import**.

   Bekreftelsesskjermbildet vises.
9. Klikk på **OK**.

   Valideringsresultatet vises.

   ❏ Edit the information read

   Klikk når du ønsker å endre informasjonen individuelt.

   ❏ Read more file

   Klikk når du ønsker å importere flere filer.
10. Klikk **Import**, og klikk deretter **OK** på skjermbildet for fullføring av importering.

    Gå tilbake til skjermbildet for enhetens egenskaper.
11. Klikk på **Transmit**.
12. Klikk **OK** på bekreftelsesmeldingen.

    Innstillingene sendes til skanneren.
13. Klikk **OK** på skjermbildet for fullført sending.

    Skannerinformasjonen er oppdatert.

    Åpne kontaktene fra Web Config eller skannerens kontrollpanel, og kontroller deretter at kontakten er oppdatert.

Samarbeid mellom LDAP-server og brukere

Ved samarbeid med LDAP-serveren, kan du bruke adresseinformasjonen registrert på LDAP-serveren som destinasjon for e-post.

Konfigurere LDAP-serveren

For å bruker informasjonen til LDAP-serveren, må den registreres på skanneren.

1. Gå inn på Web Config og velg **Nettverk**-fanen > **LDAP-server** > **Grunnleggende**.
2. Angi en verdi for hvert element.
3. Velg **OK**.

   Innstillingene du har valgt, vises.

Innstillingselementer for LDAP-server

Artikler	Innstillinger og forklaring
Bruk LDAP-server	Velg **Bruk** eller **Ikke bruk**.
LDAP-serveradresse	Skriv inn adressen til LDAP-serveren. Skriv inn mellom 1 og 255 tegn i enten IPv4-, IPv6- eller FQDN-format. Med FQDN-formatet kan du bruke alfanumeriske tegn i ASCII (0x20–0x7E) og «-», bortsett fra i starten og slutten av adressen.
LDAP-serverportnummer	Skriv inn LDAP-serverens portnummer mellom 1 og 65 535.
Sikker forbindelse	Angi godkjenningsmetoden når skanneren får tilgang til LDAP-serveren.
Sertifikatvalidering	Når dette er aktivert, er LDAP-serverens sertifikat validert. Vi anbefaler at dette settes til **Aktiver**. For å konfigurere må **CA-sertifikat** være importert til skanneren.
Tidsavbrudd for søk (sek)	Angi tiden for å søke før tidsavbrudd mellom 5 og 300.
Godkjenningsmetode	Velg en av metodene. Hvis du velger **Kerberos-autentisering**, velger du **Kerberos-innstillinger** for å angi innstillinger for Kerberos. For å gjennomføre Kerberos-autentisering, kreves følgende omgivelser. ❏ Skanneren og DNS-serveren kan kommunisere. ❏ Klokkeslettet til skanneren, KDC-serveren og serveren som kreves for godkjenning (LDAP-server, SMTP-server, filserver) er synkroniserte. ❏ Når tjenesteserveren er tilordnet som IP-adressen, er tjenesteserverens FQDN registrert på DNS-serverens reverserte oppslagssone.
Kerberos-område som skal brukes	Hvis du velger **Kerberos-autentisering** for **Godkjenningsmetode**, velger du Kerberos-riket som du vil bruke.
Administrator-DN / Brukernavn	Skriv inn brukernavnet for LDAP-serveren på 128 tegn eller mindre i Unicode (UTF-8). Du kan ikke bruke kontrolltegn, som 0x00–0x1F og 0x7F. Denne innstillingen brukes ikke når **Anonym autentisering** er valgt som **Godkjenningsmetode**. Hvis du ikke angir dette, la det stå tomt.

Artikler	Innstillinger og forklaring
Passord	Skriv inn passordet for LDAP-servergodkjenning på 128 tegn eller mindre i Unicode (UTF-8). Du kan ikke bruke kontrolltegn, som 0x00–0x1F og 0x7F. Denne innstillingen brukes ikke når **Anonym autentisering** er valgt som **Godkjenningsmetode**. Hvis du ikke angir dette, la det stå tomt.

Kerberos-innstillinger

Hvis du velger **Kerberos-autentisering** som **Godkjenningsmetode** for **LDAP-server** > **Grunnleggende**, foretar du følgende Kerberos-innstillinger fra **Nettverk**-fanen > **Kerberos-innstillinger**. Du kan registrere opptil 10 innstillinger for Kerberos-innstillingene.

Artikler	Innstillinger og forklaring
Område (domene)	Skriv inn området for Kerberos-godkjenning med maksimalt 255 i ASCII (0x20–0x7E). Hvis du ikke registrerer dette, la det stå tomt.
KDC-adresse	Skriv inn adressen til Kerberos-autentiseringsserveren. Skriv inn 255 tegn eller mindre i enten IPv4, IPv6 eller FQDN-format. Hvis du ikke registrerer dette, la det stå tomt.
Portnummer (Kerberos)	Skriv inn Kerberos-serverens portnummer mellom 1 og 65535.

Konfigurere søkeinnstillinger for LDAP-serveren

Når du konfigurerer søkeinnstillingene, kan du bruke e-postadressen registrert på LDAP-serveren.

1. Gå inn på Web Config og velg **Nettverk**-fanen > **LDAP-server** > **Søkeinnstillinger**.
2. Angi en verdi for hvert element.
3. Klikk **OK** for å vise innstillingsresultatet.

   Innstillingene du har valgt, vises.

Innstillingselementer for søk på LDAP-server

Artikler	Innstillinger og forklaring
Søkebase (unikt navn)	Hvis du vil søke på et tilfeldig domene, angir du domenenavnet til LDAP-serveren. Skriv inn mellom 0 og 128 tegn i Unicode (UTF-8). Hvis du ikke søker etter en vilkårlig attributt, la dette stå tomt. Eksempel på lokal serverkatalog: dc=server,dc=local
Antall søkeoppføringer	Angi antall søkeoppføringer mellom 5 og 500. Det angitte antallet av søkte oppføringer lagres og vises midlertidig. Selv om antall søkeoppføringer er over det angitte antallet og det vises en feilmelding, kan søket bli fullført.
Brukernavnegenskap	Angi attributtnavn som skal vises når du søker etter brukernavn. Skriv inn mellom 1 og 255 tegn i Unicode (UTF-8). Det første tegnet må være a–z eller A–Z. Eksempel: cn, uid

Artikler	Innstillinger og forklaring
Brukernavnvisningsegenskap	Angi attributtnavn som skal vises som brukernavnet. Skriv inn mellom 0 og 255 tegn i Unicode (UTF-8). Det første tegnet må være a–z eller A–Z. Eksempel: cn, sn
E-postadresseegenskap	Angi attributtnavn som skal vises når du søker etter e-postadresser. Skriv inn en kombinasjon av 1 og 255 tegn ved hjelp av A–Z, a–z, 0–9 og -. Det første tegnet må være a–z eller A–Z. Eksempel: post
Vilkårlig egenskap 1 - Vilkårlig egenskap 4	Du kan angi andre vilkårlige attributter for å søke etter. Skriv inn mellom 0 og 255 tegn i Unicode (UTF-8). Det første tegnet bør være a–z eller A–Z. La dette feltet stå tomt hvis du ikke vil søke etter tilfeldige attributter. Eksempel: o, ou

Kontrollere LDAP-servertilkoblingen

Utfører tilkoblingstesten til LDAP-serveren ved hjelp av parameteren angitt i **LDAP-server** > **Søkeinnstillinger**.

1. Gå inn på Web Config og velg **Nettverk**-fanen > **LDAP-server** > **Tilkoblingstest**.
2. Velg **Start**.

   Tilkoblingstest startet. Etter testen vil kontrollrapporten vises.

Testreferanser for LDAP-servertilkobling

Meldinger	Forklaring
Tilkoblingstesten var vellykket.	Denne meldingen vises når tilkoblingen til serveren er vellykket.
Tilkoblingstesten mislyktes. Kontroller innstillingene.	Denne meldingen vises av følgende årsaker: ❏ Det er feil adresse eller portnummer til LDAP-serveren. ❏ Det oppstod et tidsavbrudd. ❏ **Ikke bruk** er valgt som **Bruk LDAP-server**. ❏ Hvis **Kerberos-autentisering** er valgt som **Godkjenningsmetode**, innstillinger som **Område (domene)**, **KDC-adresse** og **Portnummer (Kerberos)** er feil.
Tilkoblingstesten mislyktes. Kontroller dato og klokkeslett på produktet eller serveren.	Denne meldingen vises når tilkoblingen mislykkes fordi tidsinnstillingene for skanneren og LDAP-serveren ikke samsvarer.
Autentisering mislyktes. Kontroller innstillingene.	Denne meldingen vises av følgende årsaker: ❏ **Brukernavn** og/eller **Passord** er feil. ❏ Hvis **Kerberos-autentisering** er valgt som **Godkjenningsmetode** kan ikke klokkeslett/dato konfigureres.
Får ikke tilgang til produktet før behandlingen er fullført.	Denne meldingen vises når skanneren er opptatt.

Bruke Document Capture Pro Server

Ved å bruke Document Capture Pro Server, kan du administrere sorteringmetode, lagringsformat og destinasjon for videresendte skannede dokumenter fra skannerens kontrollpanel. Du kan ringe opp og utføre en jobb som tidligere har vært registrert på serveren fra skannerens kontrollpanel.

Installer den på serverdatamaskinen.

For mer informasjon om Document Capture Pro Server, kontakt ditt lokale Epson-kontor.

Innstilling av servermodus

For å bruke Document Capture Pro Server, gjør du følgende innstillinger.

1. Gå inn på Web Config og velg **Skann**-fanen > **Document Capture Pro**.
2. Velg **Servermodus** ved **Modus**.
3. Angi adressen for skriveren med Document Capture Pro Server installert som **Serveradresse**.

   Skriv inn mellom 2 og 255 tegn i enten IPv4-, IPv6-, vertsnavn- eller FQDN-format. Med FQDN-format kan du bruke alfanumeriske tegn i ASCII (0x20–0x7E) og «-», bortsett fra i starten og slutten av adressen.
4. Klikk på **OK**.

   Nettverksforbindelsen gjenopprettes og innstillingene aktiveres.

Konfigurere AirPrint

Åpne Web Config, velg fanen **Nettverk** og velg deretter **AirPrint-innstilling**.

Artikler	Forklaring
Bonjour servicenavn	Angi navnet på en Bonjour-tjeneste med ASCII-tekst (0x20–0x7E) og opptil 41 tegn.
Bonjour-plassering	Angi en beskrivelse av plasseringen til skanneren med Unicode-tekst (UTF-8) og inntil 127 byte.
Wide-Area Bonjour	Angi hvorvidt Wide-Area Bonjour skal brukes. Hvis du bruker det, må skanneren være registrert på DNS-serveren for å kunne søke etter skanneren over segmentet.
Aktiver AirPrint	Bonjour og AirPrint (skannetjeneste) er aktivert.

Problemer ved forberedelse av nettverksskanning

Hint for å løse problemer

❏ Kontrollere feilmeldingene

Når det har oppstått et problem, må du først kontrollere om det står noen meldinger på skannerens kontrollpanel eller driverskjerm. Hvis du har angitt varsling på e-post når hendelsene oppstår, kan du raskt finne statusen.

❏ Kontrollere kommunikasjonsstatusen

Kontroller kommunikasjonsstatusen til server- eller klientdatamaskinen ved hjelp av kommandoer som ping og ipconfig.

❏ Tilkoblingstest

Utfør tilkoblingstesten fra skanneren for å kontrollere tilkoblingen mellom skanneren og e-postserveren. Kontroller også tilkoblingen fra klientdatamaskinen til serveren for å kontrollere kommunikasjonsstatusen.

❏ Initialisere innstillingene

Hvis innstillingene og kommunikasjonsstatusen ikke viser noe problem, kan problemet kanskje løses ved å deaktivere eller initialisere skannerens nettverksinnstillinger, og deretter konfigurere disse på nytt.

Får ikke tilgang til Web Config

IP-adressen er ikke tilordnet til skanneren.

Løsninger

En gyldig IP-adresse kan ikke tilordnes til skanneren. Konfigurer IP-adressen ved hjelp av skannerens kontrollpanel. Du kan bekrefte gjeldende innstillingsinformasjon fra skannerens kontrollpanel.

Nettleseren støtter ikke krypteringsstyrken for SSL/TLS.

Løsninger

SSL/TLS har Krypteringsstyrke. Du kan åpne Web Config ved hjelp av en nettleser som støtter bulkkryptering, som angitt under. Kontroller at du bruker en støttet nettleser.

❏ 80 bit: AES256/AES128/3DES

❏ 112 bit: AES256/AES128/3DES

❏ 128 bit: AES256/AES128

❏ 192 bit: AES256

❏ 256 bit: AES256

CA-signert sertifikat er utløpt.

Løsninger

Hvis det er et problem med sertifikatets utløpsdato, vises «Sertifikatet er utløpt» ved tilkobling til Web Config med SSL/TLS-kommunikasjon (https). Hvis meldingen vises før utløpsdatoen, kontrollerer du at skannerens dato er riktig konfigurert.

Sertifikatets og skannerens fellesnavn samsvarer ikke.

Løsninger

Hvis sertifikatets og skannerens fellesnavn ikke samsvarer, vises meldingen «Navnet på sikkerhetssertifikatet samsvarer ikke···» når Web Config åpnes ved hjelp av SSL/TLS-kommunikasjon (https). Dette skjer fordi følgende IP-adresser ikke samsvarer.

❏ Skannerens IP-adresse som er angitt for fellesnavn for å opprette et Selvsignert sertifikat eller CSR

❏ IP-adressen som er angitt til nettleseren når Web Config kjøres

Oppdater sertifikatet for Selvsignert sertifikat.

Ta sertifikatet igjen for skanneren for CA-signert sertifikat.

Innstillingen av lokal adresse for proxy-serveren er ikke angitt til nettleseren.

Løsninger

Når skanneren er innstilt til å bruke en proxyserver, må nettleseren konfigureres til å ikke koble til den lokale adressen via proxyserveren.

❏ Windows:

Velg **Kontrollpanel** > **Nettverk og Internett** > **Alternativer for Internett** > **Tilkoblinger** > **LAN-innstillinger** > **Proxy-server**, og deretter konfigurerer du at proxy-serveren ikke skal brukes for LAN (lokale adresser).

❏ Mac OS:

Velg **Systemvalg** > **Nettverk** > **Avansert** > **Proxyer**, og deretter registrerer du den lokale adressen for **Ignorer proxyinnstillinger for disse vertene og domenene**.

Eksempel:

192.168.1.*: Lokal adresse 192.168.1.XXX, nettverksmaske 255.255.255.0

192.168.*.*: Lokal adresse 192.168.XXX.XXX, nettverksmaske 255.255.0.0

DHCP er deaktivert i datamaskinens innstillinger.

Løsninger

Hvis DHCP for å hente en IP-adresse deaktiveres automatisk på datamaskinen, får du ikke tilgang til Web Config. Aktiver DHCP.

Eksempel for Windows 10:

Åpne kontrollpanelet og klikk **Nettverk og Internett** > **Nettverks- og delingssenter** > **Endre adapterinnstillinger**. Åpne Egenskaper-skjermbildet for tilkoblingen du bruker, og åpne deretter egenskaper-skjermbildet for **Internettprotokoll versjon 4 (TCP/IPv4)** eller **Internettprotokoll versjon 6 (TCP/IPv6)**. Kontroller at **Hent en IP-adresse automatisk** er valgt på skjermbildet som vises.

Tilpasse kontrollpanelskjermen

Registrere Forhåndsinns

Du kan registrere ofte brukte skanneinnstillinger som **Forhåndsinns**. Du kan registrere opp til 48 forhåndsinnstillinger.

Merknad:

❏ *Du kan registrere nåværende innstillinger ved å velge* ☆ *på skjermbildet for start av skanning.*

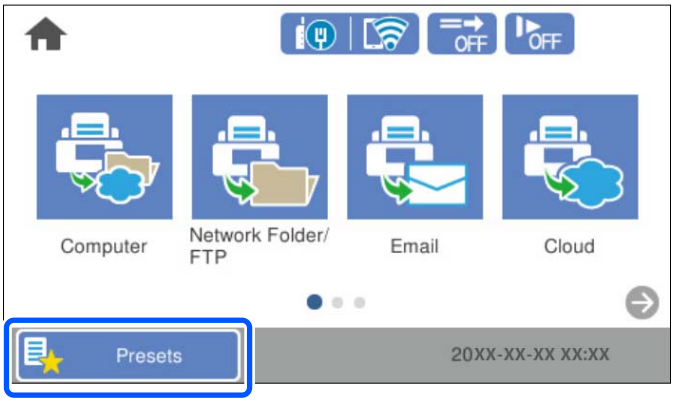
❏ *Du kan også registrere* ***Forhåndsinnstillinger*** *i Web Config.*

Velg ***Skann****-fanen >* ***Forhåndsinnstillinger****.*

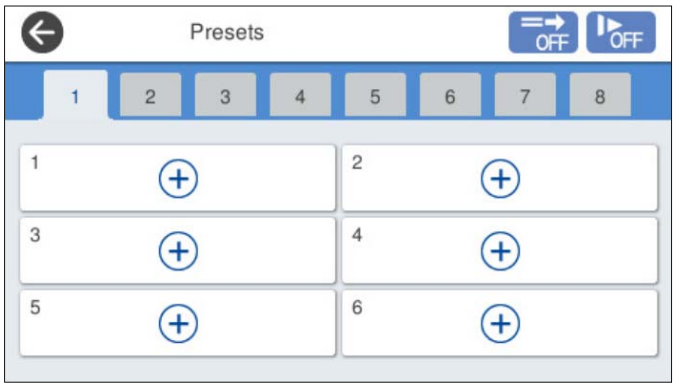
❏ *Hvis du velger* ***Skann til datamaskin*** *når du registrerer deg, kan du registrere jobben du opprettet i Document Capture Pro som* ***Forhåndsinnstillinger****. Dette er kun tilgjengelig for datamaskiner som er koblet sammen over et nettverk. Registrer jobben i Document Capture Pro på forhånd.*

❏ *Hvis autentifikasjonsfunksjonen er aktivert, kan kun administratoren registrere* ***Forhåndsinnstillinger****.*

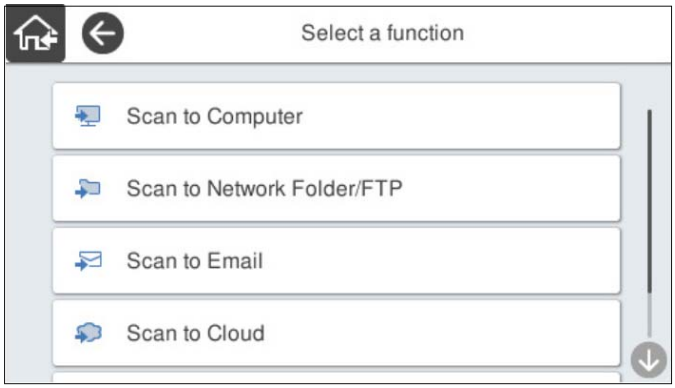
1. Velg **Forhåndsinns** på startskjermen til skannerens kontrollpanel.



2. Velg ⊕.



3. Velg menyen du vil bruke for å registrere en forhåndsinnstilling.



4. Angi hvert element og velg deretter ☆+.

Merknad:
*Når du velger **Skann til datamaskin**, velger du datamaskinen hvor Document Capture Pro er installert. Deretter velger du en registrert jobb. Dette er kun tilgjengelig for datamaskiner som er koblet sammen over et nettverk.*

5. Utfør forhåndsinnstillingene.

- ❏ **Navn**: Angi navnet.
- ❏ **Angi Ikon**: Angi bildet og fargen til bildet som skal vises.
- ❏ **Hurtigsende-innstilling**: Begynner å skanne umiddelbart uten bekreftelse når forhåndsinnstillingen velges.

  Når du bruker Document Capture Pro Server, selv om du angir programvaren for å bekrefte innholdet til en jobb før du skanner, prioriteres **Hurtigsende-innstilling** på skannerens forhåndsinnstillinger over programvaren.
- ❏ **Innhold**: Kontrollerer skanneinnstillingene.

6. Velg **OK**.

Menyalternativer for Forhåndsinns

Du kan endre forhåndsinnstillinger ved å velge › i hver forhåndsinnstilling.

Endre navn:

Endrer navnet til forhåndsinnstillingen.

Endre Ikon:

Endrer ikonbildet og fargen til forhåndsinnstillingen.

Hurtigsende-innstilling:

Begynner å skanne umiddelbart uten bekreftelse når forhåndsinnstillingen velges.

Endre posisjon:

Endre visningsrekkefølgen til forhåndsinnstillingene.

Slett:

Sletter forhåndsinnstillingen.

Legg til eller fjern Ikon på Hjem:

Legger til eller fjerner ikonet til forhåndsinnstillingen fra startskjermen.

Bekreft detaljer:

Se innstillingene til en forhåndsinnstilling. Du kan laste inn forhåndsvisningen ved å velge **Bruk denne innstillingen**.

Redigere startskjermen til kontrollpanelet

Du kan tilpasse startskjermen ved å velge **Innst.** > **Rediger Startskjerm** på skannerens kontrollpanel.

- ❏ Layout: Endrer visningsmetoden til menyikonene.
  "Endre Layout på startskjermen" på side 75
- ❏ Legg til ikon: Legger til ikoner i **Forhåndsinns**-innstillingene du har angitt, eller gjenoppretter ikoner som har blitt fjernet fra skjermen.
  "Legg til ikon" på side 76
- ❏ Fjern ikon: Fjerner ikoner fra startskjermen.
  "Fjern ikon" på side 77
- ❏ Flytt ikon: Endrer visningsrekkefølgen til ikonene.
  "Flytt ikon" på side 78
- ❏ Gjenopprett standard ikonvisning: Gjenoppretter standard skjerminnstillinger for startskjermen.
- ❏ Bakgrunn : Endre bakgrunnsfargen til startskjermen.

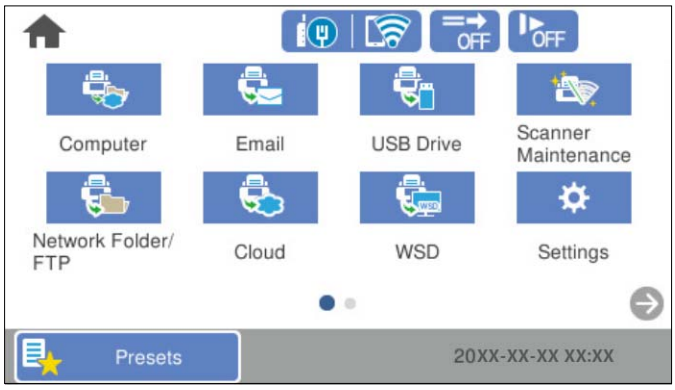
Endre Layout på startskjermen

1. Velg **Innst.** > **Rediger Startskjerm** > **Layout** på skannerens kontrollpanel.

2. Velg **Linje** eller **Matrise**.

   Linje:

   Matrise:



3. Velg for å gå tilbake og kontrollere startskjermen.

Legg til ikon

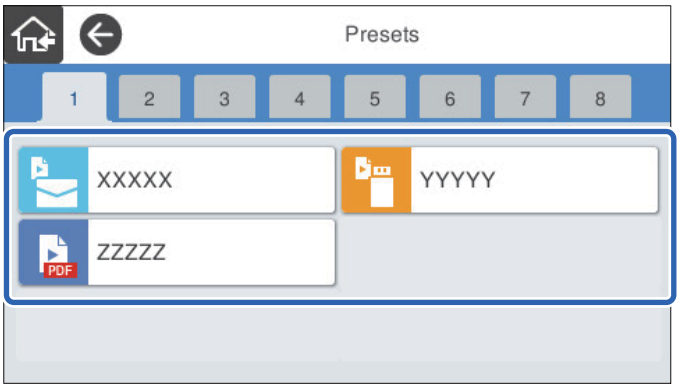
1. Velg **Innst.** > **Rediger Startskjerm** > **Legg til ikon** på skannerens kontrollpanel.

2. Velg **Funksjon** eller **Forhåndsinns**.

   ❏ Funksjon: Viser standardfunksjonene som vises for startskjermen.

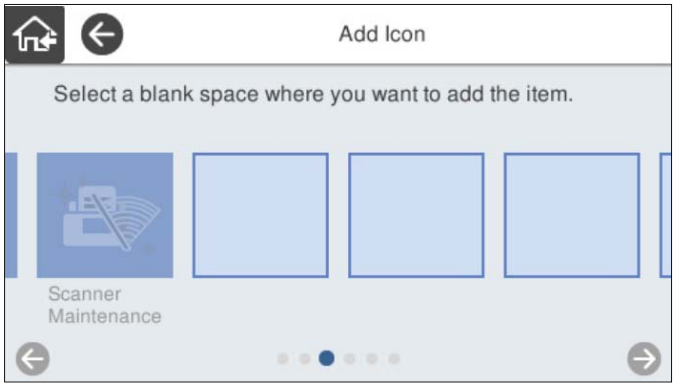
❏ Forhåndsinns: Viser registrerte forhåndsinnstillinger.

3. Velg elementet du vil legge til startskjermen.



4. Velg tomrommet hvor du vil legge til elementet.

   Hvis du vil legge til flere ikoner gjentar du trinn 3 til 4.

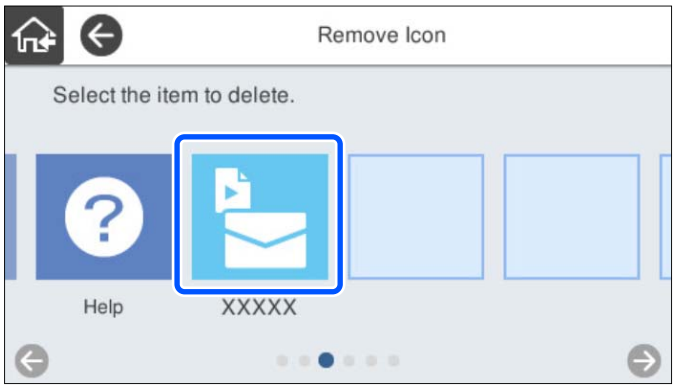


5. Velg for å gå tilbake og kontrollere startskjermen.

Fjern ikon

1. Velg **Innst.** > **Rediger Startskjerm** > **Fjern ikon** på skannerens kontrollpanel.

2. Velg ikonet du vil fjerne.



3. Velg **Ja** for å avslutte.

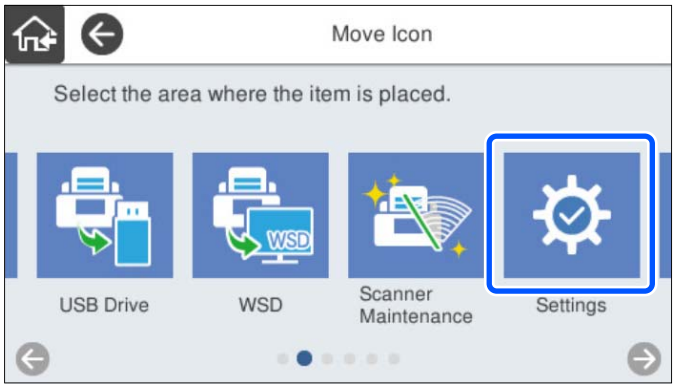
   Hvis du vil fjerne flere ikoner gjentar du prosedyre 2 til 3.

4. Velg for å gå tilbake og kontrollere startskjermen.

Flytt ikon

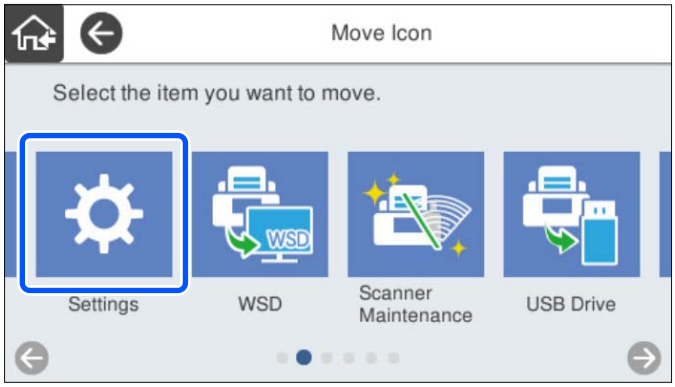
1. Velg **Innst.** > **Rediger Startskjerm** > **Flytt ikon** på skannerens kontrollpanel.

2. Velg ikonet du vil flytte.



3. Velg destinasjonsrammen.

   Hvis et annet ikon allerede befinner seg i destinasjonsrammen vil det nye ikonet erstatte det gamle.



4. Velg for å gå tilbake og kontrollere startskjermen.

Grunnleggende sikkerhetsinnstillinger

Introduksjon til de sikkerhetsfunksjonene for produktet

Dette avsnittet introduserer sikkerhetsfunksjonen til Epson-enhetene.

Funksjonsnavn	Funksjonstype	Hva skal stilles inn	Hva skal forebygges
Konfigurasjon av administratorpassord	Låser systeminnstillinger slik som tilkoblingskonfigurasjon for nettverk eller USB.	En administrator angir et passord for enheten. Du kan angi eller endre fra både Web Config og skannerens kontrollpanel.	Unngå ulovlig lesing og endring av informasjon som er lagret på enheten, slik som ID, passord, nettverksinnstillinger og så videre. Reduser også et bredt spekter av sikkerhetsrisikoer som lekkasje av informasjon til nettverksmiljøet eller sikkerhetspolitikk.
Konfigurasjon for eksternt grensesnitt	Kontrollerer grensesnittet som kobler seg til enheten.	Aktiver eller deaktiver USB-tilkobling med datamaskinen.	USB-tilkobling til datamaskin: Forhindrer uautorisert bruk av enheten ved å forby skanning uten å gå via nettverket.

Relatert informasjon

➡ "Konfigurere administratorpassordet" på side 81
➡ "Deaktivere eksternt grensesnitt" på side 87

Administratorinnstillinger

Konfigurere administratorpassordet

Når du angir et administratorpassord, kan du forhindre at brukere endrer innstillinger for systembehandling. Standardverdiene er angitt ved kjøp. Endre dem etter behov.

Merknad:
Følgende gir standardverdier for administratorinformasjon.

❏ *Brukernavn (brukes kun for Web Config): ingen (tomt)*

❏ *Passord: serienummeret til skanneren*

Du finner serienummeret på etiketten på baksiden av skanneren.

Du kan endre administratorpassordet ved å bruke enten Web Config, skannerens kontrollpanel eller Epson Device Admin. Når du bruker Epson Device Admin, bør du bruke Epson Device Admin-veiledingen.

Endre administratorpassordet ved å bruke Web Config

Endre administratorpassordet i Web Config.

1. Gå inn på Web Config og velg **Produktsikkerhet**-fanen > **Endre administratorpassord**.

2. Angi den nødvendige informasjonen i **Nåværende passord**, **Brukernavn**, **Nytt passord**, og **Bekreft nytt passord**.

   Skriv inn minst ett tegn for det nye passordet.

   Merknad:
   Følgende gir standardverdier for administratorinformasjon.

   ❏ *Brukernavn: ingen (tomt)*

   ❏ *Passord: serienummeret til skanneren*

   Du finner serienummeret på etiketten på baksiden av skanneren.

   > ***Forsiktighetsregel:***
   > *Husk administratorpassordet du angir. Du kan ikke tilbakestille passordet hvis du glemmer det, og du må be om hjelp av service-personalet.*

3. Velg **OK**.

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34

Endre administratorpassord fra kontrollpanelet

Du kan endre administratorpassord fra skannerens kontrollpanel.

1. Velg **Innst.** på skannerens kontrollpanel.

2. Velg **Systemadministrasjon** > **Administratorinnstillinger**.

3. Velg **Adminpassord** > **Endre**.

4. Angi nåværende passord.

   Merknad:
   Innstillingene ved kjøp (standardverdi) for administratorpassordet er serienummeret til skanneren.

   Du finner serienummeret på etiketten på baksiden av skanneren.

5. Skriv inn det nye passordet.

   Skriv inn minst ett tegn.

   > ***Forsiktighetsregel:***
   > *Husk administratorpassordet du angir. Du kan ikke tilbakestille passordet hvis du glemmer det, og du må be om hjelp av service-personalet.*

6. Skriv inn det nye passordet på nytt for å bekrefte det.

Det vises en fullføringsmelding.

Bruke Låsinnstilling for kontrollpanelet

Du kan bruke Låsinnstilling til å låse kontrollpanelet og hindre at brukere endrer elementer tilknyttet systeminnstillingene.

Merknad:
Hvis du aktiverer Godkjenningsinnstillinger på skanneren, Låsinnstilling er det også aktivert for kontrollpanelet. Kontrollpanelet kan ikke låses opp når Godkjenningsinnstillinger er aktivert.

Selv om du deaktiverer Godkjenningsinnstillinger, forblir Låsinnstilling aktivert. Hvis du vil deaktivere det, kan du stille dette inn fra kontrollpanelet eller Web Config.

Konfigurere Låsinnstilling fra kontrollpanelet

1. Hvis du vil avbryte **Låsinnstilling** når det er aktivert, kan du trykke på øverst til høyre på Hjem-skjermen for å logge inn som administrator.

   vises ikke når **Låsinnstilling** er deaktivert. Hvis du vil aktivere denne innstillingen, går du videre til neste trinn.

2. Velg **Innst.**.

3. Velg **Systemadministrasjon** > **Administratorinnstillinger**.

4. Velg **På** eller **Av** som **Låsinnstilling**.

Angi Låsinnstilling fra Web Config

1. Velg **Enhetsadministrasjon**-fanen > **Kontrollpanel**.

2. Velg **På** eller **Av** for **Panellås**.

3. Klikk på **OK**.

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34

Låsinnstilling-elementer i Innst.-menyen

Dette er en liste over elementer som låses i **Innst.**-menyen på kontrollpanelet gjennom Låsinnstilling.

✓: skal låses.

- : skal ikke låses.

Innst.-meny		Låsinnstilling
Basisinnstillinger		-
	LCD-lysstyrke	-
	Lyder	-
	Innsovingstid	✓
	Strøm av-tidtaker	✓
	Innstillinger dato/kl.	✓
	Språk/Language	✓/-*
	Tastatur (Denne funksjonen kan være utilgjengelig avhengig av region.)	-
	Tidsavbrudd for handling	✓
	PC-tilkobling via USB	✓
	Direkte strøm på	✓
Skannerinnstillinger		-
	Sakte	-
	Dobbelmatestopp-timing	✓
	DFDS-funksjon	-
	Papirbeskyttelse	✓
	Oppdagelse av skitt på glasset	✓
	Ultrasonisk registr. av dobbeltmating	✓
	Tidsavbrudd for Modus for automatisk mating	✓
	Bekreft mottaker	✓
Rediger Startskjerm		✓
	Layout	✓
	Legg til ikon	✓
	Fjern ikon	✓
	Flytt ikon	✓
	Gjenopprett standard ikonvisning	✓
	Bakgrunn	✓
Brukerinnstillinger		✓

Innst.-meny		Låsinnstilling
	Nettverksmapp/FTP	✓
	E-post	✓
	Nettsky	✓
	USB-stasjon	✓
Nettverksinnstillinger		✓
	Wi-Fi-oppsett	✓
	Oppsett av kablet LAN	✓
	Nettverkstatus	✓
	Avansert	✓
Web-tjenesteinnstillinger		✓
	Epson Connect-tjenester	✓
Document Capture Pro		-
	Endre innstillinger	✓
Kontaktadministrasjon		-
	Registrer/Slett	✓/-*
	Hyppig	-
	Vis alternativer	-
	Søkealternativer	-
Systemadministrasjon		✓
	Kontaktadministrasjon	✓
	Administratorinnstillinger	✓
	Begrensninger	✓
	Passordkryptering	✓
	Kundeforskning	✓
	WSD-innstillinger	✓
	Gjenopprett standardinnst.	✓
	Fastvareoppdatering	✓
Enhetsinformasjon		-

Innst.-meny			Låsinnstilling
	Serienummer		-
	Gjeldende versjon		-
	Sum skanninger		-
	Antall 1-sidige skanninger		-
	Antall 2-sidige skanninger		-
	Antall skanninger med Bæreark		-
	Antall skanninger etter valsbytte		-
	Antall skanninger etter Vanlig rengjøring		-
	Tilbakestill antall skanninger		✓
Vedlikehold av skanner			-
	Rengjøring av vals		-
	Utskiftning av vedlikeholdsvalse		-
		Tilbakestill antall skanninger	✓
		Slik bytter du den ut	-
	Vanlig rengjøring		-
		Tilbakestill antall skanninger	✓
		Hvordan rengjøre	-
	Glassrengjøring		-
Varselinnstilling for utskiftning av valse			✓
	Antallvarsling		✓
Varslingsinnstillinger for ordinær rengjøring			✓
	Varslingsinnstilling for advarsel		✓
	Antallvarsling		✓

* Du kan angi hvorvidt du vil tillate endringer i **Systemadministrasjon** > **Begrensninger**.

Logge på som en administrator fra kontrollpanelet

Du kan bruke hvilken som helst av de følgende metodene for å logge inn som administrator fra skannerens kontrollpanel.

1. Trykk på  øverst til høyre på skjermen.
   - ❏ Når Godkjenningsinnstillinger er aktivert, vises ikonet på **Velkommen**-skjermen (standby-skjermen for godkjenning).

❏ Når Godkjenningsinnstillinger er deaktivert, vises ikonet på Hjem-skjermen.

2. Trykk på **Ja** når bekreftelsesskjermbildet vises.

3. Angi administratorpassord.

   En melding som forteller at pålogging er fullført vises, så vises Hjem-skjermen på kontrollpanelet.

Trykk på  øverst til høyre på Hjem-skjermen for å logge ut.

Deaktivere eksternt grensesnitt

Du kan deaktivere grensesnittet som brukes for å koble enheten til skanneren. Angi innstillingene for begrensningen for å begrense skanning annet enn via nettverket.

Merknad:
Du kan også angi innstillinger for begrensningen på skannerens kontrollpanel.

PC-tilkobling via USB: ***Innst.*** *>* ***Basisinnstillinger*** *>* ***PC-tilkobling via USB***

1. Gå inn på Web Config og velg **Produktsikkerhet**-fanen > **Eksternt grensesnitt**.

2. Velg **Deaktiver** på funksjonene du vil angi.

   Velg **Aktiver** når du vil avbryte kontrollering.

   PC-tilkobling via USB

   Du kan begrense bruken av USB-forbindelsen fra datamaskinen. Hvis du ønsker å begrense den, velg **Deaktiver**.

3. Klikk på **OK**.

4. Kontroller at den deaktiverte porten ikke kan brukes.

   PC-tilkobling via USB

   Hvis driveren ble installert på datamaskinen

   Koble skanneren til datamaskinen med en USB-kabel, og bekreft at skanneren ikke skanner.

   Hvis driveren ikke ble installert på datamaskinen

   Windows:

   Åpne enhetsbehandling og ikke lukk den igjen, koble skanneren til datamaskinen med en USB-kabel og bekreft at enhetsbehandlerens visning av innhold ikke endres.

   Mac OS:

   Koble skanneren til datamaskinen med en USB-kabel, og bekreft deretter at du ikke kan legge til skanneren fra **Skrivere og skannere**.

Relatert informasjon

➡ “Kjøre web-konfigurasjon på en nettleser” på side 34

Administrere en ekstern skanner

Sjekke informasjon for en ekstern skanner

Du kan kontrollere følgende informasjon om skanneren fra **Status** ved å bruke Web Config.

❏ Produktets status

Sjekk status, skytjeneste, produktnummer, MAC-adresse, osv.

❏ Nettverkstatus

Sjekk informasjon om status for nettverkstilkobling, IP-adresse, DNS-server, osv.

❏ Bruksstatus

Sjekk første dags skanninger, skanningsteller, osv.

❏ Maskinvarestatus

Sjekk statusen til hver av skannerens funksjoner.

❏ Paneløyeblikksbilde

Viser et øyeblikksbilde av skjermen som vises på skannerens kontrollpanel.

Motta e-postvarslinger når det skjer hendelser

Om e-postvarsler

Dette er varslingsfunksjonen som, når hendelser som skannestopp og skannerfeil oppstår, sender e-posten til den angitte adressen.

Du kan registrere opptil fem destinasjoner og angi varslingsinnstillingene for hver destinasjon.

For å bruke denne funksjonen, må du konfigurere e-postserveren før du konfigurerer varslinger.

Relatert informasjon

➡ "Konfigurere en e-postserver" på side 40

Konfiguere e-postvarsel

Konfigurer e-postvarsel ved hjelp av Web Config.

1. Gå inn på Web Config og velg **Enhetsadministrasjon**-fanen > **E-postvarsling**.
2. Angi emnet for e-postvarsling.

   Velg innholdet som vises på emnet fra de to nedtrekkslistene.

   ❏ Det valgte innholdet vises ved siden av **Emne**.

   ❏ Det samme innholdet kan angis til venstre og høyre.

   ❏ Når antall tegn i **Sted** overskrider 32 bytes, utelates de overskridende tegnene.

3. Skriv inn e-postadressen som skal sende e-postvarslingen.

   Bruk A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @, og skriv inn mellom 1 og 255 tegn.

4. Velg språk for e-postvarsler.

5. Velg avkrysningsboksen på hendelsen du ønsker å motta varsling for.

   Antall **Varslingsinnstillinger** er knyttet til destinasjonsantallet for **E-postadresseinnstillinger**.

   Eksempel:

   Hvis du ønsker å sende et varsel til e-postadressen som er angitt for nummer 1 i **E-postadresseinnstillinger**, når administratorpassordet er endret, velger du avmerkingsboksen for kolonne **1** i linjen **Administratorpassord endret**.

6. Klikk på **OK**.

   Bekreft at en e-postvarsling vil bli sendt ved å forårsake en hendelse.

   Eksempel: Administratorpassordet har blitt endret.

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34

Elementer for e-postvarsling

Artikler	Innstillinger og forklaring
Administratorpassord endret	Varsler når administratorpassordet har blitt endret.
Skannerfeil	Varsler når det har oppstått skannerfeil.
Wi-Fi-feil	Varsler når det har oppstått feil med det trådløse LAN-grensesnittet.

Problemløsning

Glemt administratorpassordet ditt

Du trenger hjelp fra servicepersonell. Kontakt lokalforhandleren.

Merknad:
Følgende gir opprinnelige verdier for Web Config-administratoren.

❏ *Brukernavn: ingen (tomt)*

❏ *Passord: serienummeret til skanneren*

Du finner serienummeret på etiketten på baksiden av skanneren. Hvis du gjenoppretter standardinnstillingene for administratorpassordet, tilbakestilles det til opprinnelige verdier.

Avanserte sikkerhetsinnstillinger

Sikkerhetsinnstillinger og forebygging av farlige situasjoner

Når en skanner er koblet til et nettverk, kan du få tilgang til den eksternt. I tillegg kan flere personer dele skanneren, noe som er nyttig for å øke effektiviteten av driften og gi økt bekvemmelighet. Imidlertid økes risikoen for ulovlig tilgang, ulovlig bruk og manipulering av data. Hvis du bruker skanneren i et miljø hvor det er tilgang til Internett, er risikoen enda høyere.

For skannere som ikke har ekstern tilgangsbeskyttelse vil det være mulig å lese historikk for kontakter som er lagret i skanneren via Internett.

For å unngå denne risikoen tilbyr Epson-skanner en rekke ulike sikkerhetsteknologier.

Still inn skanneren etter behov i henhold til de miljøforhold som har blitt bygget etter kundens miljøinformasjon.

Navn	Funksjonstype	Hva skal stilles inn	Hva skal forebygges
Kontroll av protokoller	Styrer protokollene og tjenestene som skal brukes til kommunikasjon mellom skannere og datamaskiner, og aktiverer og deaktiverer funksjoner.	En protokoll eller en tjeneste som brukes til funksjoner som tillatt eller forbudt separat.	Reduserer sikkerhetsrisikoer som kan oppstå ved utilsiktet bruk ved å hindre brukere fra å bruke unødvendige funksjoner.
SSL/TLS-kommunikasjon	Kommunikasjonsinnholdet er kryptert med SSL/TLS-kommunikasjon ved tilgang til Epson-serveren via Internett fra skanneren, som kommuniserer til datamaskinen via nettleseren ved hjelp av Epson Connect og oppdatering av fastvare.	Få tak i et CA-signert sertifikat, og deretter importer det til skanneren.	Fjerning av en identifikasjon for skanneren gjennom CA-signerte sertifikater forhindrer etterligning og uautorisert tilgang. I tillegg er kommunikasjonsinnholdet SSL/TLS-beskyttet, noe som forhindrer lekkasje av innholdet for skannedata og installasjonsdata.
IPsec/IP-filtrering	Du kan stille inn til å tillate brudd og avkutting av data som er fra en bestemt klient eller en bestemt type. Siden IPsec beskytter dataene etter IP-pakkeenhet (kryptering og autentisering), kan du trygt kommunisere usikret protokoll.	Opprett grunnleggende retningslinjer og individuelle retningslinjer for å angi hvilke klienter eller datatyper som kan få tilgang til skanneren.	Beskytt mot uautorisert tilgang og tukling og avskjæring av kommunikasjonsdata til skanneren.
IEEE 802.1X	Tillater kun godkjente brukere å koble til nettverket. Tillater kun at en bruker med godkjenning bruker skanneren.	Godkjenningsinnstilling av RADIUS-serveren (godkjenningsserver).	Beskytt mot uautorisert tilgang og bruk av skanneren.

Relatert informasjon

- ➡ “Kontrollere med protokoller” på side 92
- ➡ “SSL/TLS-kommunikasjon med skanneren” på side 100
- ➡ “Kryptert kommunikasjon ved bruk av IPsec/IP-filtrering” på side 102
- ➡ “Koble skanneren til et IEEE802.1X-nettverk” på side 113

Innstilling av sikkerhetsfunksjoner

Ved innstilling av IPsec/IP-filtrering eller IEEE 802.1X, anbefales det at du går inn på Web Config med SSL/TLS for å kommunisere innstillingsinformasjon for å redusere faren for sikkerhetsbrudd slik som manipulering eller avskjæring.

Forsikre at du konfigurerer administratorpassordet før du angir IPsec/IP-filtrering eller IEEE 802.1X.

Kontrollere med protokoller

Du kan skanne via ulike baner og protokoller. Du kan også bruke nettverkskanning fra et uspesifisert antall datamaskiner i nettverket.

Du kan redusere utilsiktede sikkerhetsrisikoer ved å begrense skanning via bestemte baner eller ved å kontrollere de tilgjengelige funksjonene.

Kontrollprotokoller

Konfigurer protokollinnstillingene som støttes av skanneren.

1. Gå inn på Web Config, og velg deretter **Nettverkssikkerhet** tab > **Protokoll**.
2. Konfigurer hvert element.
3. Klikk på **Neste**.
4. Klikk på **OK**.

   Innstillingene brukes på skanneren.

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34

Protokoller du kan Aktivere eller Deaktivere

Protokoll	Beskrivelse
Bonjour-innstillinger	Du kan angi om du vil bruke Bonjour. Bonjour brukes til å søke etter enheter, skanne, og så videre.
SLP-innstillinger	Du kan aktivere eller deaktivere SLP-funksjonen. SLP brukes for push-skanning og nettverkssøk i EpsonNet Config.
WSD-innstillinger	Du kan aktivere eller deaktivere WSD-funksjonen. Når denne er aktivert, kan du legge til WSD-enheter og skanne fra WSD-porten.
LLTD-innstillinger	Du kan aktivere eller deaktivere LLTD-funksjonen. Når denne er aktivert, vises den på nettverkskartet i Windows.
LLMNR-innstillinger	Du kan aktivere eller deaktivere LLMNR-funksjonen. Når denne er aktivert, kan du bruke navneløsing uten NetBIOS selv om du ikke kan bruke DNS.

Protokoll	Beskrivelse
SNMPv1/v2c-innstillinger	Du kan angi om du vil aktivere SNMPv1/v2c. Dette brukes til å sette opp enheter, overvåking og så videre.
SNMPv3-innstillinger	Du kan angi om du vil aktivere SNMPv3. Dette brukes til å sette opp krypterte enheter, overvåking, osv.

Innstillingselementer for protokoll

Bonjour-innstillinger

Artikler	Innstillingsverdi og beskrivelse
Bruk Bonjour	Marker her for å søke etter eller bruke enheter via Bonjour.
Bonjour-navn	Viser Bonjour-navn.
Bonjour servicenavn	Viser Bonjour-tjenestenavn.
Sted	Viser Bonjour-plasseringsnavn.
Wide-Area Bonjour	Angi hvorvidt Wide-Area Bonjour skal brukes.

SLP-innstillinger

Artikler	Innstillingsverdi og beskrivelse
Aktiver SLP	Velg dette for å aktivere SLP-funksjonen. Dette brukes som nettverkssøk i EpsonNet Config.

WSD-innstillinger

Artikler	Innstillingsverdi og beskrivelse
Aktiver WSD	Velg dette for å aktivere tillegging av enheter med WSD og skann fra WSD-porten.
Tidsavbrudd for skanning (sek)	Skriv inn verdi for tidsavbrudd av kommunikasjon for WSD-skanning mellom 3 og 3600 sekunder.
Enhetsnavn	Viser WSD-enhetsnavn.
Sted	Viser WSD-plasseringsnavn.

LLTD-innstillinger

Artikler	Innstillingsverdi og beskrivelse
Aktiver LLTD	Velg dette for å aktivere LLTD. Skanneren vises på Windows-nettverkskartet.
Enhetsnavn	Viser LLTD-enhetsnavn.

LLMNR-innstillinger

Artikler	Innstillingsverdi og beskrivelse
Aktiver LLMNR	Velg dette for å aktivere LLMNR. Du kan bruke navneløsing uten NetBIOS selv om du ikke kan bruke DNS.

SNMPv1/v2c-innstillinger

Artikler	Innstillingsverdi og beskrivelse
Aktiver SNMPv1/v2c	Velg for å aktivere SNMPv1/v2c.
Tilgangsautoritet	Definer tilgangsrettigheter når SNMPv1/v2c er aktivert. Velg **Skrivebeskyttet** eller **Les/Skriv**.
Gruppenavn (skrivebeskyttet)	Skriv inn 0 til 32 ASCII-tegn (0x20 til 0x7E).
Gruppenavn (lese/skrive)	Skriv inn 0 til 32 ASCII-tegn (0x20 til 0x7E).

SNMPv3-innstillinger

Artikler		Innstillingsverdi og beskrivelse
Aktiver SNMPv3		SNMPv3 er aktivert når boksen er krysset av.
Brukernavn		Skriv inn mellom 1 og 32 tegn ved hjelp av 1-biters tegn.
Godkjenningsinnstillinger		
	Algoritme	Velg en algorytme for autentisering for SNMPv3.
	Passord	Velg et passord for autentisering for SNMPv3. Skriv inn mellom 8 og 32 tegn i ASCII (0x20–0x7E). Hvis du ikke angir dette, la det stå tomt.
	Bekreft passord	Skriv inn passordet du konfigurerte som bekreftelse.
Krypteringsinnstillinger		
	Algoritme	Velg en algorytme for kryptering for SNMPv3.
	Passord	Velg et passord for kryptering for SNMPv3. Skriv inn mellom 8 og 32 tegn i ASCII (0x20–0x7E). Hvis du ikke angir dette, la det stå tomt.
	Bekreft passord	Skriv inn passordet du konfigurerte som bekreftelse.
Kontekstnavn		Skriv inn maksimalt 32 tegn i Unicode (UTF-8). Hvis du ikke angir dette, la det stå tomt. Antall tegn som kan angis varierer avhengig av språket som er brukt.

Bruke et digitalt sertifikat

Om digital sertifisering

❏ CA-signert sertifikat

Dette sertifikatet er signert av CA (sertifiseringsinstans). Du kan få det ved å søke til sertifiseringsinstansen. Dette sertifikatet sertifiserer skannerens eksistens og brukes for SSL/TLS-kommunikasjon, slik at du kan påse at datakommunikasjonen er sikker.

Når dette brukes for SSL/TLS-kommunikasjon, brukes det som et serversertifikat.

Når det er angitt til kommunikasjon med IPsec/IP-filtrering eller IEEE 802.1X, brukes det som et klientsertifikat.

❏ CA-sertifikat

Dette er et sertifikat i kjeden av CA-signert sertifikat, også kalt det mellomliggende CA-sertifikatet. Det brukes av nettleseren til å validere banen til skannerens sertifikat når du åpner serveren til den andre parten eller Web Config.

For CA-sertifikatet, angi når validering skal gjennomføres for banen til serversertifikat som åpnes fra skanneren. For skanneren, angi til å sertifisere banen til CA-signert sertifikat for SSL/TLS-tilkobling.

Du kan få skannerens CA-sertifikat fra sertifiseringsinstansen hvor CA-sertifikatet ble utstedt.

Du kan også få CA-sertifikatet brukt til å validere den andre partens server fra sertifiseringsinstansen som utstedte CA-signert sertifikat til den andre serveren.

❏ Selvsignert sertifikat

Dette er et sertifikat som skanneren signerer og til utsteder selv. Det kalles også rotsertifikatet. Ettersom utstederen sertifiserer selv, er det ikke pålitelig og kan ikke forhindre falske identiteter.

Bruk det når sikkerhetsinnstilling angis og når enkel SSL/TLS-kommunikasjon utføres uten CA-signert sertifikat.

Hvis du bruker dette sertifikatet som SSL/TLS-kommunikasjon, kan det vises en sikkerhetsadvarsel i nettleseren ettersom sertifikatet ikke er registrert på en nettleseren. Du kan bare bruke Selvsignert sertifikat for SSL/TLS-kommunikasjon.

Relatert informasjon

➡ “Konfigurere et CA-signert sertifikat” på side 95

➡ “Oppdatere et selvsignert sertifikat” på side 99

➡ “Konfigurere et CA-sertifikat” på side 99

Konfigurere et CA-signert sertifikat

Hente et CA-signert sertifikat

Vil du hente et CA-signert sertifikat, oppretter du en CSR (forespørsel om sertifikatsignering) og sender den til sertifiseringsinstansen. Du kan opprette en CSR ved hjelp av Web Config og en datamaskin.

Følg trinnene for å opprette en CSR og hente et CA-signert sertifikat med Web Config. Når du oppretter en CSR med Web Config, får sertifikatet PEM/DER-format.

1. Gå inn på Web Config, og velg deretter **Nettverkssikkerhet**-fanen. Deretter velger du **SSL/TLS** > **Sertifikat**, eller **IPsec/IP-filtrering** > **Klientsertifikat** eller **IEEE802.1X** > **Klientsertifikat**.

   Uansett hva du velger, kan du få samme sertifikat og bruke det i felles.

2. Klikk **Generer** under **CSR**.

   Det åpnes en side for oppretting av CSR.

3. Angi en verdi for hvert element.

   Merknad:
   Tilgjengelig nøkkellengde og forkortelser varierer etter sertifiseringsinstans. Opprett en forespørsel i henhold til reglene for hver sertifiseringsinstans.

4. Klikk på **OK**.

   Det vises en fullføringsmelding.

5. Velg kategorien **Nettverkssikkerhet**. Deretter velger du **SSL/TLS** > **Sertifikat**, eller **IPsec/IP-filtrering** > **Klientsertifikat** eller **IEEE802.1X** > **Klientsertifikat**.

6. Klikk én av nedlastingsknappene under **CSR** i henhold til angitt format for hver sertifiseringsinstans for å laste ned en CSR til datamaskinen.

   > ***Forsiktighetsregel:***
   > *Ikke generer CSR på nytt. Hvis du gjør det, kan du ikke være i stand til å importere et utstedt CA-signert sertifikat.*

7. Send CSR-en til en sertifiseringsinstans, og hent et CA-signert sertifikat.

   Følg reglene til hver sertifiseringsinstans når det gjelder sendemetode og format.

8. Lagre utstedt CA-signert sertifikat på en datamaskin som er koblet til skanneren.

   Hentingen av et CA-signert sertifikat er fullført når du lagrer sertifikatet et sted.

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34

Innstillingselementer for CSR

Artikler	Innstillinger og forklaring
Nøkkellengde	Velg en nøkkellengde for en CSR.

Artikler	Innstillinger og forklaring
Vanlig navn	Du kan skrive inn mellom 1 og 128 tegn. Hvis dette er en IP-adresse, bør det være en statisk IP-adresse. Du kan skrive inn fra 1 til 5 IPv4-adresser, IPv6-adresser, vertsnavn og FQDN-er ved å separere dem med komma. Det første elementet lagres til fellesnavnet, og andre elementer lagres til aliasfeltet til sertifikatsemnet. Eksempel: Skannerens IP-adresse: 192.0.2.123, Skannernavn: EPSONA1B2C3 Vanlig navn: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
Organisasjon/ Organisasjonsenhet/ Beliggenhet/ Stat/provins	Du kan skrive inn mellom 0 og 64 tegn i ASCII (0x20–0x7E). Du kan skille forskjellige navn med komma.
Land	Skriv inn en tosifret landskode angitt av ISO-3166.
Avsenderens e-postadresse	Du kan skrive inn mottakers e-postadresse i innstillingene for e-postserveren. Skriv inn samme e-postadresse som **Avsenderens e-postadresse** for **Nettverk**-fanen > **E-postserver** > **Grunnleggende**.

Importere et CA-signert sertifikat

Importer det hentede CA-signert sertifikat til skanneren.

Forsiktighetsregel:

❏ *Kontroller at skannerens dato og klokkeslett er riktig innstilt. Sertifikatet kan være ugyldig.*

❏ *Hvis du henter et sertifikat med en CSR som er opprettet fra Web Config, kan du importere et sertifikat én gang.*

1. Gå inn på Web Config, og velg deretter **Nettverkssikkerhet**-fanen. Deretter velger du **SSL/TLS** > **Sertifikat**, eller **IPsec/IP-filtrering** > **Klientsertifikat** eller **IEEE802.1X** > **Klientsertifikat**.

2. Klikk **Importer**

   Det åpnes en side for import av sertifikatet.

3. Angi en verdi for hvert element. Angi **CA-sertifikat 1** og **CA-sertifikat 2** ved verifisering av sertifikatets bane på nettleseren som har tilgang til skanneren.

   Avhengig av hvor du oppretter CSR og filformatet til sertifikatet, kan påkrevde innstillingselementer variere. Skriv inn verdier for påkrevde elementer i henhold til følgende.

   ❏ Et sertifikat med PEM/DER-format som er hentet fra Web Config

   ❏ **Privat nøkkel**: Må ikke konfigureres fordi skanneren inneholder en privattast.

   ❏ **Passord**: Skal ikke konfigureres.

   ❏ **CA-sertifikat 1**/**CA-sertifikat 2**: Valgfritt

   ❏ Et sertifikat med PEM/DER-format som er hentet fra datamaskinen

   ❏ **Privat nøkkel**: Må angis.

   ❏ **Passord**: Skal ikke konfigureres.

   ❏ **CA-sertifikat 1**/**CA-sertifikat 2**: Valgfritt

❏ Et sertifikat med PKCS#12-format som er hentet fra datamaskinen

❏ **Privat nøkkel**: Skal ikke konfigureres.

❏ **Passord**: Valgfritt

❏ **CA-sertifikat 1/CA-sertifikat 2**: Skal ikke konfigureres.

4. Klikk på **OK**.

   Det vises en fullføringsmelding.

Merknad:
*Klikk **Bekreft** for å bekrefte sertifikatinformasjonen.*

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34

Innstillingselementer for import av CA-signert sertifikat

Artikler	Innstillinger og forklaring
Serversertifikat eller Klientsertifikat	Velg format for sertifikatet. For SSL/TLS-tilkobling vises Serversertifikat. For IPsec-/IP-filtrering eller IEEE 802.1X vises Klientsertifikat.
Privat nøkkel	Hvis du henter et sertifikat med PEM/DER-format med en CSR som er opprettet fra en datamaskin, angir du filen for privatnøkkelen som samsvarer med sertifikatet.
Passord	Hvis filformatet er **Sertifikat med privat nøkkel (PKCS#12)**, skriver du inn passordet for kryptering av den private nøkkelen som er angitt når du henter sertifikatet.
CA-sertifikat 1	Hvis sertifikatets format er **Sertifikat (PEM/DER)**, importerer du et sertifikat fra en CA-signert sertifikat som brukes som utsteder av serversertifikater. Angi en fil om nødvendig.
CA-sertifikat 2	Hvis sertifikatets format er **Sertifikat (PEM/DER)**, importerer du et sertifikat fra en sertifiseringsinstans som utsteder CA-sertifikat 1. Angi en fil om nødvendig.

Slette et CA-signert sertifikat

Du kan slette et importert sertifikat når sertifikatet er utløpt eller når en kryptert tilkobling ikke lenger er nødvendig.

Forsiktighetsregel:
Hvis du henter et sertifikat med en CSR som er opprettet fra Web Config, kan du ikke importere et slettet sertifikat på nytt.I så fall må du opprette en CSR og hente et sertifikat på nytt.

1. Gå inn på Web Config, og velg deretter **Nettverkssikkerhet**-fanen.Deretter velger du **SSL/TLS** > **Sertifikat**, eller **IPsec/IP-filtrering** > **Klientsertifikat** eller **IEEE802.1X** > **Klientsertifikat**.

2. Klikk på **Slett**.

3. Bekreft at du vil slette sertifikatet i meldingen som vises.

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34

Oppdatere et selvsignert sertifikat

Ettersom Selvsignert sertifikat utstedes av skanneren, kan du oppdatere det når det har utløpt eller når innholdsbeskrivelsen endres.

1. Gå inn på Web Config og velg **Nettverkssikkerhet** tab > **SSL/TLS** > **Sertifikat**.
2. Klikk på **Oppdater**.
3. Skriv inn **Vanlig navn**.

   Du kan skrive inn opptil 5 IPv4-adresser, IPv6-adresser, vertsnavn og FQDN-er mellom 1 og 128 tegn og separere dem med komma. Den første parameteren lagres til fellesnavnet, og de andre lagres til aliasfeltet for emnet til sertifikatet.

   Eksempel:

   Skannerens IP-adresse: 192.0.2.123, Skannernavn: EPSONA1B2C3

   Fellesnavn: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
4. Angi en gyldighetsperiode for sertifikatet.
5. Klikk på **Neste**.

   Det vises en bekreftelsesmelding.
6. Klikk på **OK**.

   Skanneren er oppdatert.

Merknad:
*Du kan kontrollere sertifikatinformasjonen fra **Nettverkssikkerhet**-fanen > **SSL/TLS** > **Sertifikat** > **Selvsignert sertifikat** og klikk på **Bekreft**.*

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34

Konfigurere et CA-sertifikat

Når du angir CA-sertifikat, kan du validere banen til serverens CA-sertifikat som brukes av skanneren. Dette kan forhindre falske identiteter.

Du kan få CA-sertifikat fra sertifiseringsinstansen hvor CA-signert sertifikat ble utstedt.

Importere et CA-sertifikat

Importer CA-sertifikat til skanneren.

1. Åpne Web Config og velg **Nettverkssikkerhet**-fanen > **CA-sertifikat**.
2. Klikk på **Importer**.
3. Velg CA-sertifikat du vil importere.
4. Klikk på **OK**.

Når importeringen er fullført, sendes du tilbake til **CA-sertifikat** skjermen, og importert CA-sertifikat vises.

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34

Slette et CA-sertifikat

Du kan slette et importert CA-sertifikat.

1. Gå inn på Web Config og velg deretter **Nettverkssikkerhet**-fanen > **CA-sertifikat**.
2. Klikk på **Slett** ved siden av CA-sertifikat du vil slette.
3. Bekreft at du vil slette sertifikatet i meldingen som vises.
4. Klikk på **Start nettverk på nytt** og kontroller at det slettede CA-sertifikatet ikke er oppført i det oppdaterte skjermbildet.

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34

SSL/TLS-kommunikasjon med skanneren

Når skriversertifikatet angis ved bruk av SSL/TLS (Secure Sockets Layer/Transport Layer Security)-kommunikasjon med skanneren kan du kryptere kommunikasjonsbanen mellom datamaskinene. Gjør dette dersom du ønsker å forhindre ekstern eller uautorisert tilgang.

Konfigurere grunnleggende SSL/TLS-innstillinger

Hvis skanneren støtter HTTPS-serverfunksjonen, kan du bruke SSL/TLS-kommunikasjon til å kryptere kommunikasjon. Du kan konfigurere og styre skanneren med Web Config på en sikker måte.

Konfigurer krypteringsstyrke og funksjon for videresending.

1. Gå inn på Web Config og velg **Nettverkssikkerhet**-fanen > **SSL/TLS** > **Grunnleggende**.

2. Velg en verdi for hvert element.
   - ❏ Krypteringsstyrke
     Velg nivå for krypteringsstyrke.
   - ❏ Omdiriger HTTP til HTTPS
     Omdirigering til HTTPS når HTTP åpnes.
3. Klikk på **Neste**.
   Det vises en bekreftelsesmelding.
4. Klikk på **OK**.
   Skanneren er oppdatert.

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34

Konfigurere et serversertifikat for skanneren

1. Gå inn på Web Config og velg **Nettverkssikkerhet**-fanen > **SSL/TLS** > **Sertifikat**.
2. Angi sertifikatet som skal brukes på **Serversertifikat**.
   - ❏ Selvsignert sertifikat
     Det er generert et selvsignert sertifikat av skanneren. Velg dette hvis du ikke henter et CA-signert sertifikat.
   - ❏ CA-signert sertifikat
     Hvis du har hentet og importert et CA-signert sertifikat på forhånd, kan du angi dette.
3. Klikk på **Neste**.
   Det vises en bekreftelsesmelding.
4. Klikk på **OK**.
   Skanneren er oppdatert.

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34
➡ "Konfigurere et CA-signert sertifikat" på side 95
➡ "Konfigurere et CA-sertifikat" på side 99

Kryptert kommunikasjon ved bruk av IPsec/IP-filtrering

Om IPsec/IP-filtrering

Du kan filtrere trafikk basert på IP-adresser, tjenester og port ved å bruke IPsec/IP-filtreringsfunksjon. Ved å kombinere filtreringen kan du konfigurere skanneren til å godta eller blokkere bestemte klienter og bestemte data. Du kan dessuten øke sikkerhetsnivået ved hjelp av IPsec.

Merknad:
Datamaskiner som kjører Windows Vista eller senere, eller Windows Server 2008 eller senere støtter IPsec.

Konfigurere standardpolicy

Vil du filtrere trafikk, kan du konfigurere standardpolicyen. Standardpolicyen gjelder for alle brukere eller grupper som kobler til skanneren. Du kan konfigurere gruppepolicyer hvis du vil ha mer detaljert kontroll over brukere og brukergrupper.

1. Gå inn på Web Config, og velg deretter **Nettverkssikkerhet**-fanen > **IPsec/IP-filtrering** > **Grunnleggende**.
2. Angi en verdi for hvert element.
3. Klikk på **Neste**.

   Det vises en bekreftelsesmelding.
4. Klikk på **OK**.

   Skanneren er oppdatert.

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34

Innstillingselementer for Standardpolicy

Standardpolicy

Artikler	Innstillinger og forklaring
IPsec/IP-filtrering	Du kan aktivere eller deaktivere en funksjon for IPsec-/IP-filtrering.

❏ Tilgangskontroll

Konfigurer en kontrollmetode for trafikk av IP-pakker.

Artikler	Innstillinger og forklaring
Gi tilgang	Velg dette for å tillate at konfigurerte IP-pakker passerer.
Nekt tilgang	Velg dette for å hindre at konfigurerte IP-pakker passerer.
IPsec	Velg dette for å tillate at konfigurerte IPsec-pakker passerer.

❏ **IKE-versjon**

Velg **IKEv1** eller **IKEv2** for **IKE-versjon**. Velg en av dem avhengig av hvilken enhet skanneren er koblet til.

❏ IKEv1

Følgende elementer vises når du velger **IKEv1** for **IKE-versjon**.

Artikler	Innstillinger og forklaring
Godkjenningsmetode	Vil du velge **Sertifikat**, må du på forhånd hente og importere et CA-signert sertifikat.
Forhåndsdelt nøkkel	Hvis du velger **Forhåndsdelt nøkkel** for **Godkjenningsmetode**, skriver du inn en forhåndsdelt tast på opptil 127 tegn.
Bekreft Forhåndsdelt nøkkel	Skriv inn tasten du konfigurerte for bekreftelse.

❏ IKEv2

Følgende elementer vises når du velger **IKEv2** for **IKE-versjon**.

Artikler		Innstillinger og forklaring
Lokal	Godkjenningsmetode	Vil du velge **Sertifikat**, må du på forhånd hente og importere et CA-signert sertifikat.
	ID-type	Hvis du velger **Forhåndsdelt nøkkel** som **Godkjenningsmetode**, må du velge ID-typen for skanneren.
	ID	Angi skannerens ID, som samsvarer med ID-typen. Du kan ikke bruke «@», «#» eller «=» som første tegn. **Unikt navn**: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde «=». **IP-adresse**: Angi format, enten IPv4 eller IPv6. **FQDN**: Skriv inn en kombinasjon av mellom 1 og 255 tegn med A–Z, a–z, 0–9, «-», og punktum (.). **E-postadresse**: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde «@». **Nøkkel-ID**: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E).
	Forhåndsdelt nøkkel	Hvis du velger **Forhåndsdelt nøkkel** for **Godkjenningsmetode**, skriver du inn en forhåndsdelt tast på opptil 127 tegn.
	Bekreft Forhåndsdelt nøkkel	Skriv inn tasten du konfigurerte for bekreftelse.

Artikler		Innstillinger og forklaring
Ekstern	Godkjenningsmetode	Vil du velge **Sertifikat**, må du på forhånd hente og importere et CA-signert sertifikat.
	ID-type	Hvis du velger **Forhåndsdelt nøkkel** som **Godkjenningsmetode**, må du velge ID-type for enheten du vil godkjenne.
	ID	Angi skannerens ID, som samsvarer med ID-type. Du kan ikke bruke «@», «#» eller «=» som første tegn. **Unikt navn**: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde «=». **IP-adresse**: Angi format, enten IPv4 eller IPv6. **FQDN**: Skriv inn en kombinasjon av mellom 1 og 255 tegn med A–Z, a–z, 0–9, «-», og punktum (.). **E-postadresse**: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde «@». **Nøkkel-ID**: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E).
	Forhåndsdelt nøkkel	Hvis du velger **Forhåndsdelt nøkkel** for **Godkjenningsmetode**, skriver du inn en forhåndsdelt tast på opptil 127 tegn.
	Bekreft Forhåndsdelt nøkkel	Skriv inn tasten du konfigurerte for bekreftelse.

❏ Innkapsling

Velger du **IPsec** for **Tilgangskontroll**, må du konfigurere en innkapslingsmodus.

Artikler	Innstillinger og forklaring
Transportmodus	Velg dette hvis du bare bruker skanneren på samme LAN. IP-pakker med lag 4 eller nyere blir kryptert.
Tunnelmodus	Hvis du bruker skanneren på et nettverk som kan kobles til Internett, slik som IPsec-VPN, velg dette alternativet. Toppteksten og dataene i IP-pakkene blir kryptert. **Ekstern gateway (Tunnelmodus)**: Hvis du velger **Tunnelmodus** for **Innkapsling**, skriver du inn en gateway-adresse på mellom 1 og 39 tegn.

❏ Sikkerhetsprotokoll

Velg et alternativ hvis du velger **IPsec** for **Tilgangskontroll**.

Artikler	Innstillinger og forklaring
ESP	Velg dette for å sikre integriteten til en godkjenning og dataene, samt kryptere data.
AH	Velg dette for å sikre integriteten til en godkjenning og dataene. Du kan bruke IPsec selv om det er forbudt å kryptere data.

❏ **Algoritmeinnstillinger**

Det anbefales at du velger **Enhver** for alle innstillinger, eller velger et annet element enn **Enhver** for hver innstilling. Hvis du velger **Enhver** for enkelte innstillinger, og velger et annet element enn **Enhver** for de andre innstillingene, kan enheten muligens ikke kommunisere, avhengig av den andre enheten du vil godkjenne.

Artikler		Innstillinger og forklaring
IKE	Kryptering	Velg krypteringsalgoritme for IKE. Elementene vil variere avhengig av IKE-versjon.
	Godkjenning	Velg godkjenningsalgoritme for IKE.
	Nøkkelutveksling	Velg nøkkelendringsalgoritme for IKE. Elementene vil variere avhengig av IKE-versjon.
ESP	Kryptering	Velg krypteringsalgoritme for ESP. Dette er tilgjengelig når **ESP** er valgt for **Sikkerhetsprotokoll**.
	Godkjenning	Velg godkjenningsalgoritme for ESP. Dette er tilgjengelig når **ESP** er valgt for **Sikkerhetsprotokoll**.
AH	Godkjenning	Velg krypteringsalgoritme for AH. Dette er tilgjengelig når **AH** er valgt for **Sikkerhetsprotokoll**.

Konfigurere gruppepolicy

En gruppepolicy er én eller flere regler som brukes på en bruker eller brukergruppe. Skanneren kontrollerer IP-pakker som samsvarer med konfigurerte policyer. IP-pakker godkjennes i rekkefølge som gruppepolicy 1 til 10, og deretter som standardpolicy.

1. Gå inn på Web Config, og velg deretter **Nettverkssikkerhet**-fanen > **IPsec/IP-filtrering** > **Grunnleggende**.
2. Klikk på en numerert tast du vil konfigurere.
3. Angi en verdi for hvert element.
4. Klikk på **Neste**.

   Det vises en bekreftelsesmelding.
5. Klikk på **OK**.

   Skanneren er oppdatert.

Innstillingselementer for Gruppepolicy

Artikler	Innstillinger og forklaring
Deaktiver denne Gruppepolicy	Du kan aktivere eller deaktivere en gruppepolicy.

Tilgangskontroll

Konfigurer en kontrollmetode for trafikk av IP-pakker.

Artikler	Innstillinger og forklaring
Gi tilgang	Velg dette for å tillate at konfigurerte IP-pakker passerer.
Nekt tilgang	Velg dette for å hindre at konfigurerte IP-pakker passerer.
IPsec	Velg dette for å tillate at konfigurerte IPsec-pakker passerer.

Lokal adresse (skanner)

Velg en IPv4-adresse eller IPv6-adresse som matcher ditt nettverksmiljø. Hvis en IP-adresse er gitt automatisk, kan du velge **Bruk automatisk innhentet IPv4-adresse**.

Merknad:
Hvis en IPv6-adresse tilordnes automatisk, kan tilkoblingen være utilgjengelig. Konfigurer en statisk IPv6-adresse.

Ekstern adresse (vert)

Skriv inn en enhets IP-adresse for å kontrollere tilgangen. IP-adressen må være mindre enn 43 tegn. Hvis du ikke skriver inn en IP-adresse, blir alle adressene kontrollerte.

Merknad:
Hvis en IP-adresse tilordnes automatisk (f.eks. tilordnes via DHCP), kan tilkoblingen være utilgjengelig. Konfigurer en statisk IP-adresse.

Metode for å velge port

Velg en metode for å spesifisere porter.

❏ Tjenestenavn

Velg et alternativ hvis du velger **Tjenestenavn** for **Metode for å velge port**.

❏ Transportprotokoll

Velger du **Portnummer** for **Metode for å velge port**, må du konfigurere en innkapslingsmodus.

Artikler	Innstillinger og forklaring
Alle protokoller	Velg dette for å kontrollere alle protokolltyper.
TCP	Velg dette for å kontrollere data for unikasting.
UDP	Velg dette for å kontrollere data for kringkasting og multikasting.
ICMPv4	Velg dette for å kontrollere Ping-kommando.

❏ Lokal port

Hvis du velger **Portnummer** for **Metode for å velge port** og hvis du velger **TCP** eller **UDP** for **Transportprotokoll**, skriv inn portnumre for å kontrollere mottakspakker, og separer dem med kommaer. Du kan skrive inn opptil 10 portnumre.

Eksempel: 20,80,119,5220

Hvis du ikke skriver inn et portnummer, blir alle portene kontrollert.

❏ Ekstern port

Hvis du velger **Portnummer** for **Metode for å velge port** og hvis du velger **TCP** eller **UDP** for **Transportprotokoll**, skriv inn portnumre for å kontrollere sendingspakker, og separer dem med kommaer. Du kan skrive inn opptil 10 portnumre.

Eksempel: 25,80,143,5220

Hvis du ikke skriver inn et portnummer, blir alle portene kontrollert.

IKE-versjon

Velg **IKEv1** eller **IKEv2** for **IKE-versjon**. Velg en av dem avhengig av hvilken enhet skanneren er koblet til.

❏ IKEv1

Følgende elementer vises når du velger **IKEv1** for **IKE-versjon**.

Artikler	Innstillinger og forklaring
Godkjenningsmetode	Velg et alternativ hvis du velger **IPsec** for **Tilgangskontroll**. Brukt sertifikat er det samme som standardpolicyen.
Forhåndsdelt nøkkel	Hvis du velger **Forhåndsdelt nøkkel** for **Godkjenningsmetode**, skriver du inn en forhåndsdelt tast på opptil 127 tegn.
Bekreft Forhåndsdelt nøkkel	Skriv inn tasten du konfigurerte for bekreftelse.

❏ IKEv2

Følgende elementer vises når du velger **IKEv2** for **IKE-versjon**.

Artikler		Innstillinger og forklaring
Lokal	Godkjenningsmetode	Velg et alternativ hvis du velger **IPsec** for **Tilgangskontroll**. Brukt sertifikat er det samme som standardpolicyen.
	ID-type	Hvis du velger **Forhåndsdelt nøkkel** som **Godkjenningsmetode**, må du velge ID-typen for skanneren.
	ID	Angi skannerens ID, som samsvarer med ID-typen. Du kan ikke bruke «@», «#» eller «=» som første tegn. **Unikt navn**: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde «=». **IP-adresse**: Angi format, enten IPv4 eller IPv6. **FQDN**: Skriv inn en kombinasjon av mellom 1 og 255 tegn med A–Z, a–z, 0–9, «-», og punktum (.). **E-postadresse**: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde «@». **Nøkkel-ID**: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E).
	Forhåndsdelt nøkkel	Hvis du velger **Forhåndsdelt nøkkel** for **Godkjenningsmetode**, skriver du inn en forhåndsdelt tast på opptil 127 tegn.
	Bekreft Forhåndsdelt nøkkel	Skriv inn tasten du konfigurerte for bekreftelse.
Ekstern	Godkjenningsmetode	Velg et alternativ hvis du velger **IPsec** for **Tilgangskontroll**. Brukt sertifikat er det samme som standardpolicyen.
	ID-type	Hvis du velger **Forhåndsdelt nøkkel** som **Godkjenningsmetode**, må du velge ID-type for enheten du vil godkjenne.
	ID	Angi skannerens ID, som samsvarer med ID-type. Du kan ikke bruke «@», «#» eller «=» som første tegn. **Unikt navn**: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde «=». **IP-adresse**: Angi format, enten IPv4 eller IPv6. **FQDN**: Skriv inn en kombinasjon av mellom 1 og 255 tegn med A–Z, a–z, 0–9, «-», og punktum (.). **E-postadresse**: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde «@». **Nøkkel-ID**: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E).
	Forhåndsdelt nøkkel	Hvis du velger **Forhåndsdelt nøkkel** for **Godkjenningsmetode**, skriver du inn en forhåndsdelt tast på opptil 127 tegn.
	Bekreft Forhåndsdelt nøkkel	Skriv inn tasten du konfigurerte for bekreftelse.

Innkapsling

Velger du **IPsec** for **Tilgangskontroll**, må du konfigurere en innkapslingsmodus.

Artikler	Innstillinger og forklaring
Transportmodus	Velg dette hvis du bare bruker skanneren på samme LAN. IP-pakker med lag 4 eller nyere blir kryptert.
Tunnelmodus	Hvis du bruker skanneren på et nettverk som kan kobles til Internett, slik som IPsec-VPN, velg dette alternativet. Toppteksten og dataene i IP-pakkene blir kryptert. **Ekstern gateway (Tunnelmodus)**: Hvis du velger **Tunnelmodus** for **Innkapsling**, skriver du inn en gateway-adresse på mellom 1 og 39 tegn.

Sikkerhetsprotokoll

Velg et alternativ hvis du velger **IPsec** for **Tilgangskontroll**.

Artikler	Innstillinger og forklaring
ESP	Velg dette for å sikre integriteten til en godkjenning og dataene, samt kryptere data.
AH	Velg dette for å sikre integriteten til en godkjenning og dataene. Du kan bruke IPsec selv om det er forbudt å kryptere data.

Algoritmeinnstillinger

Det anbefales at du velger **Enhver** for alle innstillinger, eller velger et annet element enn **Enhver** for hver innstilling. Hvis du velger **Enhver** for enkelte innstillinger, og velger et annet element enn **Enhver** for de andre innstillingene, kan enheten muligens ikke kommunisere, avhengig av den andre enheten du vil godkjenne.

Artikler		Innstillinger og forklaring
IKE	Kryptering	Velg krypteringsalgoritme for IKE. Elementene vil variere avhengig av IKE-versjon.
	Godkjenning	Velg godkjenningsalgoritme for IKE.
	Nøkkelutveksling	Velg nøkkelendringsalgoritme for IKE. Elementene vil variere avhengig av IKE-versjon.
ESP	Kryptering	Velg krypteringsalgoritme for ESP. Dette er tilgjengelig når **ESP** er valgt for **Sikkerhetsprotokoll**.
	Godkjenning	Velg godkjenningsalgoritme for ESP. Dette er tilgjengelig når **ESP** er valgt for **Sikkerhetsprotokoll**.
AH	Godkjenning	Velg krypteringsalgoritme for AH. Dette er tilgjengelig når **AH** er valgt for **Sikkerhetsprotokoll**.

Kombinasjon av Lokal adresse (skanner) og Ekstern adresse (vert) på Gruppepolicy

	Innstilling av Lokal adresse (skanner)		
	IPv4	IPv6*2	Alle adresser*3

Innstilling av Ekstern adresse (vert)	IPv4*1	✓	–	✓
	IPv6*1*2	–	✓	✓
	Tom	✓	✓	✓

*1 Hvis **IPsec** er valgt for **Tilgangskontroll**, kan du ikke spesifisere i en prefikslengde.

*2 Hvis **IPsec** er valgt for **Tilgangskontroll**, kan du velge en link-lokal-adresse (fe80::), men gruppepolicy vil deaktiveres.

*3 Utenom IPv6-link-lokal-adresser.

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34

Referanser for tjenestenavn på gruppepolicy

Merknad:
Utilgjengelige tjenester vil vises men kan ikke velges.

Tjenestenavn	Protokolltype	Lokalt portnummer	Eksternt portnummer	Kontrollerte funksjoner
Enhver	–	–	–	Alle tjenester
ENPC	UDP	3289	Hvilken som helst port	Søker etter en skanner fra programmer slik som Epson Device Admin og så en skannerdriver
SNMP	UDP	161	Hvilken som helst port	Henter og konfigurerer MIB fra programmer slik som Epson Device Admin og Epson-skannerdriveren
WSD	TCP	Hvilken som helst port	5357	Kontrollerer WSD
WS-Discovery	UDP	3702	Hvilken som helst port	Søker etter WSD-skannere
Network Scan	TCP	1865	Hvilken som helst port	Videresender skannede data fra Document Capture Pro
Network Push Scan	TCP	Hvilken som helst port	2968	Henter jobbinformasjon for push-skanning fra Document Capture Pro
Network Push Scan Discovery	UDP	2968	Hvilken som helst port	Søke etter en datamaskin fra skanner
FTP-data (ekstern)	TCP	Hvilken som helst port	20	FTP-klient (videresender skannede data) Denne kan imidlertid bare kontrollere en FTP-server som bruker eksternt portnummer 20.
FTP-kontroll (ekstern)	TCP	Hvilken som helst port	21	FTP-klient (kontrollerer videresendte skannede data)

Tjenestenavn	Protokolltype	Lokalt portnummer	Eksternt portnummer	Kontrollerte funksjoner
CIFS (ekstern)	TCP	Hvilken som helst port	445	CIFS-klient (videresender skannede data til en mappe)
NetBIOS Name Service (ekstern)	UDP	Hvilken som helst port	137	CIFS-klient (videresender skannede data til en mappe)
NetBIOS Datagram Service (ekstern)	UDP	Hvilken som helst port	138	
NetBIOS Session Service (ekstern)	TCP	Hvilken som helst port	139	
HTTP (lokal)	TCP	80	Hvilken som helst port	HTTP(S)-server (videresender data fra Web Config og WSD)
HTTPS (lokal)	TCP	443	Hvilken som helst port	
HTTP (ekstern)	TCP	Hvilken som helst port	80	HTTP(S)-klient (oppdaterer fastvaren og rotsertifikatet)
HTTPS (ekstern)	TCP	Hvilken som helst port	443	

Eksempler på IPsec/IP-filtrering

Mottar kun IPsec-pakker

Dette eksemplet viser kun hvordan du konfigurerer en standardpolicy.

Standardpolicy:

❏ **IPsec/IP-filtrering**: **Aktiver**

❏ **Tilgangskontroll**: **IPsec**

❏ **Godkjenningsmetode**: **Forhåndsdelt nøkkel**

❏ **Forhåndsdelt nøkkel**: Skriv inn opptil 127 tegn.

Gruppepolicy: Skal ikke konfigureres.

Mottar skannerdata og skanneinnstillinger

Dette eksemplet tillater kommunikasjon av skannerdata og skannerkonfigurasjon fra spesifiserte skannere.

Standardpolicy:

❏ **IPsec/IP-filtrering**: **Aktiver**

❏ **Tilgangskontroll**: **Nekt tilgang**

Gruppepolicy:

❏ **Deaktiver denne Gruppepolicy**: Merk av for dette alternativet.

❏ **Tilgangskontroll**: **Gi tilgang**

❏ **Ekstern adresse (vert)**: IP-adresse til en klient

❏ **Metode for å velge port**: **Tjenestenavn**

❏ **Tjenestenavn**: Huk av boksen for **ENPC**, **SNMP**, **HTTP (lokal)**, **HTTPS (lokal)** og **Network Scan**.

Få tilgang kun fra en angitt IP-adresse

Dette eksemplet tillater at en angitt IP-adresse får tilgang til skanneren.

Standardpolicy:

❏ **IPsec/IP-filtrering**: **Aktiver**

❏ **Tilgangskontroll**:**Nekt tilgang**

Gruppepolicy:

❏ **Deaktiver denne Gruppepolicy**: Merk av for dette alternativet.

❏ **Tilgangskontroll**: **Gi tilgang**

❏ **Ekstern adresse (vert)**: IP-adresse til en administrators klient

Merknad:
Uavhengig av policykonfigurasjonen vil klienten kunne få tilgang til og konfigurere skanneren.

Konfigurere et sertifikat for IPsec/IP-filtrering

Konfigurer klientsertifikat for IPsec/IP-filtrering. Når du angir det, kan du bruke sertifikatet som en godkjenningsmetode for IPsec/IP-filtrering. Hvis du vil konfigurere sertifiseringsinstans, går du til **CA-sertifikat**.

1. Gå inn på Web Config og velg deretter **Nettverkssikkerhet**-fanen > **IPsec/IP-filtrering** > **Klientsertifikat**.

2. Importer sertifikatet i **Klientsertifikat**.

   Hvis du allerede har importert et sertifikat utgitt av en sertifiseringsinstans, kan du kopiere sertifikatet og bruke det i IPsec/IP-filtrering. Slik kopierer du det: Velg sertifikatet fra **Kopier fra**, og klikk deretter på **Kopi**.

Relatert informasjon

➡ “Kjøre web-konfigurasjon på en nettleser” på side 34

➡ “Konfigurere et CA-signert sertifikat” på side 95

➡ “Konfigurere et CA-sertifikat” på side 99

Koble skanneren til et IEEE802.1X-nettverk

Konfigurere et IEEE 802.1X-nettverk

Når du angir IEEE 802.1X til skanneren, kan du bruke det på nettverket koblet til en RADIUS-server, en LAN-bryter med godkjenningsfunksjon eller et tilgangspunkt.

1. Gå inn på Web Config, og velg deretter **Nettverkssikkerhet**-fanen > **IEEE802.1X** > **Grunnleggende**.

2. Angi en verdi for hvert element.

   Hvis du vil bruke skanneren på et trådløst nettverk, klikk på **Wi-Fi-konfigurering** og velg eller fyll inn en SSID.

   Merknad:
   Du kan dele innstillingene mellom Ethernet og Wi-Fi.

3. Klikk på **Neste**.

   Det vises en bekreftelsesmelding.

4. Klikk på **OK**.

   Skanneren er oppdatert.

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34

Innstillingselementer for IEEE 802.1X-nettverk

Artikler	Innstillinger og forklaring	
IEEE802.1X (kablet LAN)	Du kan aktivere eller deaktivere innstillingene på siden (**IEEE802.1X** > **Grunnleggende**) for IEEE802.1X (kablet LAN).	
IEEE802.1X (Wi-Fi)	Tilkoblingsstatusen for IEEE802.1X (Wi-Fi) vises.	
Tilkoblingsmetode	Tilkoblingsmetoden for gjeldende nettverk vises.	
EAP-type	Velg et alternativ for en godkjenningsmetode mellom skanneren og en RADIUS-server.	
	EAP-TLS	Du må få tak i og importere et CA-signert sertifikat.
	PEAP-TLS	
	PEAP/MSCHAPv2	Du må konfigurere et passord.
	EAP-TTLS	
Bruker-ID	Konfigurer en ID som skal brukes som godkjenning av en RADIUS-server. Skriv inn 1 til 128 enkeltbyte ASCII-tegn (0x20 til 0x7E).	
Passord	Konfigurer et passord for å godkjenne skanneren. Skriv inn 1 til 128 enkeltbyte ASCII-tegn (0x20 til 0x7E). Hvis du bruker en Windows-server som en RADIUS-server, kan du angi opptil 127 tegn.	
Bekreft passord	Skriv inn passordet du konfigurerte som bekreftelse.	
Server-ID	Du kan konfigurere en server-ID for å godkjenne med en bestemt RADIUS-server. Godkjenner bekrefter om det finnes en server-ID i feltet subject/subjectAltName til et serversertifikat som er sendt fra en RADIUS-server. Skriv inn 0 til 128 enkeltbyte ASCII-tegn (0x20 til 0x7E).	
Sertifikatvalidering	Du kan stille inn sertifikatvalidering uavhengig av autentiseringsmetode. Importer sertifikatet i **CA-sertifikat**.	

Artikler	Innstillinger og forklaring	
Anonymt navn	Hvis du velger **PEAP-TLS** eller **PEAP/MSCHAPv2** for **EAP-type**, kan du konfigurere et anonymt navn i stedet for en bruker-ID for fase 1 i en PEAP-godkjenning. Skriv inn 0 til 128 enkeltbyte ASCII-tegn (0x20 til 0x7E).	
Krypteringsstyrke	Du kan velge én av følgende.	
	Høy	AES256/3DES
	Middels	AES256/3DES/AES128/RC4

Konfigurere et sertifikat for IEEE 802.1X

Konfigurer klientsertifikat for IEEE802.1X. Når du angir det, kan du bruke **EAP-TLS** og **PEAP-TLS** som godkjenningsmetode for IEEE 802.1X. Hvis du vil konfigurere sertifiseringsinstanssertifikatet, går du til **CA-sertifikat**.

1. Gå inn på Web Config og velg deretter **Nettverkssikkerhet**-fanen > **IEEE802.1X** > **Klientsertifikat**.
2. Angi et sertifikat i **Klientsertifikat**.

   Hvis du allerede har importert et sertifikat utgitt av en sertifiseringsinstans, kan du kopiere sertifikatet og bruke det i IEEE802.1X. Slik kopierer du det: Velg sertifikatet fra **Kopier fra**, og klikk deretter på **Kopi**.

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34

Løse problemer med avanserte sikkerhetsinnstillinger

Gjenopprette sikkerhetsinnstillingene

Når du oppretter et svært sikkert miljø slik som IPsec/IP-filtrering, vil du kanskje ikke være i stand til å kommunisere med enheter på grunn av feil innstillinger eller problemer med enheten eller serveren. I dette tilfellet, gjenoppretter du sikkerhetsinnstillingene for å foreta innstillinger av enheten på nytt eller muliggjøre midlertidig bruk.

Deaktivere sikkerhetsfunksjonen med Web Config

Du kan deaktivere IPsec/IP-filtrering med Web Config.

1. Gå inn på Web Config og velg **Nettverkssikkerhet**-fanen > **IPsec/IP-filtrering** > **Grunnleggende**.
2. Deaktiver **IPsec/IP-filtrering**.

Problemer ved bruk av funksjoner for nettverkssikkerhet

Glemt en forhåndsdelt tast

Konfigurere en forhåndsdelt tast på nytt.

For å endre tasten, gå inn på Web Config og velg **Nettverkssikkerhet**-fanen > **IPsec/IP-filtrering** > **Grunnleggende** > **Standardpolicy** eller **Gruppepolicy**.

Når du endrer den forhåndsdelte nøkkelen, konfigurer den forhåndsdelte nøkkelen for datamaskiner.

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34
➡ "Kryptert kommunikasjon ved bruk av IPsec/IP-filtrering" på side 102

Kan ikke kommunisere med IPsec-kommunikasjon

Spesifiser algoritmen som skanneren eller datamaskinen ikke støtter.

Skanneren støtter følgende algoritmer. Kontroller innstillingene på datamaskinen.

Sikkerhetsmetoder	Algeritmer
IKE-krypteringsalgoritme	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE-godkjenningsalgoritme	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE nøkkelendringsalgoritme	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-krypteringsalgoritme	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP-godkjenningsalgoritme	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH-godkjenningsalgoritme	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* kun tilgjengelig for IKEv2

Relatert informasjon

➡ "Kryptert kommunikasjon ved bruk av IPsec/IP-filtrering" på side 102

Kan plutselig ikke kommunisere

Skannerens IP-adresse har blitt endret eller kan ikke brukes.

Når IP-adressen registrert til den lokale adressen på Gruppepolicy har blitt endret eller ikke kan brukes, kan ikke IPsec-kommunisering gjennomføres. Deaktiver IPsec via skannerens kontrollpanel.

Hvis DHCP er utgått, eller omstart eller IPv6-adresse er utgått eller ikke har blitt hentet, vil IP-adressen som er registrert i skannerens Web Config (**Nettverkssikkerhet**-fanen > **IPsec/IP-filtrering** > **Grunnleggende** > **Gruppepolicy** > **Lokal adresse (skanner)**), kanskje ikke bli oppdaget.

Bruk en statisk IP-adresse.

Datamaskinens IP-adresse har blitt endret eller kan ikke brukes.

Når IP-adressen registrert til den eksterne adressen på Gruppepolicy har blitt endret eller ikke kan brukes, kan ikke IPsec-kommunisering gjennomføres.

Deaktiver IPsec via skannerens kontrollpanel.

Hvis DHCP er utgått, eller omstart eller IPv6-adresse er utgått eller ikke har blitt hentet, vil IP-adressen som er registrert i skannerens Web Config (**Nettverkssikkerhet**-fanen > **IPsec/IP-filtrering** > **Grunnleggende** > **Gruppepolicy** > **Ekstern adresse (vert)**), kanskje ikke bli oppdaget.

Bruk en statisk IP-adresse.

Relatert informasjon

➡ “Kjøre web-konfigurasjon på en nettleser” på side 34

➡ “Kryptert kommunikasjon ved bruk av IPsec/IP-filtrering” på side 102

Kan ikke koble til etter konfigurering av IPsec/IP-filtrering

Innstillingene til IPsec/IP-filtrering er feil.

Deaktiver IPsec/IP-filtrering via skannerens kontrollpanel. Koble sammen skanneren og datamaskinen og still inn IPsec/IP-filtrering på nytt.

Relatert informasjon

➡ “Kryptert kommunikasjon ved bruk av IPsec/IP-filtrering” på side 102

Får ikke tilgang til skanner etter konfigurering av IEEE802.1X

Innstillingene til IEEE 802.1X er feil.

Deaktiver IEEE 802.1X og Wi-Fi fra skannerens kontrollpanel. Koble til skanneren og en datamaskin, og konfigurer deretter IEEE 802.1X igjen.

Koble til skanneren og en datamaskin, og konfigurer deretter IEEE 802.1X igjen.

Relatert informasjon

➡ “Konfigurere et IEEE 802.1X-nettverk” på side 113

Problemer med å bruke et digitalt sertifikat

Kan ikke importere et CA-signert sertifikat

CA-signert sertifikat og informasjonen på CSR samsvarer ikke.

Hvis CA-signert sertifikat og CSR-en ikke har samme informasjon, kan ikke CSR importeres. Kontroller følgende:

❏ Prøver du å importere sertifikatet til en enhet som ikke har den samme informasjonen?
Kontroller informasjonen til CSR-en, og importer deretter sertifikatet til en enhet som har samme informasjon.

❏ Overskrev du CSR-en som var lagret på skanneren etter at du sendte CSR-en til sertifiseringsinstansen?
Hent det CA-signerte sertifikatet på nytt med CSR-en.

CA-signert sertifikat er mer enn 5 kB.

Du kan ikke importere et CA-signert sertifikat som er større enn 5 kB.

Passordet for å importere sertifikatet er feil.

Oppgi riktig passord. Hvis du glemmer passordet, kan du ikke importere sertifikatet. Innhent CA-signert sertifikat på nytt.

Relatert informasjon

➡ "Importere et CA-signert sertifikat" på side 97

Kan ikke oppdatere et selvsignert sertifikat

Vanlig navn har ikke blitt skrevet inn.

Vanlig navn må være angitt.

Det har blitt skrevet inn tegn i Vanlig navn som ikke støttes.

Skriv inn mellom 1 og 128 tegn med enten IPv4, IPv6, vertsnavn eller FQDN-format i ASCII (0x20–0x7E).

Det finnes komma eller mellomrom i fellesnavnet.

Hvis du har skrevet inn et komma, vil **Vanlig navn** være delt på det stedet. Det oppstår en feil hvis du har skrevet inn bare et mellomrom før eller etter et komma.

Relatert informasjon

➡ "Oppdatere et selvsignert sertifikat" på side 99

Kan ikke opprette CSR

Vanlig navn har ikke blitt skrevet inn.

Vanlig navn må være angitt.

Det har blitt skrevet inn tegn i Vanlig navn, Organisasjon, Organisasjonsenhet, Beliggenhet og Stat/provins som ikke støttes.

Skriv inn tegn med enten IPv4, IPv6, vertsnavn eller FQDN-format i ASCII (0x20–0x7E).

Det finnes komma eller mellomrom i Vanlig navn.

Hvis du har skrevet inn et komma, vil **Vanlig navn** være delt på det stedet. Det oppstår en feil hvis du har skrevet inn bare et mellomrom før eller etter et komma.

Relatert informasjon

➡ "Hente et CA-signert sertifikat" på side 95

Det vises en advarsel om digitalt sertifikat

Meldinger	Årsak/Dette skal du gjøre
Skriv inn et Serversertifikat.	**Årsak:** Du har ikke valgt hvilken fil som skal importeres. **Dette skal du gjøre:** Velg filen, og klikk **Importer**.
CA-sertifikat 1 er ikke angitt.	**Årsak:** CA-sertifikat 1 er ikke angitt, og kun CA-sertifikat 2 er angitt. **Dette skal du gjøre:** Importer CA-sertifikat 1 først.
Ugyldig verdi nedenfor.	**Årsak:** Filbanen og/eller passordet inneholder tegn som ikke støttes. **Dette skal du gjøre:** Kontroller at tegnene er riktig angitt for elementet.
Ugyldig dato og klokkeslett.	**Årsak:** Dato og klokkeslett for skanneren er ikke angitt. **Dette skal du gjøre:** Angi dato og klokkeslett ved hjelp av Web Config eller EpsonNet Config.
Ugyldig passord.	**Årsak:** Passordet som er angitt for CA-sertifikatet og angitt passord samsvarer ikke. **Dette skal du gjøre:** Skriv inn riktig passord.

Meldinger	Årsak/Dette skal du gjøre
Ugyldig fil.	**Årsak:** Du importerer ikke en sertifikatfil i X509-format. **Dette skal du gjøre:** Kontroller at du velger riktig sertifikat som er sendt fra en klarert sertifiseringsinstans.
	Årsak: Filen du har importert er for stor. Maksimal filstørrelse er 5 kB. **Dette skal du gjøre:** Hvis du velger riktig fil, kan sertifikatet bli skadet eller forfalsket.
	Årsak: Kjeden i sertifikatet er ugyldig. **Dette skal du gjøre:** Du finner mer informasjon om sertifikatet på nettstedet til sertifiseringsinstansen.
Kan ikke bruke Serversertifikater som inkluderer mer enn tre CA-sertifikater.	**Årsak:** Sertifikatfilen i PKCS#12-format inneholder mer enn 3 CA-sertifikater. **Dette skal du gjøre:** Importer hvert enkelt sertifikat ved å konvertere dem fra PKCS#12-format til PEM-format, eller importer sertifikatfilen i PKCS#12-format som inneholder opptil 2 CA-sertifikater.
Sertifikatet er utløpt. Kontroller at sertifikatet er gyldig, eller kontroller dato og klokkeslett på produktet.	**Årsak:** Sertifikatet er foreldet. **Dette skal du gjøre:** ❏ Hvis sertifikatet er foreldet, må du hente og importere det nye sertifikatet. ❏ Hvis sertifikatet ikke er foreldet, kontrollerer du at skannerens dato og klokkeslett er riktig angitt.
Privat nøkkel kreves.	**Årsak:** Det finnes ingen paret privatnøkkel med sertifikatet. **Dette skal du gjøre:** ❏ Hvis sertifikatet er i PEM/DER-format og det er hentet fra en CSR ved hjelp av en datamaskin, angir du filen for privatnøkkelen. ❏ Hvis sertifikatet er i PKCS#12-format og det er hentet fra en CSR ved hjelp av en datamaskin, oppretter du en fil som inneholder privatnøkkelen.
	Årsak: Du har importert PEM/DER-sertifikatet du hentet fra en CSR på nytt ved hjelp av Web Config. **Dette skal du gjøre:** Hvis sertifikatet er i PEM/DER-format og det er hentet fra en CSR ved hjelp av Web Config, kan du bare importere det én gang.

Meldinger	Årsak/Dette skal du gjøre
Innstilling mislykket.	**Årsak:** Kan ikke fullføre konfigurasjonen fordi kommunikasjonen mellom skanneren og datamaskinen mislyktes eller filen ikke kan leses pga. feil. **Dette skal du gjøre:** Når du har kontrollert angitt fil og kommunikasjon, importerer du filen på nytt.

Relatert informasjon

➡ "Om digital sertifisering" på side 95

Slette et CA-signert sertifikat ved et uhell

Det finnes ingen sikkerhetskopifil for det CA-signerte sertifikatet.

Hvis du har sikkerhetskopifilen, kan du importere sertifikatet på nytt.

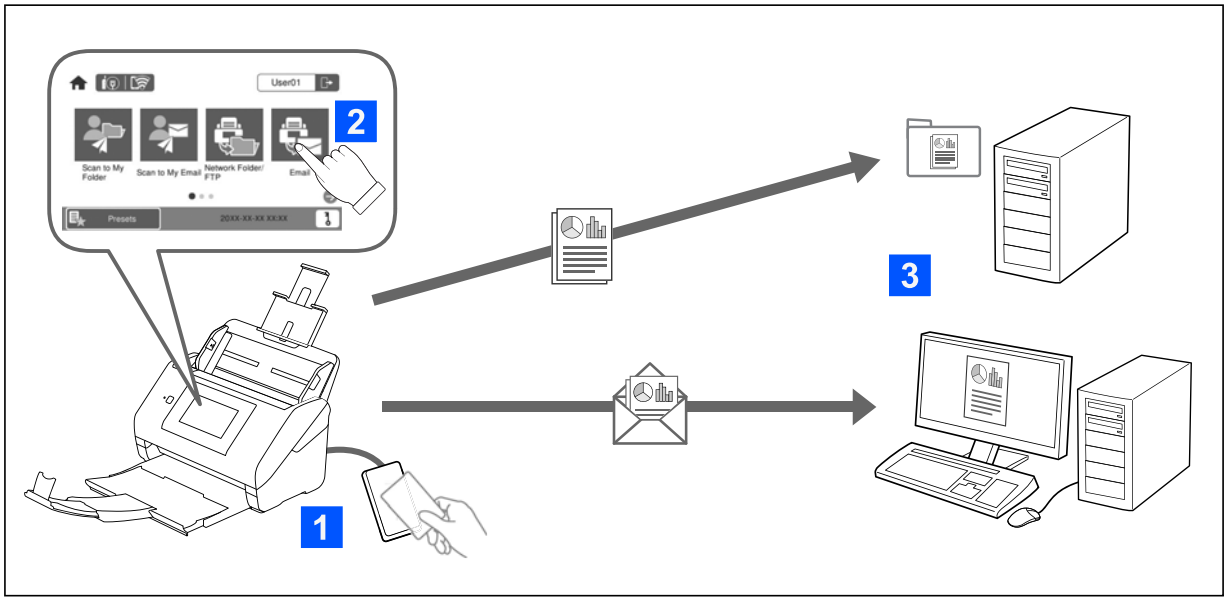
Hvis du henter et sertifikat med en CSR som er opprettet fra Web Config, kan du ikke importere et slettet sertifikat på nytt. Opprett en CSR, og hent et nytt sertifikat.

Relatert informasjon

➡ "Importere et CA-signert sertifikat" på side 97
➡ "Slette et CA-signert sertifikat" på side 98

Godkjenningsinnstillinger

Om Godkjenningsinnstillinger



Når Godkjenningsinnstillinger er aktivert, kreves brukergodkjenning før skanning. Du kan angi hvilke skannemetoder som kan brukes av hver bruker, og forhindre utilsiktede operasjoner.

Du kan spesifisere e-postadressen til godkjente brukere som skannemålet (Skann til min e-post), eller lagre hver brukers data i en personlig mappe (Skann til min mappe). Du kan også spesifisere andre skannemetoder.

Merknad:

❏ *Du kan ikke skanne fra en datamaskin eller en smartenhet når Godkjenningsinnstillinger er aktivert.*

❏ *I tillegg til disse Godkjenningsinnstillinger som ble introdusert i denne bruksanvisningen, kan du også bygge et godkjenningssystem med en godkjenningsserver. For å bygge et system bruker du Document Capture Pro Server Authentication Edition (det forkortede navnet er Document Capture Pro Server AE). Kontakt ditt lokale Epson kontor for ytterligere informasjon.*

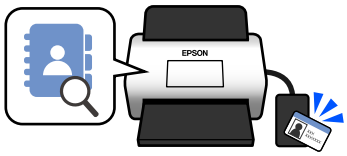
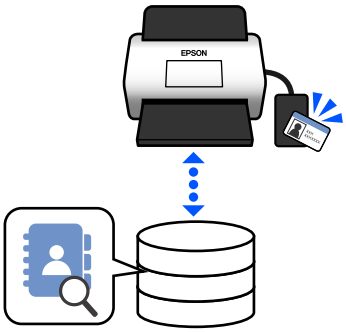
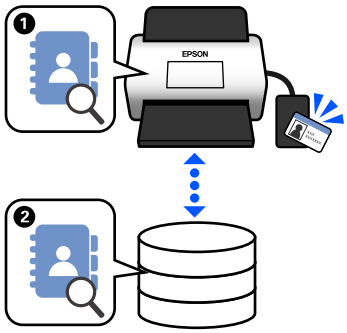
Tilgjengelige funksjoner for Godkjenningsinnstillinger

Skannefunksjoner på kontrollpanelet	Godkjenningsinnstillinger	
	Når aktivert	Når deaktivert
Skann til min mappe Lagrer bilder i mappen som er tilordnet den godkjente brukeren.	✓	-
Skann til min e-post Sender bilder til e-postadressen til den godkjente brukeren.	✓	-
Skann t. nettverksmappe/FTP Lagrer bilder i en mappe på et nettverk.	✓	✓

Skannefunksjoner på kontrollpanelet	Godkjenningsinnstillinger	
	Når aktivert	Når deaktivert
Skann til datamaskin Lagrer bilder på en tilkoblet datamaskin som bruker jobber opprettet i Document Capture Pro (Windows)/Document Capture (Mac OS). * Når Godkjenningsinnstillinger er aktivert, kan du bare bruke jobber som er registrert i **Forhåndsinns**.	✓*	✓
Skann til e-post Sender bilder til e-postadressen du har angitt.	✓	✓
Skann til nettsky Sender bilder til skytjenesten du har angitt.	✓	✓
Skann til USB-stasjon Lagrer bilder på en USB-stasjon som er koblet til skanneren. Dette er kun tilgjengelig når ingen autentiseringsenhet er koblet til skanneren.	✓	✓
Skann til WSD Lagrer bilder på en tilkoblet datamaskin gjennom WSD-funksjonen.	-	✓
Forhåndsinns Du kan registrere opp til 48 forhåndsinnstillinger for skanning. Du kan tilordne opptil fem Forhåndsinns til brukere som er registrert i Lokal DB. Tilordnede Forhåndsinns er bare tilgjengelige for den bestemte brukeren. Forhåndsinns som ikke er tilordnet en bruker, kan brukes av alle brukere.	✓	✓

Om Godkjenningsmetode

Denne skanneren tilbyr godkjenning med følgende metoder, uten å måtte bygge en godkjenningsserver.

	Lokal DB	LDAP	Lokal DB og LDAP
Plassering en til brukerinformasjon	**Skannerens minne** Denne godkjenningsmetoden sjekker brukerinformasjonen som er registrert i skanneren og sammenligner den med brukeren som bruker skannefunksjonen.	**LDAP-server*** Denne godkjenningsmetoden kontrollerer brukerinformasjonen til LDAP-serveren som er synkronisert med skanneren. Siden opptil 300 elementer med brukerinformasjon fra LDAP-serveren kan lagres midlertidig i skanneren som hurtigbuffer, kan du utføre en godkjenning med hurtigbufferen hvis LDAP-serveren er nede. * En server som leverer en katalogtjeneste som kan kommunisere med LDAP.	**Skannerens minne og LDAP-serveren** Sjekk brukerinformasjonen som er registrert i skanneren først (❶), og hvis den ikke finner en match, kan du sjekke informasjonen med LDAP-serveren (❷).
			
Antall registrerte brukere	50 (skannerens minne)	Ubegrenset (LDAP-server)	50 (skannerens minne) Ubegrenset (LDAP-server)
Skannerens hurtigbufferminne	-	300	Maks. 300 (50 av hurtigbuffersporene deles med Brukerinnstillinger i Lokal DB)
Påloggingsmetoder	Du kan bruke en av de følgende metodene. ❏ Presenter et godkjenningskort, eller skriv inn en **Bruker-ID** og et **Passord** ❏ Presenter et godkjenningskort, eller skriv inn et **ID-nummer** ❏ Skriv inn en **Bruker-ID** og et **Passord** ❏ Skriv inn en **Bruker-ID** ❏ Skriv inn et **ID-nummer**		
Begrenser «Skann til»-funksjonen	Angi individuelt for hver bruker	Samme innstillinger for alle LDAP-brukerne	Lokal DB-brukere: angi individuelt LDAP-brukere: samme innstillinger for alle brukerne
Tilordne Forhåndsinns til brukere	Opptil fem per bruker	- (Kan ikke angis individuelt)	Lokal DB-bruker: opptil fem per bruker LDAP-brukere: -

Programvare for å konfigurere

Konfigurer med Web Config eller Epson Device Admin.

❏ Ved bruk av Web Config kan du konfigurere skanneren kun ved hjelp av en nettleser.
"Web Config" på side 34

❏ Ved bruk av Epson Device Admin kan du konfigurere flere skannere på en gang med en konfigurasjonsmal.
"Epson Device Admin" på side 35

Oppdatere skannerens fastvare

Før du aktiverer Godkjenningsinnstillinger, må du oppdatere skannerens fastvare til den nyeste versjonen. Koble skanneren til internett på forhånd.

Forsiktighetsregel:
Ikke slå av datamaskinen eller skanneren under oppdatering.

Når du konfigurerer fra Web Config:

Velg fanen **Enhetsadministrasjon** > **Fastvareoppdatering** og følg instruksene på skjermen for å oppdatere fastvaren.

Når du konfigurerer fra Epson Device Admin:

Velg **Home** > **Firmware** > **Update** på listen over enheter og følg instruksene på skjermen for å oppdatere fastvaren.

Merknad:
Hvis den siste fastvaren allerede er installert, trenger du ikke å oppdatere den.

Koble til og konfigurere en godkjenningsenhet

Hvis du vil koble til og bruke en godkjenningsenhet, som en IC-kortleser, må du først konfigurere enheten. Dette er ikke nødvendig hvis du ikke bruker en godkjenningsenhet.

Relatert informasjon

➡ "Koble til en godkjenningsenhet" på side 129
➡ "Innstillinger for autentiseringsenhet" på side 130

Liste over kompatible kortlesere

Denne listen garanterer ikke driften til kortleserne i listen.

Ja: støttes (ID-informasjonen kan leses med standard innstillinger for kortlesere.)

Nei: ikke kompatibel

Produsent	Modell	Modellnummer	Godkjenningskort							Modus
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
RF IDEAS	pcProx Plus	RDR-80081AKU	Ja	Ja[*1]	Ja[*1]	Ja[*1]	Nei	Nei	Nei	Tastatur
RF IDEAS	pcProx	RDR-7081BKU	Ja[*1]	Nei	Ja	Ja	Nei	Nei	Nei	Tastatur
RF IDEAS	pcProx	RDR-7581AKU	Ja	Nei	Ja[*1]	Ja[*1]	Nei	Nei	Nei	Tastatur
ELATEC	TWN3 MIFARE	T3DT-MB2BEL T3DT-MB2WEL	Nei	Nei	Ja	Ja	Nei	Nei	Nei	Tastatur
ELATEC	TWN3 MIFARE NFC	T3DT-FB2BEL T3DT-FB2WEL	Ja	Nei	Ja	Ja	Ja	Ja	Ja	Tastatur
ELATEC	TWN4 MULTI-TECH	T4DT-FB2BEL-PI T4DT-FB2WEL-PI	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Tastatur
ELATEC	TWN4 Multi-Tech 2 BLE-PI	T4LK-FB4BLZ-PI	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Tastatur
ELATEC	TWN4 Slim	T4QC-FC3B7	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Tastatur
HID Global	OMNIKEY 5427	OMNIKEY5427CK OMNIKEY5427CK gen2	Ja	Ja	Ja	Ja	Ja	Nei	Ja	Tastatur[*1]
ACS	ACR122U	ACR122U	Nei	Nei	Ja[*2]	Ja[*2]	Ja	Nei	Ja[*2]	PC/SC

Produsent	Modell	Modellnummer	Godkjenningskort							Modus
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
ACS	ACR1252	ACR1252	Nei	Nei	Ja*2	Ja*2	Ja	Ja	Ja*2	PC/SC
Sony	PaSoRi	RC-S330/S	Nei	Nei	Ja*2	Ja*2	Ja*2	Ja*2	Ja*2	PaSoRi
Sony	PaSoRi	RC-S380/P RC-S380/S	Nei	Nei	Ja*2	Ja*2	Ja*2	Ja*2	Ja*2	PaSoRi
DMZ	Leitor RFID Universal	DMZ008	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Tastatur
DMZ	Leitor RFID Multi-125	DMZ087	Nei	Ja	Nei	Nei	Nei	Nei	Nei	Tastatur
DMZ	Leitor RFID Mifare	DMZ088	Nei	Nei	Ja	Ja	Nei	Nei	Nei	Tastatur
DMZ	Biometric & RFID Reader	DMZ073	Nei	Ja	Nei	Nei	Nei	Nei	Nei	Tastatur
inepro	SCR708	SCR708	Ja*1	Ja*1	Ja*1	Ja*1	Ja*1	Ja*1	Ja*1	Tastatur
Y Soft	YU030888 001	MU0388	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Tastatur
Cartadis	TCM3 Cartadis MiFare Card Reader	ZTCM3-MIFARE	Nei	Nei	Ja	Ja	Nei	Nei	Ja	Tastatur
MICI Network Co., Ltd.	EM & Mifare Card Reader	mCR-600	Nei	Nei	Ja	Ja	Nei	Nei	Ja	Tastatur

Produsent	Modell	Modellnummer	Godkjenningskort							Modus
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/Lite-S		
NT-ware	MiCard Multi-Tech4-PI	T4DT-FB4WUF-PI	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Tastatur
NT-ware	MiCard Plus-2-V2	RDR-80081AGU-NT2-20	Ja*1	Ja*1	Ja*1	Ja*1	Nei	Nei	Nei	Tastatur
NT-ware	MiCard V3 Multi	MiCard V3 Multi	Ja	Ja	Ja	Ja	Ja	Ja	Nei	Tastatur

*1 Du må endre innstillingene til kortleseren ved å bruke produsenten av kortleserens egen programvare.

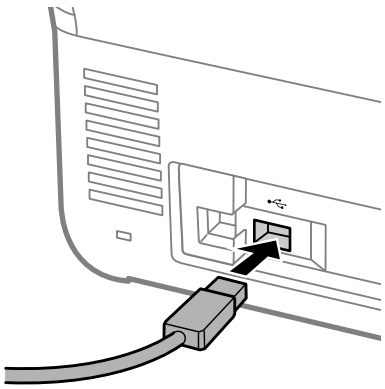
*2 Hvis du må konfigurere produktinnstillingene for å bruke data fra et spesielt område på kortet som ikke er standard ID for kortet som en godkjennings-ID, kan du ta kontakt med Epson-partneren eller en lokal representant om mer informasjon om hvordan du kan konfigurere produktet.

Koble til en godkjenningsenhet

Forsiktighetsregel:

Når du kobler godkjenningsenheten til flere skannere, må du bruke et produkt med samme modellnummer.

Koble kortleserens USB-kabel til USB-porten for eksterne grensesnitt på skanneren.



Driftssjekk for godkjenningsenheter

Du kan sjekke tilkoblingsstatusen og gjenkjenning av godkjenningskortet for godkjenningsenheten fra skannerens kontrollpanel.

Informasjonen vises når du velger **Innst.** > **Enhetsinformasjon** > **Status for godkjenningsenhet**.

Innstillinger for autentiseringsenhet

Angi leseformat for godkjenningsinformasjon som mottas fra et godkjenningskort.

Du kan angi følgende lesemetode for autentiseringsenheten.

❏ Les det bestemte området på godkjenningskortet, for eksempel ansattnummer eller personlig ID-nummer.

❏ Bruk godkjenningskortinformasjonen med unntak av UID (informasjon som for eksempel serienummer).

Du kan bruke et verktøy til å generere valgfrie parametere. Spør forhandleren din hvis du vil ha mer informasjon.

Merknad:
Bruke godkjenningskort fra ulike produsenter:

Når du bruker UID-kortinformasjon (kort-ID-informasjon, som serienummeret), kan du bruke en blanding av ulike typer godkjenningskort. Dette kan ikke blandes når det brukes annen kortinformasjon.

Når du konfigurerer fra Web Config:

Velg **Enhetsadministrasjon**-fanen > **Kortleser**.

Når du konfigurerer fra Epson Device Admin:

Velg **Administrator Settings** > **Authentication Settings** > **Card Reader** fra konfigurasjonsmalen.

Element	Forklaring
Vendor ID	Angi leverandør-ID for autentiseringsenheten som begrenser bruk fra 0000 til FFFF med fire alfanumeriske tegn. Skriv 0000 hvis du ikke ønsker å begrense denne.
Product ID	Angi produkt-ID for autentiseringsenheten som begrenser bruk fra 0000 til FFFF med fire alfanumeriske tegn. Skriv 0000 hvis du ikke ønsker å begrense denne.
Driftsparameter	Angi driftsparameter for autentiseringsenheten mellom 0 og 8192 tegn. A–Z, a–z, 0–9, +, /, =, mellomrom og linjeskift er tilgjengelig.
Kortleser	Velg konverteringsformat for autentiseringsenheten. Du kan sjekke formatdetaljene. Se koblingen som er inkludert i elementbeskrivelsen.
Lagringsformat for Godkjenningskort-ID	Velg konverteringsformat for godkjenningsinformasjonen til et ID-kort. Du kan sjekke formatdetaljene. Se koblingen som er inkludert i elementbeskrivelsen.
Sett kort-ID-område	Aktiver spesifikasjon av leseposisjonen.
Startplassering for tekst	Spesifiser tekst-startposisjonen for å lese ID-informasjonen. Du kan angi mellom 1 og 4096.
Antall tegn	Spesifiser antallet tegn som skal leses fra startposisjonen til ID-informasjonen. Du kan angi mellom 1 og 4096.

Registrere og stille inn informasjon

Konfigurere

Angi de nødvendige innstillingene, avhengig av Godkjenningsmetode og skanningsmetoden som brukes.

Forsiktighetsregel:

Før du begynner konfigureringen, må du kontrollere at tidsinnstillingen til skanneren er riktig.

Hvis tidsinnstillingen er feil, vises feilmeldingen «Lisens utgått», som kan føre til konfigurasjonsfeil for skanneren. For å kunne bruke en sikkerhetsfunksjon som SSL/TLS-kommunikasjon eller IPsec, må i tillegg riktig klokkeslett være angitt. Du kan konfigurere klokkeslettet på følgende vis.

- ❏ *Web Config:* ***Enhetsadministrasjon****-fanen >* ***Dato og klokkeslett*** *>* ***Dato og klokkeslett****.*
- ❏ *Skannerens kontrollpanel:* ***Innst.*** *>* ***Basisinnstillinger*** *>* ***Innstillinger dato/kl.****.*

Innstillinger	Lokal DB	LDAP	Lokal DB og LDAP
Aktivere godkjenning Du må aktivere godkjenning før du kan angi godkjenningsinnstillinger. "Aktivere godkjenning" på side 132	✓	✓	✓
Godkjenningsinnstillinger Konfigurere Godkjenningsmetode og hvordan du godkjenner brukeren. "Godkjenningsinnstillinger" på side 132	✓	✓	✓
Registrere Brukerinnstillinger Registrer innstillingene for hver bruker. Du kan også masseregistrere brukere med en CSV-fil. "Registrere Brukerinnstillinger" på side 133	✓	–	✓
Synkronisere med LDAP-server Angi synkroniseringsinnstillingene for LDAP-serveren. "Synkronisere med LDAP-server" på side 140	–	✓	✓
Konfigurere E-postserver Angi innstillingene for e-postserveren. Angi dette når du bruker funksjoner som krever innstillinger som Skann til min e-post i e-postserveren. "Konfigurere e-postserveren" på side 143	✓	✓	✓
Konfigurere Skann til min mappe Angi målmapper. Angi dette når du bruker Skann til min mappe-funksjonen. "Angi Skann til min mappe" på side 144	✓	✓	✓

Innstillinger	Lokal DB	LDAP	Lokal DB og LDAP
Tilpass Ett-trykksfunksjoner Konfigurer dette når du endrer elementene som vises på skannerens kontrollpanel. Du kan vise kun ikonene du trenger på kontrollpanelet, eller endre rekkefølgen til ikonene. "Tilpass Ett-trykksfunksjoner" på side 146	✓	✓	✓

Aktivere godkjenning

Du må aktivere godkjenning før du kan angi godkjenningsinnstillinger.

Når du konfigurerer fra Web Config:

Velg **På (enhet/LDAP-server)** fra fanen **Produktsikkerhet** > **Grunnleggende** > **Godkjenning**.

Når du konfigurerer fra Epson Device Admin:

Fra konfigurasjonsmalen, velger du **På (enhet/LDAP-server)** fra **Administrator Settings** > **Authentication Settings** > **Basic** > **Authentication**.

Merknad:
Hvis du aktiverer Godkjenningsinnstillinger på skanneren, Låsinnstilling er det også aktivert for kontrollpanelet. Kontrollpanelet kan ikke låses opp når Godkjenningsinnstillinger er aktivert.

Selv om du deaktiverer Godkjenningsinnstillinger, forblir Låsinnstilling aktivert. Hvis du vil deaktivere det, kan du stille dette inn fra kontrollpanelet eller Web Config.

Relatert informasjon

➡ "Konfigurere Låsinnstilling fra kontrollpanelet" på side 83
➡ "Angi Låsinnstilling fra Web Config" på side 83

Godkjenningsinnstillinger

Konfigurere Godkjenningsmetode og hvordan du godkjenner brukeren.

Når du konfigurerer fra Web Config:

Velg **Produktsikkerhet**-fanen > **Godkjenningsinnstillinger**.

Når du konfigurerer fra Epson Device Admin:

Velg **Administrator Settings** > **Authentication Settings** > **Authentication Settings** fra konfigurasjonsmalen.

Element	Forklaring
Godkjenningsmetode	Velg Godkjenningsmetode. ❏ Lokal DB Godkjenn med Brukerinnstillinger som er registrert på skanneren. Brukeren må registreres på skanneren. ❏ LDAP Godkjenn med brukerinformasjonen på LDAP-serveren som er synkronisert med skanneren. Du må konfigurere innstillingene for LDAP-serveren på forhånd. ❏ Lokal DB og LDAP Godkjenn med brukerinformasjonen registrert på skanneren eller LDAP-serveren som er synkronisert med skanneren. Du må registrere brukeren på skanneren og LDAP-serveren må konfigureres.
Slik godkjenner du brukeren	Velg hvordan en bruker skal godkjennes. ❏ Kort eller Bruker-ID og passord Bruk et godkjenningskort til å godkjenne brukere. Du kan også benytte bruker-ID og passord for å godkjenne. ❏ Bruker-ID og passord Benytt bruker ID og passord til å godkjenne brukere. Du kan ikke bruke godkjenningskort til å godkjenne når du velger denne funksjonen. ❏ Bruker-ID Bruk kun ID-kort til å godkjenne brukere. Du må ikke angi passord. ❏ Kort eller ID-nummer Bruk et godkjenningskort til å godkjenne brukere. Du kan også bruke ID-nummer. ❏ ID-nummer Bruk kun ID-nummer til å godkjenne brukere.
Tillat brukere å registrere godkjenningskort	Aktiver for å la brukere registrere godkjenningskortet til systemet. Hvis du velger **LDAP** for **Godkjenningsmetode**, kan du ikke angi dette. For mer informasjon om hvordan brukere kan registrere autentiseringskortene sine, kan du se «Registrere et godkjenningskort» i *Brukerhåndbok*.
Minimum antall sifre for ID-nummer	Velg minimum antall sifre for ID-nummeret.
Hurtigbufring for LDAP-godkjente brukere	Når du bruker LDAP-servergodkjenning, kan du stille inn hvorvidt hurtigbuffer skal brukes for brukerinformasjon.
Brukerinformasjon i SMTP-godkjenning	Når bruker-ID og passord brukes til godkjenning, kan du angi hvorvidt brukerinformasjonen skal brukes til SMTP-godkjenning. Systemet bruker bruker-ID-en og passordet fra siste pålogging.
Restriksjoner for LDAP-godkjente bruker	Hvis du bruker LDAP, kan du angi funksjonene som skal være tilgjengelige for brukeren.

Registrere Brukerinnstillinger

Registrer Brukerinnstillinger som ble brukt til brukergodkjenning. Du kan registrere med en av de følgende metodene.

❏ Registrere en Brukerinnstillinger om gangen (Web Config)

❏ Registrere flere Brukerinnstillinger om gangen med en CSV-fil (Web Config)

❏ Registrere User Settings på flere skannere som en pakke ved hjelp av en konfigurasjonsmal (Epson Device Admin)

Relatert informasjon

➡ "Registrere Brukerinnstillinger individuelt (Web Config)" på side 134

➡ "Registrere flere Brukerinnstillinger med en CSV-fil (Web Config)" på side 135

➡ "Registrere User Settings på flere skannere som en pakke (Epson Device Admin)" på side 138

Registrere Brukerinnstillinger individuelt (Web Config)

Åpne Web Config og velg fanen **Produktsikkerhet** > **Brukerinnstillinger** > **Legg til**, og gå til Brukerinnstillinger.

Element	Forklaring
Bruker-ID	Skriv inn bruker-ID-en du vil bruke for autentisering innenfor 1 til 83 bytes, som kan uttrykkes i Unicode (UTF-8). Bruker-ID skiller ikke mellom store og små bokstaver, så du kan logge på med begge deler.
Brukernavnvisning	Angi brukernavnet som vises på skannerens kontrollpanel inntil 32 tegn, som kan uttrykkes i Unicode (UTF-16). Dette kan stå tomt.
Passord	Angi passordet du vil bruke til godkjenning inntil 32 tegn i ASCII. Det er forskjell på store og små bokstaver i passordet. La dette stå tomt hvis du velger **Bruker-ID** for **Slik godkjenner du brukeren**.
Godkjenningskort-ID	Angi ID for godkjenningskortet som skal brukes til godkjenning inntil 116 tegn i ASCII. Dette kan stå tomt. Hvis du tillater **Tillat brukere å registrere godkjenningskort** for **Godkjenningsinnstillinger**, gjenspeiles resultatet som registreres av brukere.
ID-nummer	Dette elementet vises når **Kort eller ID-nummer** eller **ID-nummer** velges i **Godkjenningsinnstillinger** > **Slik godkjenner du brukeren**. Angi et tall som er inkludert i tallsettet i **Godkjenningsinnstillinger** > **Minimum antall sifre for ID-nummer** og som består av opptil åtte siffer.
Generer automatisk	Dette elementet vises når **Kort eller ID-nummer** eller **ID-nummer** velges i **Godkjenningsinnstillinger** > **Slik godkjenner du brukeren**. Klikk for automatisk å generere et ID-nummer med samme antall siffer som det du valgte i **Minimum antall sifre for ID-nummer**.
Avdeling	Angi avdelingsnavnet og så videre som identifiserer brukeren inntil 40 tegn som kan uttrykkes i Unicode (UTF-16). Dette kan stå tomt.
E-postadresse	Angi brukerens e-postadresse inntil 200 tegn i ASCII. Dette brukes som målet for **Skann til min e-post**. Dette kan stå tomt.

Element	Forklaring
Skann til min mappe	Lagre målene individuelt når du velger **Individuell** i **Skann til min mappe** > **Innstillingstype**. Se følgende for mer informasjon om innstillingselementene. "Angi Skann til min mappe" på side 144
Begrensninger	Du kan begrense funksjonene for hver bruker. Velg funksjonen du tillater å bruke.
Forhåndsinnstillinger	Du kan stille inntil fem forhåndsinnstillinger som bare er tilgjengelige for den valgte brukeren fra Forhåndsinnstillinger som er registrert på skanneren. ❏ Forhåndsinnstillinger som ble tilordnet en bruker kan bare brukes av denne brukeren. Forhåndsinnstillinger som ikke er tilordnet en bruker, kan brukes av alle brukere. ❏ Hvis en bruker har tilgang til én Forhåndsinnstillinger, blir den automatisk lastet inn etter autentisering. Hvis flere Forhåndsinnstillinger er tilgjengelige, vises en liste over Forhåndsinnstillinger etter autentiseringen. ❏ Du kan ikke lage eller vise Forhåndsinnstillinger som bruker funksjoner som er begrenset i **Begrensninger**.

Registrere flere Brukerinnstillinger med en CSV-fil (Web Config)

Angi innstillingene for hver bruker i en CSV-fil og registrer dem som en pakke.

Opprette en CSV-fil

Opprett en CSV-fil for å importere Brukerinnstillinger.

Merknad:
Hvis du registrerer én eller flere Brukerinnstillinger på forhånd og deretter eksporterer en formattert fil (CSV-fil), kan du bruke de registrerte innstillingene som en referanse for å angi innstillingselementer.

1. Gå inn på Web Config og velg **Produktsikkerhet**-fanen > **Brukerinnstillinger**.
2. Klikk på **Eksporter**.
3. Velg filformatet for **Filformat**.

   Velg ved å se under.

Element	Forklaring
CSV UTF-16 (tabulatordelt)	Velg når du redigerer filen med Microsoft Excel. Alle parameterne er innelukket av «[ ]» (klammeparenteser). Angi parametrene i «[ ]». Vi anbefaler å overskrive filen når du oppdaterer den. Hvis du nylig har lagret filen, velger du Unicode-teskt (*.txt) som filformat.
CSV UTF-8 (kommadelt)	Velg når du redigerer filen med et tekstredigeringsprogram eller en makro, uten Microsoft Excel.
CSV UTF-8 (semikolondelt)	

4. Klikk på **Eksporter**.

5. Rediger og lagre denne CSV-filen i et regnearkprogram som Microsoft Excel eller et tekstredigeringsprogram.

> ***Forsiktighetsregel:***
> *Ikke endre koding eller tittelinformasjon når du endrer filen.*

Innstillingselementer for CSV-fil

Element	Innstillinger og forklaring
UserID	Angi bruker-ID som skal brukes til godkjenning mellom 1 og 83 byte i Unicode.
UserName	Angi brukernavnet som vises på skannerens kontrollpanel inntil 32 tegn i Unicode. Dette kan stå tomt.
Password	Angi passordet som skal brukes til godkjenning inntil 32 tegn i ASCII. Ved importering er dette satt som passord i stedet for **EncPassword**. La dette stå tomt hvis du velger **Bruker-ID** for **Slik godkjenner du brukeren**. Ved eksportering er dette alltid tomt.
AuthenticationCardID	Angi leseresultat for godkjenningskortet. Når du tillater **Tillat brukere å registrere godkjenningskort** i **Godkjenningsinnstillinger**, gjenspeiles resultatet som registreres av brukerne. Skriv inntil 116 tegn i ASCII. Dette kan stå tomt.
IDNumber	Dette elementet vises når **Kort eller ID-nummer** eller **ID-nummer** velges i **Godkjenningsinnstillinger** > **Slik godkjenner du brukeren**. Angi et tall som er inkludert i tallsettet i **Godkjenningsinnstillinger** > **Minimum antall sifre for ID-nummer** og som består av opptil åtte siffer. Du kan ikke duplisere et ID-nummer. Ved duplisering vil du få varsel om feilen ved importering av filen. Når det er tomt, blir et nummer automatisk tildelt.
Department	Angi avdelingsnavnet vilkårlig for å skille brukerne fra hverandre. Skriv inntil 40 tegn i Unicode. Dette kan stå tomt.
MailAddress	Angi e-postadressen til brukerne. Dette brukes som målet for **Skann til min e-post**. Du kan bruke A-Z, a-z, 0-9, !#'%&'*+-./=?^_{|}~@. Skriv inn maksimalt 200 tegn. Du kan ikke bruke «,» (komma) som første tegn. Dette kan stå tomt.
FolderProtocol	Angi typen for Skann til min mappe-funksjon. Nettverksmappe/FTP (SMB): 0, FTP: 1
FolderPath	Angi lagringsmål for Skann til min mappe-funksjonen.
FolderUserName	Angi brukernavn for Skann til min mappe-funksjonen.
FolderPassword	Angi et passord for å godkjenne målmappen for Skann til min mappe-funksjonen på inntil 32 ASCII-tegn. Ved importering er dette satt som passord i stedet for **EncPassword**. Ved eksportering er dette alltid tomt.
FtpPassive	Angi tilkoblingsmodus for FTP-serveren når **FTP** er valgt som **Type** for Skann til min mappe-funksjonen. Aktiv modus: 0, passiv modus: 1

Element	Innstillinger og forklaring
FtpPort	Angi portnummer for å sende skannede data til FTP-serveren mellom 0 og 65535 når **FTP** er valgt som **Type** for Skann til min mappe-funksjonen.
ScanToMemory	Angi restriksjoner for Skann til USB-stasjon. Ikke tillatt: 0, tillatt: 1
ScanToMail	Angi restriksjoner for Skann til e-post. Du kan bare angi **Skann til min e-post** når **Skann til e-post** er aktivert. Ikke tillatt: 0, tillatt: 1
ScanToFolder	Angi restriksjoner for Skann til nettverksmappe /FTP. Du kan bare angi **Skann til min mappe** når **Skann til nettverksmappe /FTP** er aktivert. Ikke tillatt: 0, tillatt: 1
ScanToCloud	Angi restriksjoner for Skann til nettsky. Ikke tillatt: 0, tillatt: 1
ScanToComputer	Angi restriksjoner for Skann til datamaskin. Ikke tillatt: 0, tillatt: 1
PresetIndex	Angi Forhåndsinnstillinger som du vil knytte til brukeren. Du kan angi opptil fem Forhåndsinnstillinger-registreringsnumre adskilt med komma.
EncPassword	Ved eksportering av brukerinnstillinger krypteres parameteren angitt for **Password**, og deretter kodes verdien av BASE64 og utdata. Ved importering med det nye passordet for **Password**, blir denne verdien ignorert. Hvis **Password** står tomt, brukes denne verdien og passordet blir det samme som før eksportering.
EncFolderPassword	Ved eksportering krypteres parameteren angitt for **FolderPassword**, og deretter kodes verdien av BASE64 og utdata. Ved importering med det nye passordet for **FolderPassword**, blir denne verdien ignorert. Hvis **FolderPassword** står tomt, brukes denne verdien og passordet blir det samme som før eksportering.

Importere en CSV-fil

1. Gå inn på Web Config og velg **Produktsikkerhet**-fanen > **Brukerinnstillinger**.
2. Klikk på **Importer**.
3. Velg filen du ønsker å importere.
4. Klikk på **Importer**.
5. Etter kontrollering av informasjonen som vises, klikk **OK**.

Registrere User Settings på flere skannere som en pakke (Epson Device Admin)

Du kan registrere User Settings som ble brukt i Lokal DB som en pakke ved å bruke en LDAP-server eller en CSV-/ENE-fil.

Merknad:
*En ENE-fil er en binær fil levert av Epson som krypterer og lagrer informasjon for **Contacts**, som personopplysninger og Brukerinnstillinger. Den kan eksporteres fra Epson Device Admin og du kan angi et passord. Dette er nyttig når du ønsker å importere Brukerinnstillinger fra sikkerhetskopifilen.*

Importere fra CSV-/ENE-fil

1. Velg **Administrator Settings** > **Authentication Settings** > **User Settings** fra konfigurasjonsmalen.
2. Klikk på **Import**.
3. Velg **CSV or ENE File** under **Import Source**.
4. Klikk på **Browse**.

   Skjermbildet for filvalg vises.
5. Velg filen du vil importere for å åpne den.
6. Velg en importmetode.
   - ❏ Overwrite and Add: skriver over hvis samme bruker-ID finnes, legger til ny ID hvis den ikke finnes.
   - ❏ Replace All: erstatter alt med brukerinnstillingene du vil importere.
7. Klikk på **Import**.

   Bekreftelsesskjermbildet for innstillinger vises.
8. Klikk på **OK**.

   Valideringsresultatet vises.

   Merknad:
   - ❏ *Hvis antallet importerte brukerinnstillinger overskrider antallet som kan importeres, vises en melding som ber deg slette noen av brukerinnstillingene. Slett overflødige brukerinnstillinger før du importerer.*
   - ❏ *Velg brukerinnstillingene du vil slette før du importerer, og klikk deretter på **Delete**.*
9. Klikk på **Import**.

   Brukerinnstillingene importeres til konfigurasjonsmalen.

Importere fra LDAP-serveren

1. Velg **Administrator Settings** > **Authentication Settings** > **User Settings** fra konfigurasjonsmalen.
2. Klikk på **Import**.

3. Velg **LDAP** under **Import Source**.

4. Klikk på **Settings**.

   LDAP Server-innstillingene vises.

   Merknad:
   Denne LDAP-serverinnstillingen importerer brukerinnstillinger fra LDAP-serveren. De importere (kopierte) brukerinnstillingene brukes til å godkjenne brukere med skanneren.

   *På den andre siden, når du velger **LDAP** eller **Local DB and LDAP** som godkjenningsmetoden, godkjennes brukerne ved å kommunisere med LDAP-serveren.*

5. Still inn hvert element.

   Når du importerer brukerinnstillinger fra en LDAP-server, kan du konfigurere de følgende innstillingene i tillegg til LDAP-innstillingene.

   Se relatert informasjon for andre elementer.

Element			Forklaring
LDAP Server Settings	LDAP Server Type		Lar deg velge typen LDAP-server.
Search Settings	Search Filter		Du kan angi teksten som brukes for LDAP-søkefilteret. Velg **Custom** for å redigere søketeksten.
	Options	Type	Du kan angi typen lagringsmål for **Scan To My Folder**.
		Connection Mode	Når **Type** er angitt som **FTP**, kan du angi FTP-tilkoblingsmetoden.
		Port Number	Når **Type** er angitt som **FTP**, kan du angi portnummeret du vil bruke.

6. Utfør tilkoblingstesten etter behov ved å klikke **Connection Test**.

   Henter og viser 10 brukerinnstillinger fra LDAP-serveren.

7. Klikk på **OK**.

8. Velg en importmetode.

   ❏ Overwrite and Add: skriver over hvis samme bruker-ID finnes, legger til ny ID hvis den ikke finnes.

   ❏ Replace All: erstatter alt med brukerinnstillingene du vil importere.

9. Klikk på **Import**.

   Bekreftelsesskjermbildet for innstillinger vises.

10. Klikk på **OK**.

    Valideringsresultatet vises.

11. Klikk på **Import**.

    Brukerinnstillingene importeres til konfigurasjonsmalen.

Relatert informasjon

➡ "Konfigurere en LDAP-server" på side 140
➡ "Konfigurere søkeinnstillinger for LDAP-serveren" på side 142

Synkronisere med LDAP-server

Angi LDAP-server-innstillinger for skanneren.

Angi innstillinger for både hovedserveren og den sekundære serveren hvis det er nødvendig.

Merknad:
*Innstillingene for **LDAP-server** deles med **Kontakter**.*

Tilgjengelige tjenester

Følgende katalogtjenester støttes.

Tjenestenavn	Versjon
Active Directory	Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
OpenLDAP	Ver.2.3, Ver.2.4

Konfigurere en LDAP-server

For å bruke en LDAP-server, må du konfigurere LDAP-serveren.

Når du konfigurerer fra Web Config:

Velg fanen **Nettverk** > **LDAP-server** > **Grunnleggende (Primær server)** eller **Grunnleggende (Sekundær server)**.

Hvis du velger **Kerberos-autentisering** som **Godkjenningsmetode**, må du velge **Nettverk** > **Kerberos-innstillinger** for å angi innstillingene for Kerberos.

Når du konfigurerer fra Epson Device Admin:

Velg **Network** > **LDAP server** > **Server Settings (Primary Server)** eller **Server Settings (Secondary Server)** fra konfigurasjonsmalen.

Hvis du velger **Kerberos-autentisering** som **Godkjenningsmetode**, må du velge **Network — Security** > **Kerberos-innstillinger** for å angi innstillingene for Kerberos.

Element	Innstillinger og forklaring
Bruk LDAP-server	Velg **Bruk** eller **Ikke bruk**.
LDAP-serveradresse	Skriv inn LDAP-serveradressen. Skriv inn mellom 1 og 255 tegn i enten IPv4-, IPv6- eller FQDN-format. For FQDN-format kan du bruke alfanumeriske tegn i ASCII (0x20–0x7E) og anførselstegn, bortsett fra i begynnelsen og slutten av adressen.
LDAP-serverportnummer (Port number)	Skriv inn LDAP-serverens portnummer mellom 1 og 65535.
Sikker forbindelse	Angi godkjenningsmetoden for skanneren som skal få tilgang til LDAP-serveren.

Element	Innstillinger og forklaring
Sertifikatvalidering	Sertifikatet for LDAP-serveren godkjennes når dette er aktivert. Vi anbefaler å stille dette inn som **Aktiver**. For å konfigurere må **CA-sertifikat** være importert til skanneren.
Tidsavbrudd for søk (sek)	Angi tiden for å søke før tidsavbrudd mellom 5 og 300 sekunder.
Godkjenningsmetode	Velg godkjenningsmetode. Hvis du velger **Kerberos-autentisering**, må du angi innstillingene for Kerberos på forhånd. For å gjennomføre Kerberos-autentisering, kreves følgende omgivelser. ❏ Skanneren og DNS-serveren kan kommunisere. ❏ Klokkeslettet til skanneren, KDC-serveren og serveren som kreves for godkjenning (LDAP-server, SMTP-server, filserver) er synkroniserte. ❏ Når tjenesteserveren er tilordnet som IP-adressen, er tjenesteserverens FQDN registrert på DNS-serverens reverserte oppslagssone.
Kerberos-område som skal brukes	Hvis du velger **Kerberos-autentisering** for **Godkjenningsmetode**, velger du Kerberos-riket som du vil bruke.
Administrator-DN / Brukernavn	Skriv inn brukernavnet for LDAP-serveren på 128 tegn eller mindre i Unicode (UTF-8). Du kan ikke bruke kontrolltegn, som 0x00–0x1F og 0x7F. Denne innstillingen brukes ikke når **Anonym autentisering** er valgt som **Godkjenningsmetode**. Hvis du ikke vil angi dette, la det stå tomt.
Passord	Skriv inn passordet for LDAP-servergodkjenning på 128 tegn eller mindre i Unicode (UTF-8). Du kan ikke bruke kontrolltegn, som 0x00–0x1F og 0x7F. Denne innstillingen brukes ikke når **Anonym autentisering** er valgt som **Godkjenningsmetode**. Hvis du ikke vil angi dette, la det stå tomt.

Kerberos-innstillinger

Hvis du velger **Kerberos-autentisering** som **Godkjenningsmetode**, må du angi innstillingene for Kerberos. Du kan registrere opp til 10 Kerberos-innstillinger.

Når du konfigurerer fra Web Config:

Velg **Nettverk**-fanen > **Kerberos-innstillinger**.

Når du konfigurerer fra Epson Device Admin:

Velg **Network** > **Security** > **Kerberos-innstillinger** fra konfigurasjonsmalen.

Element	Innstillinger og forklaring
Område (domene)	Skriv inn området for Kerberos-godkjenning med maksimalt 255 i ASCII (0x20–0x7E). Hvis du ikke vil registrere dette, la det stå tomt.
KDC-adresse	Skriv inn adressen til Kerberos-autentiseringsserveren. Skriv inn 255 tegn eller mindre i enten IPv4, IPv6 eller FQDN-format. Hvis du ikke vil registrere dette, la det stå tomt.
Portnummer (Kerberos)	Skriv inn Kerberos-serverens portnummer mellom 1 og 65535.

Konfigurere søkeinnstillinger for LDAP-serveren

Angir søkeegenskapene for brukerinnstillinger.

Når du konfigurerer fra Web Config:

Velg **Nettverk**-fanen > **LDAP-server** > **Søkeinnstillinger (godkjenning)**.

Når du konfigurerer fra Epson Device Admin:

Velg **Administrator Settings** > **Authentication Settings** > **LDAP server** > **Search Settings (Authentication)** fra konfigurasjonsmalen.

Element	Innstillinger og forklaring
Search Base (Distinguished Name)	Angi startposisjonen når du søker etter brukerinformasjon fra LDAP-serveren. Skriv inn mellom 0 og 128 tegn i Unicode (UTF-8). Hvis du ikke søker etter en vilkårlig attributt, la dette stå tomt. Eksempel på lokal serverkatalog: dc=server, dc=lokal
User ID Attribute	Angi attributtnavnet som skal vises ved søk etter ID-nummer. Skriv inn mellom 1 og 255 tegn i ASCII. Det første tegnet må være a–z eller A–Z. Eksempel: cn, uid
User name Display Attribute	Angi attributtnavn som skal vises som brukernavnet. Skriv inn mellom 0 og 255 tegn i ASCII. Det første tegnet må være a–z eller A–Z. Dette kan stå tomt. Eksempel: cn, name
Authentication Card ID Attribute	Angi attributtnavnet som skal vises som ID for godkjenningskortet. Skriv inn mellom 0 og 255 tegn i ASCII. Det første tegnet må være a–z eller A–Z. Dette kan stå tomt. Eksempel: cn, sn
ID Number Attribute	Angi attributtnavnet som skal vises ved søk etter ID-nummer. Skriv inn mellom 1 og 255 tegn i ASCII. Det første tegnet må være a–z eller A–Z. Eksempel: cn, id
Department Attribute	Angi attributtnavnet som skal vises som avdelingsnavn. Skriv inn mellom 0 og 255 tegn i ASCII. Det første tegnet må være a–z eller A–Z. Dette kan stå tomt. Eksempel: ou, ou-cl
Email Address Attribute	Angi attributtnavn som skal vises når du søker etter e-postadresser. Skriv inn mellom 1 og 255 tegn i ASCII. Det første tegnet må være a–z eller A–Z. Eksempel: mail
Save To Attribute	Angi attributtnavnet som peker til målet for Scan To My Folder. Skriv inn mellom 0 og 255 tegn i ASCII. Eksempel: homeDirectory

Kontrollere LDAP-servertilkoblingen

Utfører tilkoblingstesten til LDAP-serveren ved hjelp av parameteren angitt i **LDAP-server** > **Søkeinnstillinger**.

1. Gå inn på Web Config og velg **Nettverk**-fanen > **LDAP-server** > **Tilkoblingstest**.

2. Velg **Start**.

   Tilkoblingstest startet. Etter testen vil kontrollrapporten vises.

Testreferanser for LDAP-servertilkobling

Meldinger	Forklaring
Tilkoblingstesten var vellykket.	Denne meldingen vises når tilkoblingen til serveren er vellykket.
Tilkoblingstesten mislyktes. Kontroller innstillingene.	Denne meldingen vises av følgende årsaker: ❏ Det er feil adresse eller portnummer til LDAP-serveren. ❏ Det oppstod et tidsavbrudd. ❏ **Ikke bruk** er valgt som **Bruk LDAP-server**. ❏ Hvis **Kerberos-autentisering** er valgt som **Godkjenningsmetode**, innstillinger som **Område (domene)**, **KDC-adresse** og **Portnummer (Kerberos)** er feil.
Tilkoblingstesten mislyktes. Kontroller dato og klokkeslett på produktet eller serveren.	Denne meldingen vises når tilkoblingen mislykkes fordi tidsinnstillingene for skanneren og LDAP-serveren ikke samsvarer.
Autentisering mislyktes. Kontroller innstillingene.	Denne meldingen vises av følgende årsaker: ❏ **Brukernavn** og/eller **Passord** er feil. ❏ Hvis **Kerberos-autentisering** er valgt som **Godkjenningsmetode** kan ikke klokkeslett/dato konfigureres.
Får ikke tilgang til produktet før behandlingen er fullført.	Denne meldingen vises når skanneren er opptatt.

Konfigurere e-postserveren

Angi e-postserveren når du bruker **Skann til min e-post**.

Merknad:
*Du kan bare angi **Skann til min e-post** når **Skann til e-post** er aktivert.*

Når du konfigurerer fra Web Config:

Velg **Nettverk**-fanen > **E-postserver** > **Grunnleggende**.

Når du konfigurerer fra Epson Device Admin:

Velg **Common** > **Email Server** > **Mail Server Settings** fra konfigurasjonsmalen.

Element	Innstillinger og forklaring	
Godkjenningsmetode	Angi godkjenningsmetoden for skanneren som skal få tilgang til e-postserveren.	
	Av	Autentifisering er deaktivert under kommunikasjon med en e-postserver.
	SMTP-autentisering	E-postserveren må støtte SMTP-godkjenning.
	POP før SMTP	Angi en POP3-server når du velger dette elementet.

Element	Innstillinger og forklaring	
Godkjent konto	Hvis du velger **SMTP-autentisering** eller **POP før SMTP** som **Godkjenningsmetode**, må du angi navnet til den godkjente kontoen. Skriv inn mellom 0 og 255 tegn i ASCII (0x20–0x7E).	
Godkjent passord	Hvis du velger **SMTP-autentisering** eller **POP før SMTP** som **Godkjenningsmetode**, må du angi det godkjente passordet. Skriv inn mellom 0 og 20 tegn i ASCII (0x20–0x7E).	
Avsenderens e-postadresse	Skriv inn avsenderens e-postadresse. Skriv inn mellom 0 og 255 tegn i ASCII (0x20–0x7E), bortsett fra : ( ) < > [ ] ; ¥. Det første tegnet kan ikke være et punktum «.».	
SMTP-server adresse	Skriv inn mellom 0 og 255 tegn ved hjelp av A–Z a–z 0–9 . -. Du kan bruke IPv4- eller FQDN-format.	
SMTP-server portnummer	Skriv inn et tall mellom 1 og 65535.	
Sikker forbindelse	Spesifiser sikker tilkobling metode for e-postserveren.	
	Ingen	Hvis du velger **POP før SMTP** i **Godkjenningsmetode**, blir tilkoblingsmetoden satt til **Ingen**.
	SSL/TLS	Dette er tilgjengelig når **Godkjenningsmetode** er satt til **Av** eller **SMTP-autentisering**.
	STARTTLS	Dette er tilgjengelig når **Godkjenningsmetode** er satt til **Av** eller **SMTP-autentisering**.
Sertifikatvalidering	Sertifikatet er godkjent når dette er aktivert. Vi anbefaler å stille dette inn som **Aktiver**.	
POP3-server adresse	Hvis du velger **POP før SMTP** som **Godkjenningsmetode**, må du angi POP3-serveradressen. Du kan skrive inn mellom 0 og 255 tegn ved hjelp av A–Z, a–z, 0–9. Du kan bruke IPv4- eller FQDN-format.	
POP3-server portnummer	Hvis du velger **POP før SMTP** som **Godkjenningsmetode**, må du spesifisere portnummeret. Skriv inn et tall mellom 1 og 65535.	

Angi Skann til min mappe

Lagrer skannede bilder i mappen som er tilordnet hver bruker. Du kan angi følgende som en dedikert mappe.

Merknad:
*Du kan bare angi **Scan To My Folder** når **Skann til nettverksmappe /FTP** er aktivert.*

Lagre i innstillinger	Godkjenningsmetode	Sted for innstilling av mappebane
Spesifiser én nettverksmappe for hele Godkjenningsinnstillinger for automatisk å opprette en personlig mappe under den spesifiserte mappen med navnet til bruker-ID-en.	❏ Lokal DB ❏ LDAP ❏ Lokal DB og LDAP	Skanner (Innstillingen Skann til min mappe)
Tilordne ulike nettverksmapper individuelt for hver bruker.	Lokal DB	Skanner (Brukerinnstillinger)
	LDAP	LDAP-attributter
	Lokal DB og LDAP	Skanner (Brukerinnstillinger) eller LDAP-attributter

Når du konfigurerer fra Web Config:

Velg **Produktsikkerhet**-fanen > **Skann til nettverksmappe /FTP**.

Når du konfigurerer fra Epson Device Admin:

Velg **Administrator Settings** > **Authentication Settings** > **Skann til nettverksmappe /FTP** > **Scan to My Folder** fra konfigurasjonsmalen.

Element		Forklaring
Lagre til innstilling	Innstillingstype	❏ **Delt**: Oppretter automatisk en mappe oppkalt etter brukerens ID under mappebanen eller nettadressen som er angitt i **Lagre til**, og lagrer de skannede bildene i denne mappen. ❏ **Individuell**: Angi lagringsmål for skanningsresultater for hver bruker. Lokal DB-brukere kan angis i brukerinnstillingene. LDAP-brukere bruker lagringsplasseringen som kreves av LDAP-serverens søkeegenskaper.
	Type	Velg overføringsprotokollen i henhold til målet for skanningen. For en nettverksmappe: **Nettverksmappe (SMB)** For en FTP-server: **FTP**
	Lagre til	Spesifiser banen eller URL-en til utdatabanen. Skriv inntil 160 tegn i Unicode (UTF-16).
	Tilkoblingsmodus	Når du velger, sett **FTP** i **Type**. Velg tilkoblingsmodus for FTP-serveren.
	Portnummer	Når du velger, sett **FTP** i **Type**. Angi portnummeret og send skannede data til en FTP-server mellom 0 og 65535.
Godkjenningsinnstillinger	Innstillingstype	Når du velger **Individuell** som **Innstillingstype** i **Lagre til innstilling**. Angi «Brukernavn» og «Passord» for å åpne mappen. ❏ **Delt**: Bruk et felles **Brukernavn** og **Passord** for alle brukerne. ❏ **Individuell**: For Lokal DB-brukere, kan du angi **Brukernavn** og **Passord** individuelt i **Brukerinnstillinger**. LDAP-brukere kan ikke konfigureres individuelt. **Brukernavn** og **Passord** som angis her brukes som en pakke.
	Brukernavn	Angi brukernavnet fr å få tilgang til mappen for lagring av skannede utdata. Skriv inntil 30 tegn i Unicode (UTF-16). Angi dette når du bruker en **Delt** eller LDAP-server.
	Passord	Oppgi passordet som tilhører **Brukernavn**. Skriv inntil 20 tegn i Unicode (UTF-16). Angi dette når du bruker en **Delt** eller LDAP-server.

Forhindre endring av mål for Skann til nettverksmappe /FTP

Element	Forklaring
Forby manuell inntasting av mål	Brukeren kan ikke endre standardmål når dette er aktivert.

Tilpass Ett-trykksfunksjoner

Du kan vise bare de ikonene som er nødvendige ved å redigere ikonoppsettet som vises på hjem-skjermen for kontrollpanelet.

Når du konfigurerer fra Web Config:

Velg **Produktsikkerhet**-fanen > **Tilpass Ett-trykksfunksjoner**.

Når du konfigurerer fra Epson Device Admin:

Velg **Administrator Settings** > **Authentication Settings** > **Customize One-touch Functions** fra konfigurasjonsmalen.

Merknad:
I følgende tilfeller vises ikke ikonene for tilgjengelige funksjoner på startskjermen.

- ❏ *Når du velger funksjoner som ikke er tillatt på grunn av **Begrensninger**.*
- ❏ *Når e-postadressen for en pålogget bruker ikke er registrert. (Skann til min e-post)*
- ❏ *Når målmappen ikke er angitt. (Skann til min mappe)*

Element	Forklaring
Maksimalt antall funksjoner per skjerm	Velg oppsett for ikonene som vises på kontrollpanelet fra kontrollpanelet. Bildet endres i henhold til valgt oppsett.
Skjerm(er)	Velg antall sider.
Nummer	Velg funksjonene du vil vise for hver nummererte posisjon.

Job History-rapporter som bruker Epson Device Admin

Du kan opprette en Job History-rapport for hver gruppe og hver bruker med Epson Device Admin. Du kan lagre opptil 3000 forekomster av brukshistorikken på skanneren. Du kan opprette rapporten ved å angi en tidsperiode eller en vanlig tidsplan.

For å eksportere Job History som en rapport, velger du **Options** > **Epson Print Admin Serverless/Authentication Settings** > **Manage the Epson Print Admin Serverless/Authentication compatible devices** fra båndmenyen på Enhetsliste-skjermen.

For mer informasjon om hvordan du lager en brukerrapport, kan du se dokumentasjonen for Epson Device Admin.

Elementer som kan inkluderes i rapporten

Du kan oppgi følgende elementer i brukerrapporten.

Date/Job ID/Operation/User ID/Department/Result/Result details/Scan: Destination type/Scan: Destination/Scan: Paper Size/Scan: 2-Sided/Scan: Color/Scan: Pages/Devices: Model/Devices: IP Address/Devices: Serial Number/ Devices: Department/Devices: Location/Devices: Remark/Devices: Note

Logge på som en administrator fra kontrollpanelet

Du kan bruke hvilken som helst av de følgende metodene for å logge inn som administrator fra skannerens kontrollpanel.

1. Trykk på  øverst til høyre på skjermen.
   - ❏ Når Godkjenningsinnstillinger er aktivert, vises ikonet på **Velkommen**-skjermen (standby-skjermen for godkjenning).
   - ❏ Når Godkjenningsinnstillinger er deaktivert, vises ikonet på Hjem-skjermen.
2. Trykk på **Ja** når bekreftelsesskjermbildet vises.
3. Angi administratorpassord.

   En melding som forteller at pålogging er fullført vises, så vises Hjem-skjermen på kontrollpanelet.

Trykk på  øverst til høyre på Hjem-skjermen for å logge ut.

Deaktivere Godkjenningsinnstillinger

Du kan deaktivere Godkjenningsinnstillinger med Web Config.

Merknad:
Brukerinnstillinger som er registrert i skanneren lagres selv om Godkjenningsinnstillinger er deaktivert. Du kan fjerne dem ved å gjenopprette standardinnstillingene til skanneren.

1. Åpne Web Config.
2. Velg **Produktsikkerhet**-fanen > **Grunnleggende** > **Godkjenning**.
3. Velg **Av**.
4. Klikk på **Neste**.
5. Klikk på **OK**.

Merknad:
Selv om du deaktiverer Godkjenningsinnstillinger, forblir Låsinnstilling aktivert. Hvis du vil deaktivere det, kan du stille dette inn fra kontrollpanelet eller Web Config.

Relatert informasjon

➡ "Konfigurere Låsinnstilling fra kontrollpanelet" på side 83
➡ "Angi Låsinnstilling fra Web Config" på side 83

Slette informasjon om Godkjenningsinnstillinger (Gjenopprett standardinnst.)

For å slette all informasjonen om Godkjenningsinnstillinger (Kortleser, Godkjenningsmetode, Brukerinnstillinger, og så videre), må du gjenopprette alle skannerinnstillingene til standardinnstillingene som de var ved kjøp.

Velg **Innst.** > **Systemadministrasjon** > **Gjenopprett standardinnst.** > **Alle innstillinger** på kontrollpanelet.

> ***Forsiktighetsregel:***
> *Alle kontakter og andre nettverksinnstillinger slettes også. Slettede innstillinger kan ikke gjenopprettes.*

Problemløsning

Kan ikke lese godkjenningskortet

Kontroller følgende.

❏ Sjekk om godkjenningsenheten er koblet riktig til skanneren.
Koble godkjenningsenheten til USB-porten for eksternt grensesnitt på baksiden av skanneren.

❏ Sjekk at godkjenningsenheten og godkjenningskortet støttes.

Vedlikehold

Rengjøre utsiden av skanneren

Tørk av eventuelle flekker på kabinettet med en tørr klut eller en klut fuktet med mildt rengjøringsmiddel og vann.

Forsiktighetsregel:

- ❏ *Bruk aldri alkohol, fortynningsmidler eller etsende løsemidler til å rengjøre skanneren. Misdannelse eller misfaring kan oppstå.*
- ❏ *Ikke la vann tre inn i produktet. Dette kan forårsake en funksjonssvikt.*
- ❏ *Ikke åpne skannerkabinettet.*

1. Trykk ⏻-knappen for å slå av skanneren.
2. Koble AC-adapteren fra skanneren.
3. Rengjør kabinettet med en klut fuktet med et mildt vaskemiddel og vann.

   Merknad:
   Tørk av berøringsskjermen med en myk, tørr klut.

Rengjøre innsiden av skanneren

Etter å ha brukt skanneren en stund, kan papir og romstøv på rulleren eller glassdelen på innsiden av skanneren forårsake problemer med papirmating eller kvalitet av skannede bilder. Rengjør innsiden av skanneren i intervaller på 5,000 skanninger.

Du kan sjekke siste antall skanninger på kontrollpanelet eller i Epson Scan 2 Utility.

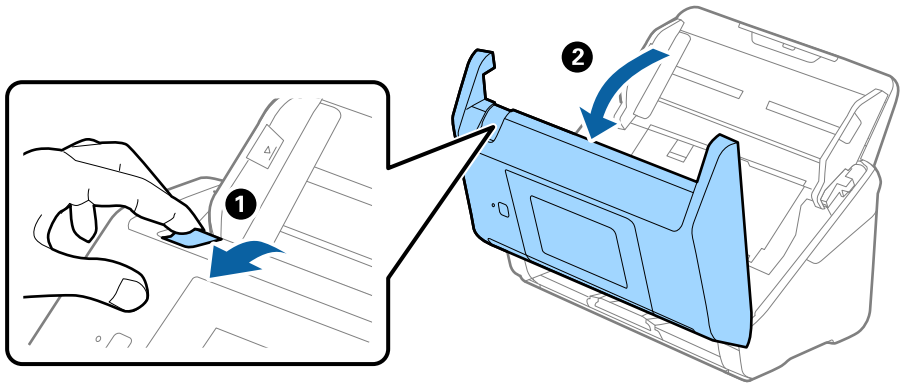
Dersom det har kommet vanskelige flekker på overflaten, bruk et ekte Epson rensesett for å fjerne dem. Bruk en liten mengde rensemiddel på kluten og fjern flekkene.

Forsiktighetsregel:

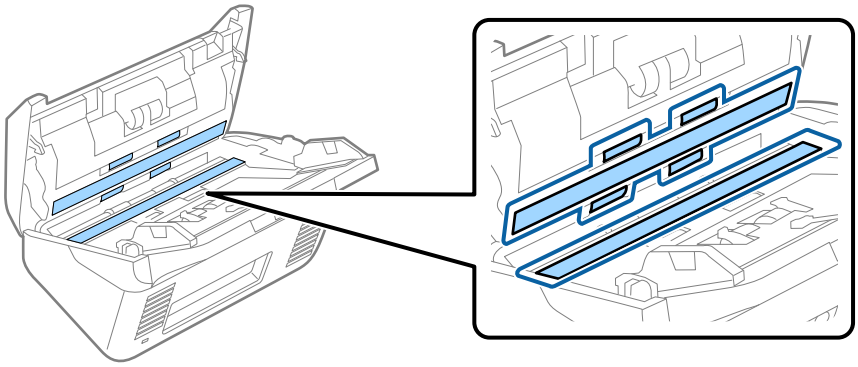
- ❏ *Bruk aldri alkohol, fortynningsmidler eller etsende løsemidler til å rengjøre skanneren. Misdannelse eller misfaring kan oppstå.*
- ❏ *Spray aldri væsker eller smøremiddel på skanneren. Skade på utstyr eller kretser kan forårsake unormal drift.*
- ❏ *Ikke åpne skannerkabinettet.*

1. Trykk ⏻-knappen for å slå av skanneren.
2. Koble AC-adapteren fra skanneren.

3. Dra i spaken og åpne skannerdekselet.



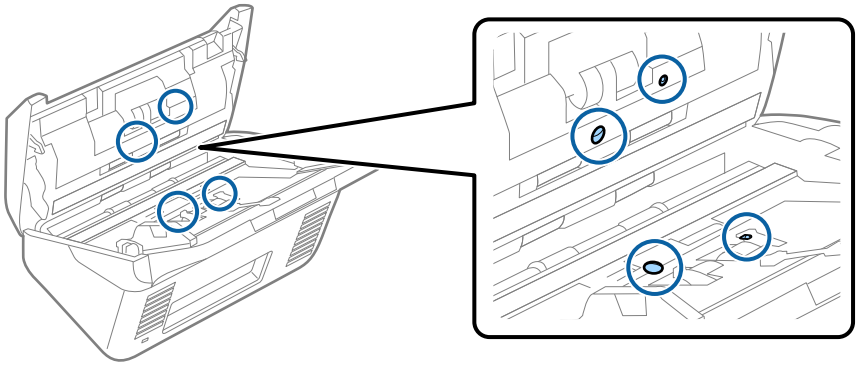
4. Tørk av eventuelle flekker på plastrullen og glassoverflaten på undersiden av skannerdekselet med en myk klut eller et ekte Epson-rengjøringssett.



Forsiktighetsregel:

- *Ikke påfør for mye kraft på glassoverflaten.*
- *Ikke bruk en børste eller et hardt verktøy. Eventuelle skraper på glasset kan påvirke skannekvaliteten.*
- *Ikke spray rengjøringsmiddel direkte på glassoverflaten.*

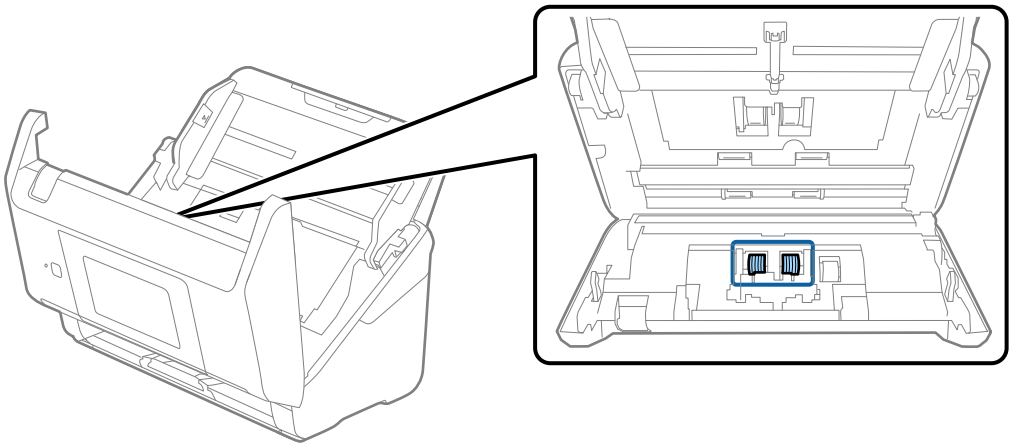
5. Tørk av eventuelle flekker på sensorene med en bomullspinne.



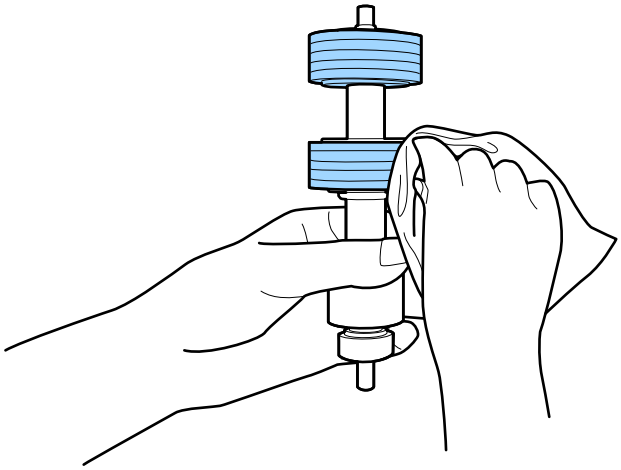
> ***Forsiktighetsregel:***
> *Ikke bruk væsker slik som et rengjøringsmiddel på en bomullspinne.*

6. Åpne dekselet og fjern så separasjonsrullen.

   Se «Bytte ut rullersettet» for mer informasjon.



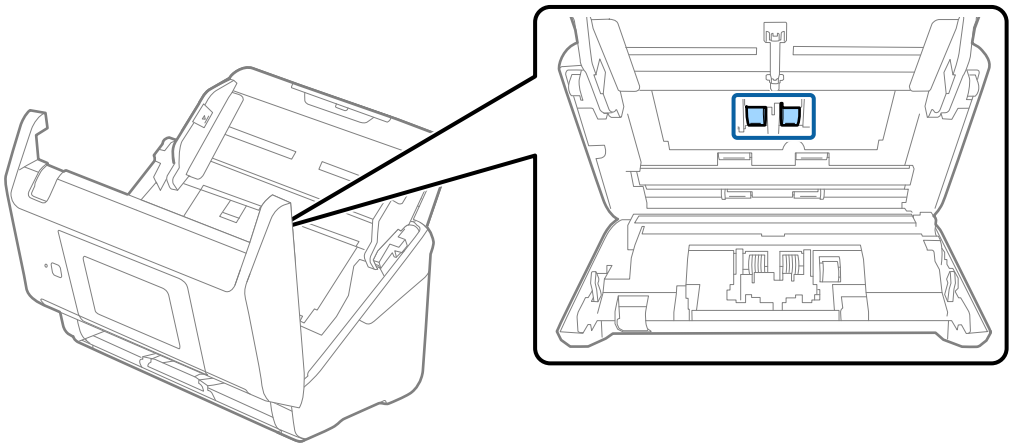
7. Tørk av støv eller skitt på separasjonsvalsen ved hjelp av et ekte Epson-rensesett eller en myk, fuktig klut.



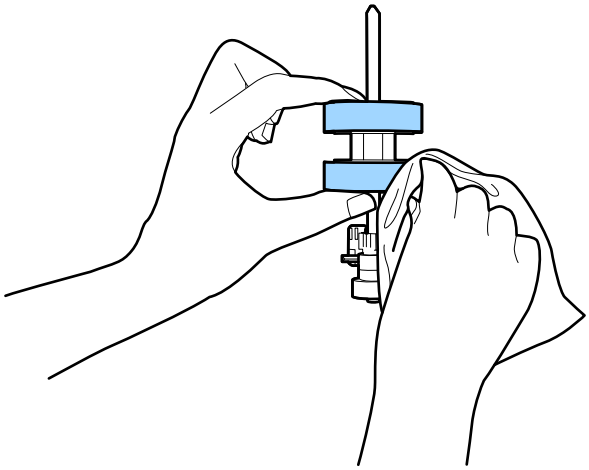
> ***Forsiktighetsregel:***
> *Bruk kun et ekte Epson-rensesett eller en myk, fuktig klut til å rengjøre valsen. Bruk av tørr klut kan skade overflaten av valsen.*

8. Åpne dekselet og fjern så oppsamlingsrullen.

   Se «Bytte ut rullersettet» for mer informasjon.



9. Tørk av støv eller skitt på oppsamlingsrullen ved hjelp av et ekte Epson-rensesett eller en myk, fuktig klut.



> ***Forsiktighetsregel:***
>
> *Bruk kun et ekte Epson-rensesett eller en myk, fuktig klut til å rengjøre valsen. Bruk av tørr klut kan skade overflaten av valsen.*

10. Lukk skannerdekselet.

11. Sett inn AC-adapteren og slå så på skanneren.

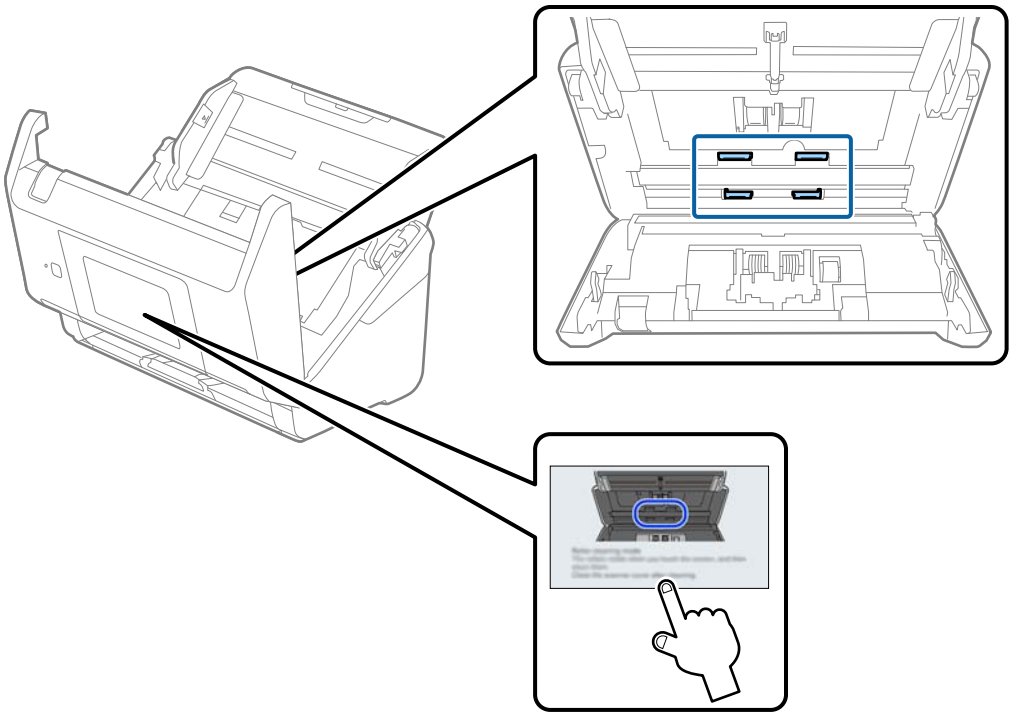
12. Velg **Vedlikehold av skanner** fra hjemmeskjermen.

13. Velg **Rengjøring av vals** på **Vedlikehold av skanner** skjermen.

14. Trekk i spaken for å åpne skannerdekslet.

    Skanneren går inn i rulle-rengjøringsmodus.

15. Sakte roter rullene i bunnen ved å trykke hvor som helst på skjermen. Tørk av valsene med et ekte Epson-rensesett eller en myk klut fuktet med vann. Gjenta inntil rullene er rengjort.



> ***Forsiktig:***
>
> *Vær forsiktig så hendene dine eller håret ditt ikke setter seg fast i mekanismen mens du opererer rullen. Dette kan forårsake en ulykke.*

16. Lukk skannerdekselet.

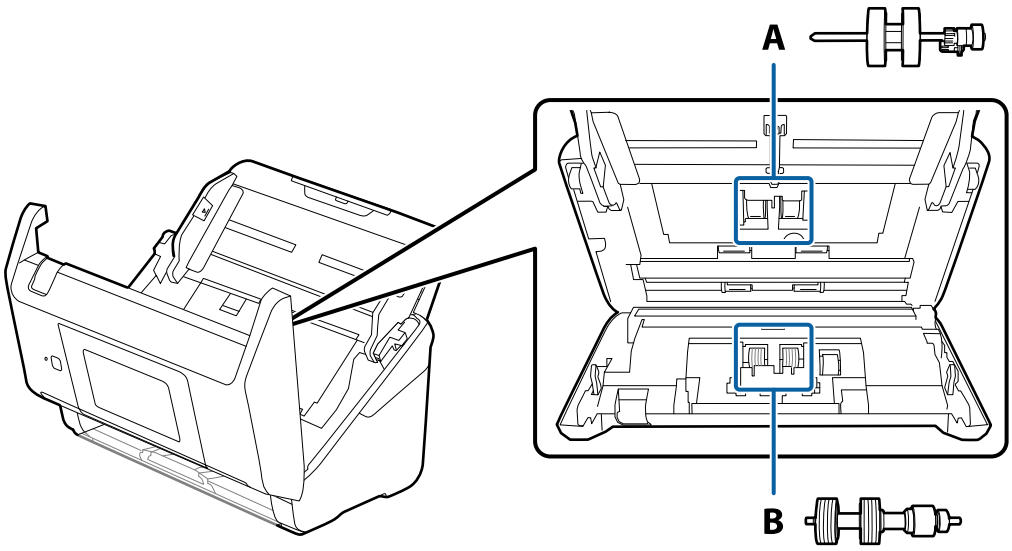
    Skanneren går ut av rulle-rengjøringsmodus.

Relatert informasjon

➡ "Bytte ut rullersettet" på side 155

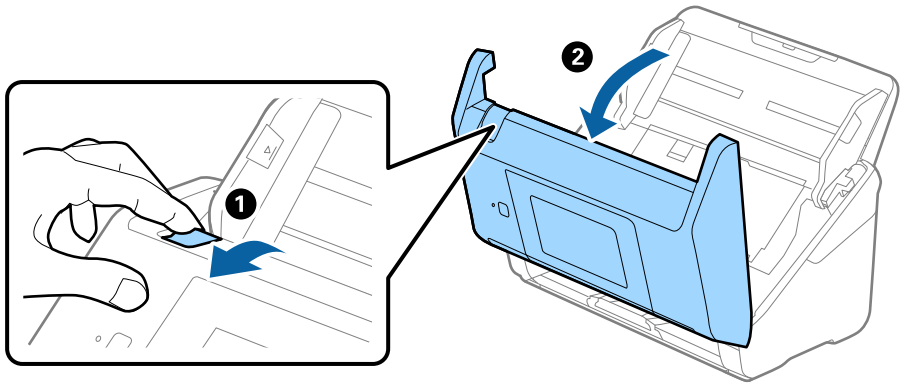
Bytte ut rullersettet

Rullersettet (pickup-rulleren og separeringsrulleren) må byttes ut når antall skanninger overskrider livssyklusen til rullene. Når en erstatningsmelding vises på kontrollpanelet eller dataskjermen, følger du trinnene nedenfor for å erstatte det.

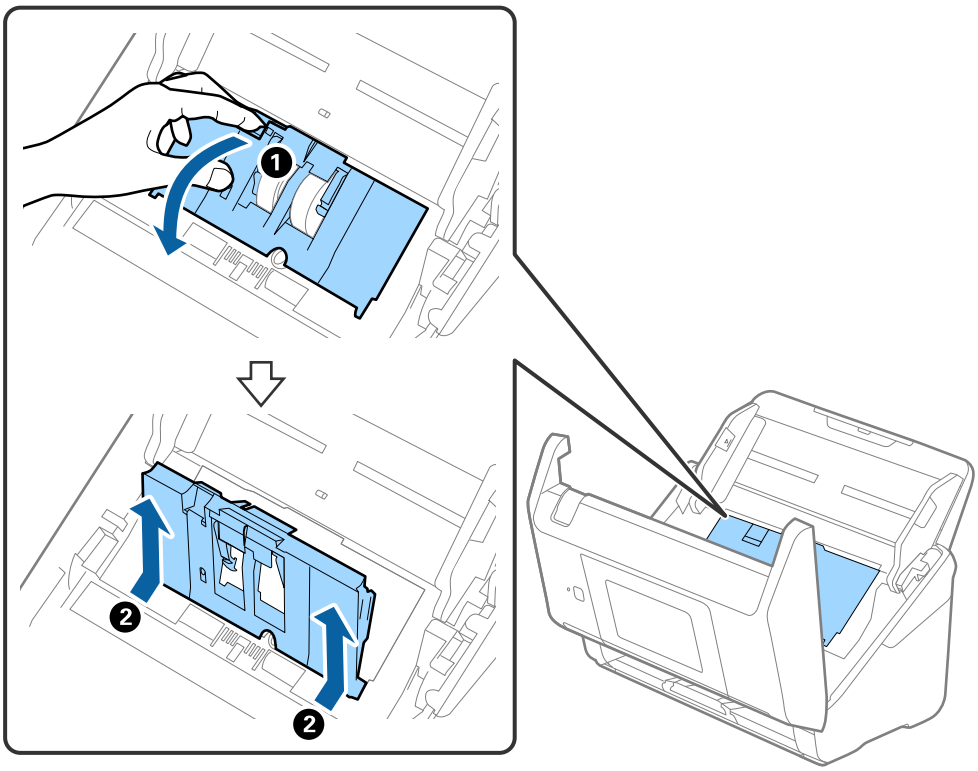


A: pickup-rulle, B: separeringsrulle

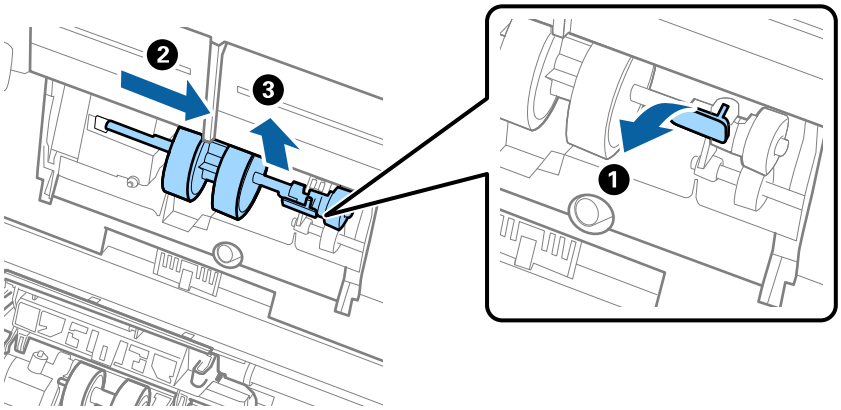
1. Trykk ⏻-knappen for å slå av skanneren.
2. Koble AC-adapteren fra skanneren.
3. Dra i spaken og åpne skannerdekselet.



4. Åpne dekselet til oppsamlingsrulleren og så glir og fjerner du den.

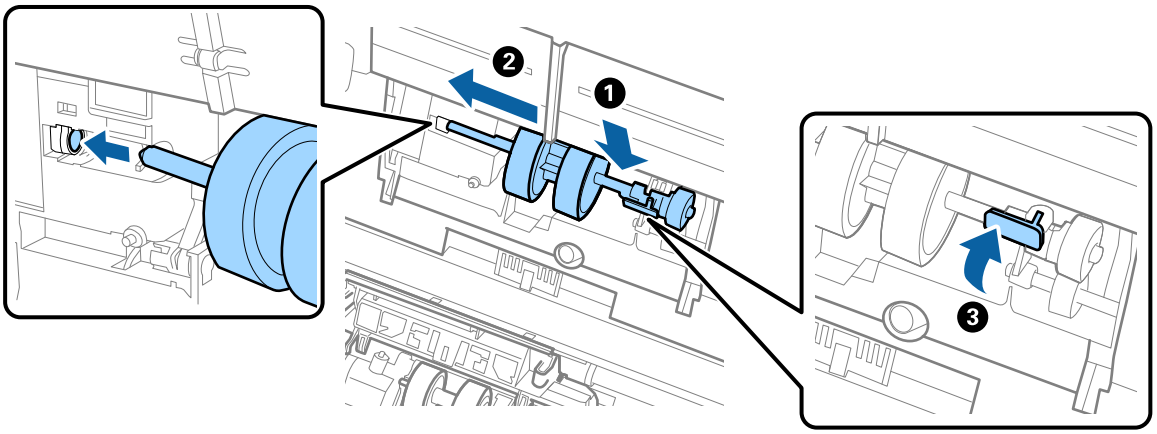


5. Trekk så fiksturen av rulleraksen og så glir du og fjerner de monterte oppsamlingsrullene.

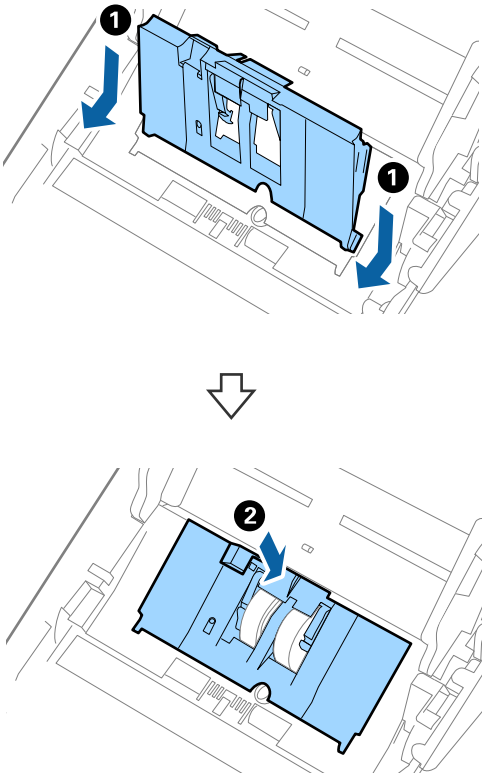


> ***Forsiktighetsregel:***
> *Ikke dra ut oppsamlingsrullen med makt. Dette kan skade innsiden av skanneren.*

6. Mens du holder fiksturen nede, glir du den nye oppsamlingsrullen til venstre og setter den inn i hullet i skanneren. Trykk fiksturen for å sikre den.

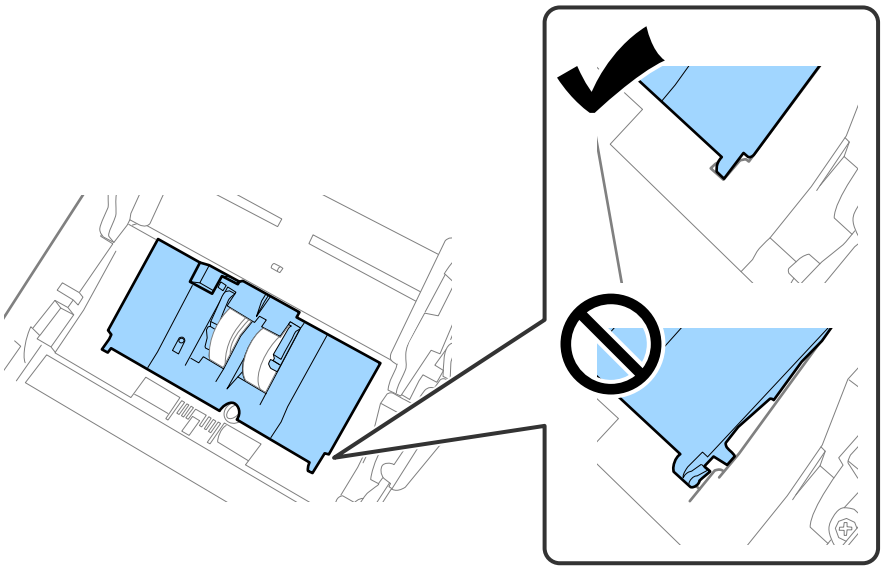


7. Sett kanten av dekselet til oppsamlingsrullen inn i sporet og gli den inn. Lukk dekselet godt.

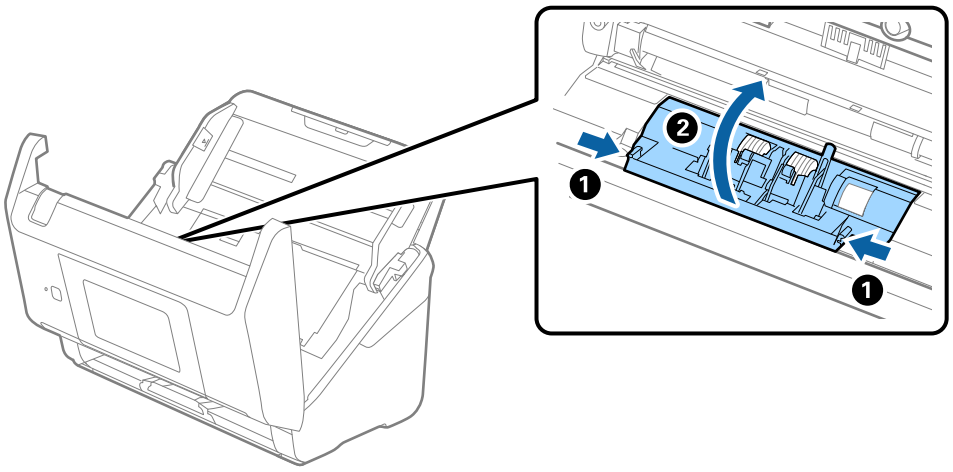


Forsiktighetsregel:

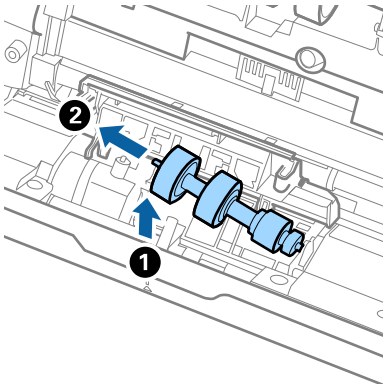
- ❏ *Sørg for at oppsamlingsdekselet er riktig lukket.*
- ❏ *Kontroller at oppsamlingsrullene er riktig montert hvis det er vanskelig å lukke dekselet.*
- ❏ *Ikke monter dekselet mens det er hevet.*



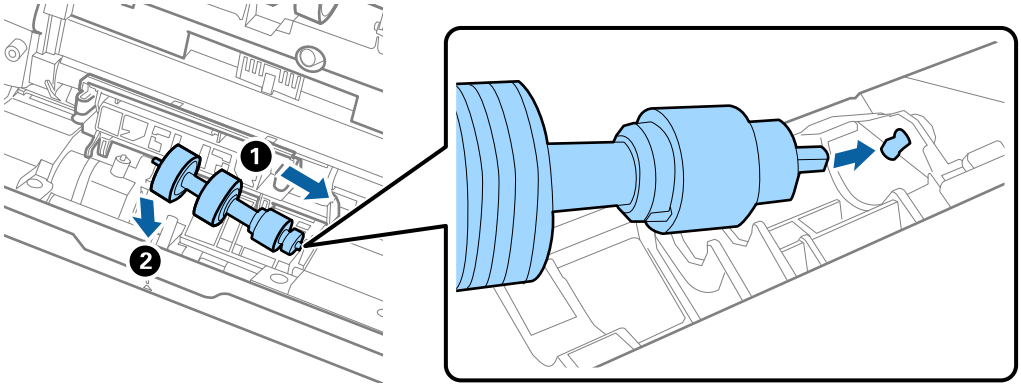
8. Dytt krokene på begge sider av dekselet til oppsamlingsrullen for å åpne dekselet.



9. Løft venstre side av separasjonsrullen og så glir du og fjerner de monterte separasjonsrullene.



10. Sett den nye aksen for separasjonsrullen inn i hullet på høyre side, og så senker du rullen.



11. Lukk dekselet for separasjonsrullen.

> ***Forsiktighetsregel:***
> *Hvis dekselet er vanskelig å lukke, sjekk at separasjonsrullene er riktig installert.*

12. Lukk skannerdekselet.

13. Sett inn AC-adapteren og slå så på skanneren.

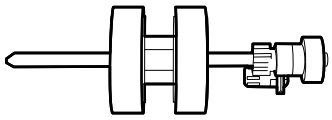
14. Tilbakestill skanningsantallet på kontrollpanelet.

Merknad:
Avhend oppsamlingsrullen og separasjonsrullen i henhold til lokale regler og bestemmelser. Ikke demonter dem.

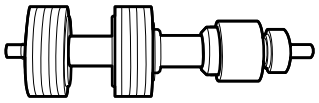
Koder for rullersett

Deler (oppsamlingsruller og separasjonsruller) bør skiftes når antall skanninger overstiger tjenestenummer. Du kan sjekke siste antall skanninger på kontrollpanelet i Epson Scan 2 Utility.

A



B



A: oppsamingsruller, B: separasjonsruller

Delenavn	Koder	Livssyklus
Rullersett	B12B819671 B12B819681 (bare India)	200,000*

* Dette antallet ble nådd med etterfølgende skanning med Epson-originalpapir for testing og er en veiledning for utskiftningssyklusen. Utskiftningssyklusen kan avvike avhengig av forskjellige papirtyper, slik som et papir som genererer masse papirstøv eller papir med en ujevn overflate kan forkorte livssyklusen.

Tilbakestille antall skanner

Nullstiller antall skanninger etter rullersettet har blitt byttet ut.

1. Velg **Innst.** > **Enhetsinformasjon** > **Tilbakestill antall skanninger** > **Antall skanninger etter valsbytte** fra startskjermen.
2. Trykk **Ja**.

Relatert informasjon

➡ "Bytte ut rullersettet" på side 155

Energisparing

Du kan spare energi ved å bruke hvilemodus eller auto strøm av-modus når ingen operasjoner blir utført av skanneren. Du kan angi tidsperioden før skanneren går inn i hvilemodus og slår seg av automatisk. Økning vil påvirke produktets energieffektivitet. Tenk på miljøet før du gjør endringer.

1. Velg **Innst.** på startskjermen.
2. Velg **Basisinnstillinger**.

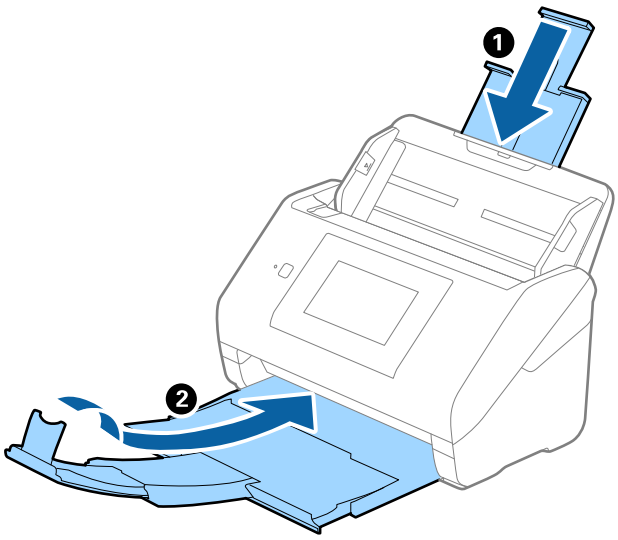
3. Velg **Avslåingsinnst.**, og angi deretter innstillingene.

   Merknad:
   Tilgjengelige funksjoner kan variere avhengig av kjøpssted.

Transportere skanneren

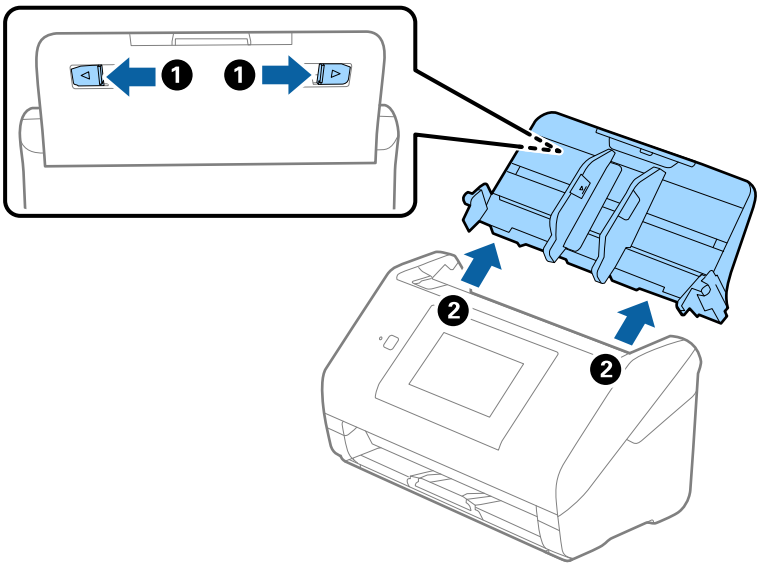
Når du må transportere skanneren pga flytting eller reparasjon, må du følge trinnene under for å pakke skanneren.

1. Trykk ⏻-knappen for å slå av skanneren.
2. Koble fra strømadapteren.
3. Fjern kablene og enhetene.
4. Lukk innskuffens forlengelse og utskuffen.



Forsiktighetsregel:
Sørg for at du lukker utskuffen godt, ellers kan den bli skadet under transport.

5. Fjern innskuffen.



6. Fest emballasjen som fulgte med skanneren og pakk deretter skanneren ned igjen i originalesken eller en solid eske.

Sikkerhetskopier innstillingene

Du kan eksportere innstillingsverdien angitt fra Web Config til filen. Du kan bruke den til å sikkerhetskopiere kontaktene, stille inn verdier, bytte skanneren, osv.

Den eksporterte filen kan redigeres fordi den eksporteres som en binær fil.

Eksportere innstillingene

Eksporter innstillingen for skanneren.

1. Gå inn på Web Config, og velg deretter **Enhetsadministrasjon**-fanen > **Innstillingsverdi for eksportering og importering** > **Eksporter**.

2. Velg innstillingene du vil eksportere.

   Velg innstillingene du vil eksportere. Hvis du velger en overordnet kategori, velges også underkategorier. Imidlertid kan underkategorier som forårsaker feil ved duplisering innenfor samme nettverk (for eksempel IP-adresser og så videre) ikke velges.

3. Skriv inn et passord for å kryptere den eksporterte filen.

   Du trenger passordet for å importere filen. La dette stå tomt hvis du ikke ønsker å kryptere filen.

4. Klikk på **Eksporter**.

> ***Forsiktighetsregel:***
> *Hvis du vil eksportere nettverksinnstillingene til skanneren, som enhetsnavnet og IPv6-adresse, velger du* ***Aktiver for å velge individuelle innstillinger for enhet*** *og velger flere elementer. Bruk bare de valgte verdiene for skanneren som utskiftes.*

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34

Importere innstillingene

Importer den eksporterte Web Config-filen til skanneren.

> ***Forsiktighetsregel:***
> *Ved import av verdier som inkluderer individuell informasjon, for eksempel skannernavn eller IP-adresse, må du kontrollere at den samme IP-adressen ikke eksisterer på samme nettverk.*

1. Åpne Web Config og velg **Enhetsadministrasjon**-fanen > **Innstillingsverdi for eksportering og importering** > **Importer**.
2. Velg den eksporterte filen og skriv deretter inn det krypterte passordet.
3. Klikk på **Neste**.
4. Velg innstillingene du vil importere, og klikk deretter **Neste**.
5. Klikk på **OK**.

Innstillingene brukes på skanneren.

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34

Gjenopprett standardinnst.

Velg **Innst.** > **Systemadministrasjon** > **Gjenopprett standardinnst.** fra kontrollpanelet, og velg deretter elementene du vil gjenopprette til standardinnstillingene.

- ❏ Nettverksinnstillinger: gjenopprette nettverksrelaterte innstillinger til sin opprinnelige status.
- ❏ Alt unntatt Nettverksinnstillinger: gjenopprette andre innstillinger til sin opprinnelige status unntatt nettverksrelaterte innstillinger.
- ❏ Alle innstillinger: gjenopprette alle innstillinger til sin opprinnelige status når kjøpt.

Forsiktighetsregel:

*Hvis du velger og kjører **Alle innstillinger**, slettes alle innstillingsdata som er registrert på skanneren, inkludert kontakter og brukerinnstillingene for autentifikasjon. Slettede innstillinger kan ikke gjenopprettes.*

Oppdatere programmer og fastvare

Du kan bli kvitt visse problemer og forbedre eller legge til funksjoner ved å oppdatere programmene og fastvaren. Forsikre deg om at du bruker den seneste versjonen av programmene og fastvaren.

Forsiktighetsregel:

❏ *Ikke slå av datamaskinen eller skanneren under oppdatering.*

Merknad:
*Når skanneren kan koble til Internett, kan du oppdatere fastvaren via Web Config. Velg **Enhetsadministrasjon**-fanen > **Fastvareoppdatering**, sjekk meldingen som vises og klikk deretter på **Start**.*

1. Kontroller at skanneren og datamaskinen er koblet sammen, og at datamaskinen er koblet til Internett.

2. Start EPSON Software Updater, og oppdater programmene eller fastvaren.

   Merknad:
   Windows Server-operativsystem støttes ikke.

   ❏ Windows 10

   Klikk på startknappen og velg **Epson Software** > **EPSON Software Updater**.

   ❏ Windows 8.1/Windows 8

   Angi programvarens navn i søkeboksen og velg deretter det viste ikonet.

   ❏ Windows 7

   Klikk Start-knappen, og velg deretter **Alle programmer** eller **Programmer** > **Epson Software** > **EPSON Software Updater**.

   ❏ Mac OS

   Velg **Finder** > **Gå** > **Programmer** > **Epson Software** > **EPSON Software Updater**.

Merknad:
Hvis du ikke finner programmet du vil oppdatere i listen, kan du ikke oppdatere det ved hjelp av EPSON Software Updater. Se etter seneste versjoner av programmene på Epsons lokale nettside.

http://www.epson.com

Oppdatere skannerens fastvare ved hjelp av kontrollpanelet

Hvis skanneren kan bli koblet til Internett, kan du oppdatere skannerens fastvare via kontrollpanelet. Du kan også angi at skanneren jevnlig skal se etter fastvareoppdateringer og varsle deg hvis det er noen.

1. Velg **Innst.** på startskjermen.

2. Velg **Systemadministrasjon** > **Fastvareoppdatering** > **Oppdater**.

   Merknad:
   *Velg **Varsel** > **På** for å angi at skanneren jevnlig skal se etter tilgjengelige fastvareoppdateringer.*

3. Se meldingen som vises på skjermen og begynn å søke etter tilgjengelige oppdateringer.

4. Hvis det vises en melding på LCD-skjermen om at det finnes en fastvareoppdatering, følger du instruksjonene på skjermen for å starte oppdateringen.

   Forsiktighetsregel:
   - *Du må ikke slå av eller trekke ut kontakten til skanneren før oppdateringen er fullført, ellers kan det oppstå feil på skanneren.*
   - *Hvis fastvareoppdateringen ikke fullføres eller er vellykket starter ikke skanneren som normalt og meldingen «Recovery Mode» vises på LCD-skjermen neste gang skanneren blir slått på. I så fall må du oppdatere fastvaren på nytt ved hjelp av datamaskinen. Koble skanneren til datamaskinen med en USB-kabel. Når «Recovery Mode» vises på skanneren, kan du ikke oppdatere fastvaren via en nettverkstilkobling. På datamaskinen går du til det lokale nettstedet til Epson, og deretter laster du ned den nyeste skannerfastvaren. Se i instruksjonene på nettstedet for hva du skal gjøre videre.*

Oppdatere fastvaren ved å bruke Web Config

Når skanneren kan koble til Internett, kan du oppdatere fastvaren via Web Config.

1. Gå inn på Web Config og velg **Enhetsadministrasjon**-fanen > **Fastvareoppdatering**.

2. Klikk på **Start**, og følg instruksjonene på skjermen.

   Fastvarekontrollen starter, og fastvareinformasjonen vises dersom oppdatert fastvare finnes.

Merknad:
Du kan også oppdatere fastvarer ved å bruke Epson Device Admin. Du kan ta en visuell sjekk av fastvareinformasjonen på enhetslisten. Dette er nyttig når du ønsker å oppdatere fastvaren på flere enheter. Se Epson Device Admin-veiledningen for mer informasjon.

Relatert informasjon

➡ "Kjøre web-konfigurasjon på en nettleser" på side 34

Oppdatere fastvaren uten å koble til Internett

Du kan laste ned enhetens fastvare fra Epson-nettstedet på en datamaskin og deretter koble enheten til datamaskinen med en USB-kabel for å oppdatere fastvaren. Hvis du ikke kan oppdatere over nettverket, kan du forsøke denne metoden.

Merknad:
Før du oppdaterer må du passe på at skannerdriveren Epson Scan 2 er installert på datamaskinen. Hvis Epson Scan 2 ikke er installert, må du installere den på nytt.

1. Sjekk Epson-nettstedet for de siste fastvare-oppdateringene.

   http://www.epson.com

❏ Hvis fastvaren til skanneren din er der, laster du den ned og går til neste trinn.

❏ Hvis det ikke finnes fastvareinformasjon på nettstedet bruker du allerede den siste fastvaren.

2. Koble datamaskinen som fastvaren ble lastet ned til skanneren ved å bruke en USB-kabel.

3. Dobbeltklikk på den nedlastede .exe-filen.
   Epson Firmware Updater starter.

4. Følg instruksjonene på skjermen.