EPSON
EXCEED YOUR VISION

Administratorhåndbok

NPD5668-00 NO

Innholdsfortegnelse

Tillegg

Avanserte sikkerhetsinnstillinger for bedrift

Opphavsrett

Varemerker

- ❏ EPSON® er et registrert varemerke, og EPSON EXCEED YOUR VISION eller EXCEED YOUR VISION er varemerker for Seiko Epson Corporation.
- ❏ Epson Scan 2 software is based in part on the work of the Independent JPEG Group.
- ❏ Google Cloud Print™, Chrome™, Chrome OS™, and Android™ are trademarks of Google Inc.
- ❏ Microsoft®, Windows®, Windows Server®, and Windows Vista® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Macintosh, Mac OS, OS X, AirMac, Bonjour, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint is a trademark of Apple Inc.
- ❏ 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.

Om denne håndboken

Ikoner og symboler

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

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

Merknad:
Instruksjoner som inneholder nyttige tips og begrensninger for bruk av skanneren.

Relatert informasjon

➡ Det vises relatert informasjon når du klikker dette ikonet.

Beskrivelser brukt i denne brukerhåndboken

❏ Skjermbildene av skannerdriveren og Epson Scan 2(skannerdriver) stammer fra Windows 10 eller OS X El Capitan. Innholdet som vises på skjermene, varierer avhengig av modellen og situasjonen.

❏ Illustrasjonene som brukes i denne brukerhåndboken er kun eksempler. Selv om det kan være mindre forskjeller på modellen, er operasjonsmetoden den samme.

❏ Noen av menyelementene på LCD-skjermen kan variere avhengig av modell og innstillinger.

Operativsystemreferanser

Windows

I denne brukerhåndboken referer "Windows 10", "Windows 8.1", "Windows 8", "Windows 7", "Windows Vista", "Windows XP", Windows Server 2016, "Windows Server 2012 R2", "Windows Server 2012", "Windows Server 2008 R2", "Windows Server 2008", "Windows Server 2003 R2" og "Windows Server 2003" til følgende operativsystemer. I tillegg brukes "Windows" for å referere til alle versjoner.

❏ Microsoft® Windows® 10 operativsystem

❏ Microsoft® Windows® 8.1 operativsystem

❏ Microsoft® Windows® 8 operativsystem

❏ Microsoft® Windows® 7 operativsystem

❏ Microsoft® Windows Vista® operativsystem

❏ Microsoft® Windows® XP operativsystem

❏ Microsoft® Windows® XP Professional x64 Edition operativsystem

- ❏ Microsoft® Windows Server® 2016 operativsystem
- ❏ Microsoft® Windows Server® 2012 R2 operativsystem
- ❏ Microsoft® Windows Server® 2012 operativsystem
- ❏ Microsoft® Windows Server® 2008 R2 operativsystem
- ❏ Microsoft® Windows Server® 2008 operativsystem
- ❏ Microsoft® Windows Server® 2003 R2 operativsystem
- ❏ Microsoft® Windows Server® 2003 operativsystem

Mac OS

I tillegg brukes "Mac OS" for å referere til macOS Sierra, OS X El Capitan, OS X Yosemite, OS X Mavericks, OS X Mountain Lion, Mac OS X v10.7.x og Mac OS X v10.6.8.

Innledning

Manuell komponent

Denne manualen er for enhetsadministratoren som er ansvarlig for å koble skriveren eller skanneren til nettverket, og den inneholder informasjon om hvordan du kan gjøre innstillinger for å bruke funksjonene.

Se *Brukerhåndbok* for informasjon om bruk av funksjoner.

Forberedelse

Forklarer administratoroppgaver, hvordan stille inn enheter og programvare brukt til administrasjon.

Tilkobling

Forklarer hvordan en enhet kobles til nettverket eller telefonlinjen. Den forklarer også nettverksmiljøet, som for eksempel informasjon om bruk av porter på enheten, DNS og proxy-server.

Innstillinger av funksjoner

Forklarer innstillingene for hver funksjon av enheten.

Grunnleggende sikkerhetsinnstillinger

Forklarer innstillingene for hver funksjon, slik som utskrift, skanning og faksing.

Drifts- og administrasjonsinnstillinger

Forklarer prosedyrer i etterkant av første bruk av enheter, slik som å sjekke informasjon og vedlikehold.

Løse problemer

Forklarer hvordan du foretar innstillinger og feilsøking for nettverket.

Avanserte sikkerhetsinnstillinger for bedrift

Forklarer innstillingsmetode for å forsterke enhetens sikkerhet for eksempel gjennom bruk av CA-sertifikat, SSL/TLS-kommunikasjon og IPsec/IP-filtrering.

Avhengig av modell, kan enkelte funksjoner omtalt i dette kapittelet ikke være støttet.

Definisjoner på termer som brukes i denne veiledningen

Termene nedenfor brukes i denne veiledningen.

Administrator

Personen som er ansvarlig for installasjon og konfigurasjon av enheten eller nettverket ved et kontor eller en organisasjon. I mindre organisasjoner, kan denne personen være ansvarlig for administrasjonen av både enheten og nettverket. I større organisasjoner styrer administratorer nettverket eller enhetene i gruppeenheten under en

avdeling eller filial, og nettverksadministratorer styrer over kommunikasjonsinnstillingene utover selve organisasjonen, slik som Internett.

Nettverksadministrator

Personen som er ansvarlig for nettverkskommunikasjonen. Personen som konfigurerte ruteren, proxy-serveren, DNS-serveren og e-postserveren for å administrere kommunikasjonen over Internett eller nettverket.

Bruker

Personen som bruker enheter som skrivere eller skannere.

Web Config (enhetens nettside)

Webserveren som er bygget inn i enheten. Den kalles for Web Config. Du kan sjekke og endre enhetens status på denne fra nettleseren.

Verktøy

Et generisk begrep for programvare for installasjon eller administrasjon av en enhet, slik som Epson Device Admin, EpsonNet Config, EpsonNet SetupManager, o.l.

Push scan

Et generisk begrep for skanning fra enhetens kontrollpanel.

ASCII (American Standard Code for Information Interchange)

Én av de standard karakterkodene. 128 tegn er definert, inkludert tegn som alfabetet (a–z, A–Z), arabiske tall (0–9), symboler, blanke tegn, og kontrolltegn. Når det henvises til "ASCII" i denne veildeningen, vises det til 0x20–0x7E (heksadesimale numre) som er listet opp under, og inkluderer ikke kontrolltegn.

SP*	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	

* Blanktegn.

Unicode (UTF-8)

En internasjonal standard kode som dekker alle de største internasjonale språkene. Når det henvises til "UTF-8" i denne veiledningen, refereres det til koding av tegn i UTF-8-format.

Forberedelse

Dette kapittelet forklarer administratorens rolle samt forberedelsesprosessen før innstillinger foretas.

Flyt av skannerinnstillinger og administrasjon

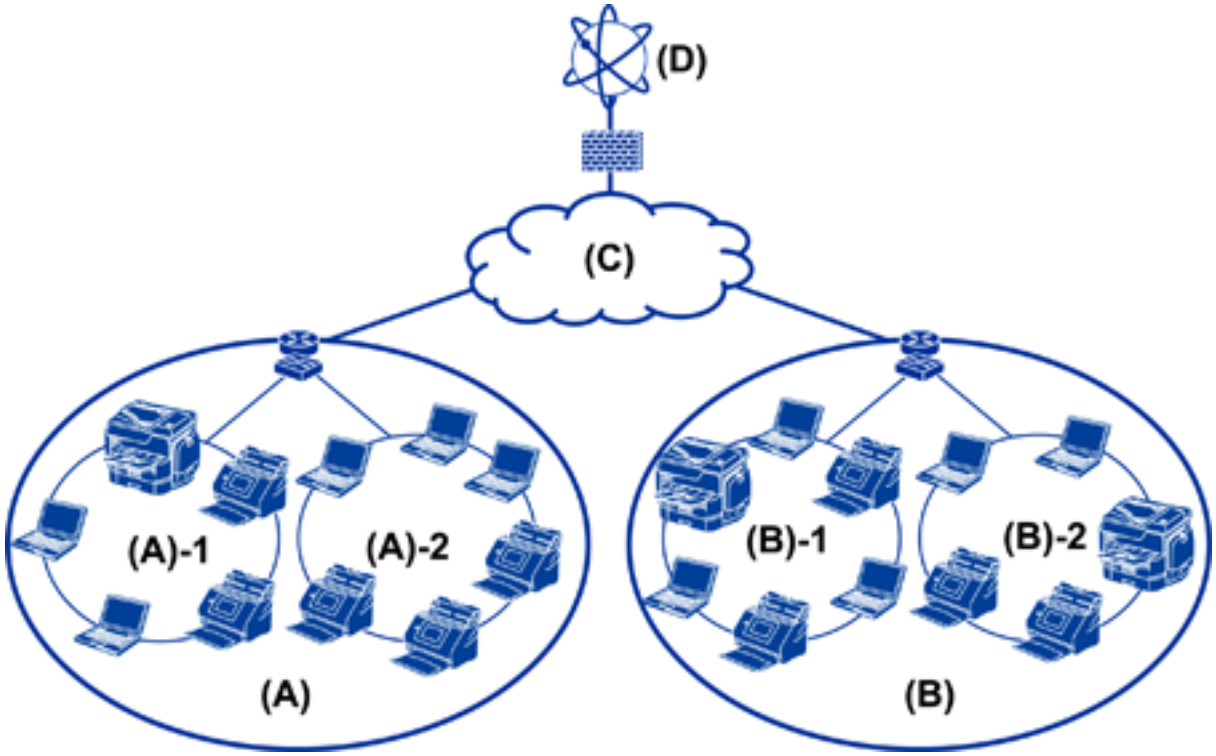
Administratoren foretar innstillinger av nettverkstilkoblingen, konfigurasjon og vedlikehold for skanneren, slik at de er tilgjengelige for brukerne.

1. Klargjøring
   - ❏ Samling av informasjon om nettverksinnstillinger
   - ❏ Valg av tilkoblingsmetode
2. Tilkobling
   - ❏ Nettverkstilkobling fra skannerens kontrollpanel
3. Innstilling av funksjoner
   - ❏ Innstillinger av skannerdriver
   - ❏ Andre avanserte innstillinger
4. Sikkerhetsinnstillinger
   - ❏ Administratorinnstillinger
   - ❏ SSL/TLS
   - ❏ Protokollkontroll
   - ❏ Avanserte sikkerhetsinnstillinger (alternativ)
5. Drift og administrasjon
   - ❏ Sjekke enhetstatus
   - ❏ Håndtering av nødtilfeller
   - ❏ Sikkerhetskopiering av enhetsinnstillinger

Relatert informasjon

➡ “Forberedelse” på side 10
➡ “Tilkobling” på side 15
➡ “Innstillinger av funksjoner” på side 22
➡ “Grunnleggende sikkerhetsinnstillinger” på side 32
➡ “Drifts- og administrasjonsinnstillinger” på side 40

Eksempel på nettverksmiljø



(A): Office 1

❏ (A) – 1: LAN 1

❏ (A) – 2: LAN 2

(B): Office 2

❏ (B) – 1: LAN 1

❏ (B) – 2: LAN 2

(C): WAN

(D): Internet

Introduksjon til eksempel på innstillinger for skannertilkobling

Det er i hovedsak to tilkoblingstyper, avhengig av hvordan du bruker skanneren. Begge vil koble skanneren til nettverket med datamaskinen via hubben.

❏ Server/klient-tilkobling (skanner med Windows-server, jobb-behandling)

❏ Node-til-node-tilkobling (direkte tilkobling etter klientdatamaskin)

Relatert informasjon

➡ “Server/klient-tilkobling” på side 12

➡ “Node-til-node-tilkobling” på side 12

Server/klient-tilkobling

Sentraliser skanner og prosjektstyring med Document Capture Pro Server installert på serveren. Det er mest egnet for arbeid som bruker flere skannere for å skanne et stort antall dokumenter i et bestemt format.

Relatert informasjon

➡ "Definisjoner på termer som brukes i denne veiledningen" på side 8

Node-til-node-tilkobling

Bruk en individuell skanner med en skannerdriver slik som Epson Scan 2 installert på klientdatamaskinen. Å installere Document Capture Pro (Document Capture) på klientmaskinen lar deg kjøre jobber på skannerens individuelle klientmaskiner.

Relatert informasjon

➡ "Definisjoner på termer som brukes i denne veiledningen" på side 8

Opprette forbindelse med et nettverk

Informasjonssamling i tilkoblingsinnstilling

Du må ha en IP-adresse, gateway-adresse, o.l. for å koble til Internett. Sjekk følgende på forhånd.

Divisjoner	Artikler	Merk
Enhetens tilkoblingsmetode	❏ Ethernet	Bruk en kabel i kategori 5e eller høyere STP (skjermet, tvunnet parkabel) for Ethernet-tilkobling.
LAN-tilkoblingsinformasjon	❏ IP-adresse ❏ Nettverksmaske ❏ Standard gateway	Hvis du angir IP-adresse automatisk ved å bruke DHCP-funksjonen på ruteren, kreves ikke dette.
DNS-serverinformasjon	❏ IP-adresse for primær DNS ❏ IP-adresse for sekundær DNS	Hvis du bruker statisk IP-adresse som IP-adresse, konfigurerer du DNS-server. Konfigurer ved automatisk tilordning ved å bruke DHCP-funksjon og når DNS-server ikke kan tilordnes automatisk.
Proxy-serverinformasjon	❏ Proxy-servernavn ❏ Portnummer	Konfigurer ved bruk av proxy-server for Internett-tilkobling samt ved bruk av Epson Connect-tjenesten eller fastvarens automatiske oppdateringsfunksjon.

Skannerspesifikasjoner

Spesifikasjonen som skanneren støtter er standard eller tilkoblingsmodus. Se *Brukerhåndbok*.

Bruke portnummer

Se "Bilag" for å finne portnummeret som skanneren bruker.

Relatert informasjon

➡ “Bruke porten for skanneren” på side 60

Type IP-adressetildeling

Det finnes to typer tildeling av IP-adresse på skanneren.

Statisk IP-adresse:

Tildel forhåndsbestemt unik IP-adresse til skanneren.

IP-adressen endres ikke selv når skanneren eller tureren slås av, så du kan administrere enheten med IP-adresse.

Denne typen er egnet for et nettverk hvor flere skannere administreres, slik som et stort kontor eller en skole.

Automatisk tildeling med DHCP-funksjon:

Korrekt IP-adresse tildeles automatisk når kommunikasjonen mellom skanneren og ruteren som støtter DHCP-funksjon er vellykket.

Dersom det ikke er praktisk å endre IP-adresse for en bestemt enhet, kan du reservere IP-adressen på forhånd og så tildele den.

DNS-server og proxy-server

Hvis du bruker en Internett-tilkoblingstjeneste, konfigurerer du DNS-server. Hvis du ikke konfigurerer en, vil du spesifisere IP-adresse for tilgang, da navneløsning kanskje ikke vil godkjennes.

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.

Du kan nekte tilgang for en bestemt URL ved hjelp av filtreringsfunksjonen, ettersom proxy-serveren er i stand til å kontrollere innholdet i kommunikasjonen.

Metode for innstilling av nettverkstilkobling

For tilkoblingsinnstillinger av skannerens IP-adresse, nettverksmaske og standard gateway, gjør du følgende.

Bruke kontrollpanelet:

Konfigurer innstillingene ved hjelp av skriverens kontrollpanel for hver skanner. Koble til nettverket etter å ha konfigurert skannerens tilkoblingsinnstillinger.

Bruke installasjonsprogrammet:

Hvis installasjonsprogrammet brukes blir skannerens nettverk og klientmaskinen konfigurert automatisk. Innstillingen gjøres ved å følge installasjonsveiledningen, selv om du ikke har kjennskap til nettverket.

Bruke et verktøy:

Bruke et verktøy fra administratorens datamaskin. Du kan oppdage en skanner og deretter konfigurere skanneren eller opprette en SYLK-fil for å foreta satsvise innstillinger av skannere. Du kan konfigurere flere skannere, men de må være koblet til fysisk med en Ethernet-kabel før du de stilles inn. Derfor anbefales dette dersom du kan bygge Ethernet som innstilling.

Relatert informasjon

➡ “Koble til nettverket fra kontrollpanelet” på side 15

➡ “Koble til nettverket ved å bruke installasjonsprogrammet” på side 19

➡ “Tilordne IP-adresse ved å bruke EpsonNet Config” på side 56

Tilkobling

Dette kapittelet forklarer miljøet eller prosedyren som kreves for å koble skanneren til nettverket.

Koble til et nettverk

Koble til nettverket fra kontrollpanelet

Koble skanneren til nettverket ved å bruke kontrollpanelet på skanneren.

Se *Brukerhåndbok* for mer informasjon om skannerens kontrollpanel.

Tilordne IP-adressen

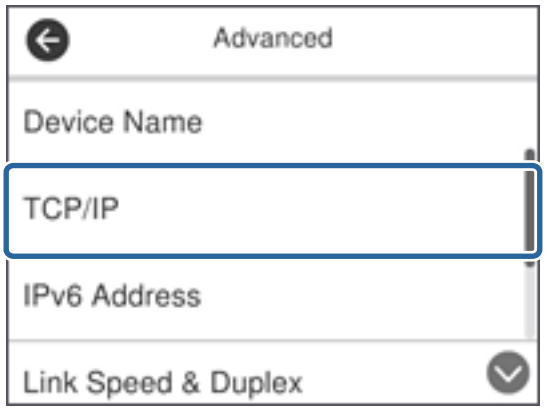
Still inn grunnleggende elementer som IP-adresse, Nettverksmaske og Standard gateway.

1. Slå av skanneren.
2. Brett opp skjermen mot venstre på skannerens kontrollpanel, og trykk så **Innst.**.

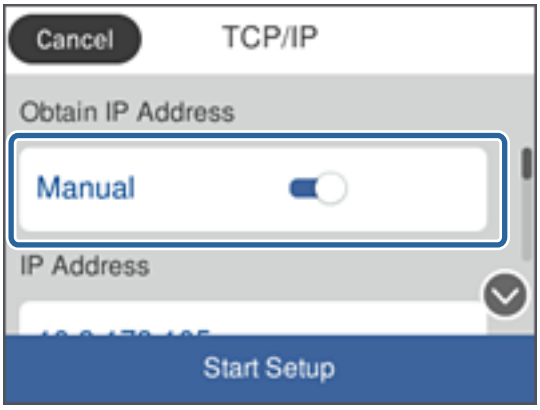
3. Trykk **Nettverksinnstillinger** > **Endre innstillinger**.

   Hvis elementet ikke vises, vender du skjermen opp for å se det.

4. Trykk **TCP/IP**.

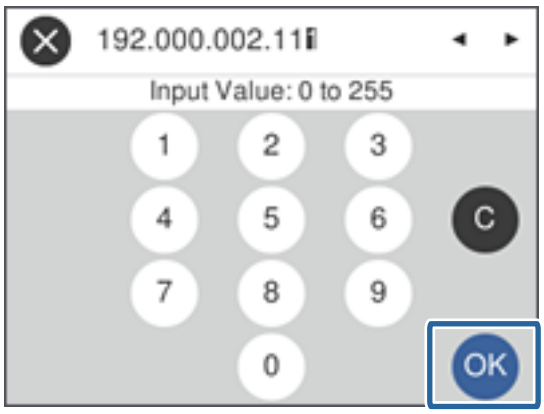


5. Velg **Manuell** ved **Skaff IP-adresse**.



Merknad:
*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 6 til 7 inn automatisk. Gå derfor til trinn 8.*

6. Trykk på **IP-adresse**-feltet, skriv inn IP-adressen ved å bruke tastaturet vist på skjermen, og trykk så **OK**.



Bekreft verdien som ble vist på forrige skjerm.

7. Konfigurer **Nettverksmaske** og **Standard gateway**.

Bekreft verdien som ble vist på forrige skjerm.

Merknad:
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.*

8. Trykk på **Primær DNS**-feltet for **DNS-server**, skriv inn adressen for primær DNS-server ved å bruke tastaturet vist på skjermen, og trykk så **OK**.

   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****, kan du gå til trinn 10.*

9. Trykk på **Sekundær DNS**-feltet, skriv inn adressen for sekundær DNS-server ved å bruke tastaturet vist på skjermen, og trykk så **OK**.

   Bekreft verdien som ble vist på forrige skjerm.

10. Trykk **Start oppsett**.

11. Trykk **Lukk** på bekreftelsesskjermen.

    Skjermen lukkes automatisk etter en viss tid hvis du ikke trykker **Lukk**.

Koble til Ethernet

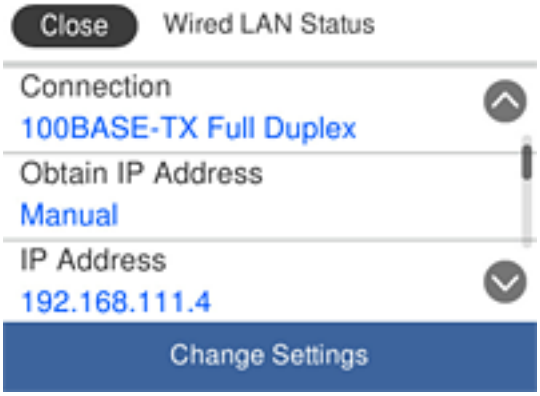
Koble skanneren til nettverket ved å bruke en Ethernet-kabel, og kontroller tilkoblingen.

1. Koble skanneren til hub (L2-svitsj) med en Ethernet-kabel.

   Ikonet på hjem-skjermen endres til  .

2. Trykk  på startsiden.

3. Vipp skjermen oppover, og sørg deretter for at tilkoblingsstatusen og IP-adressen er riktig.



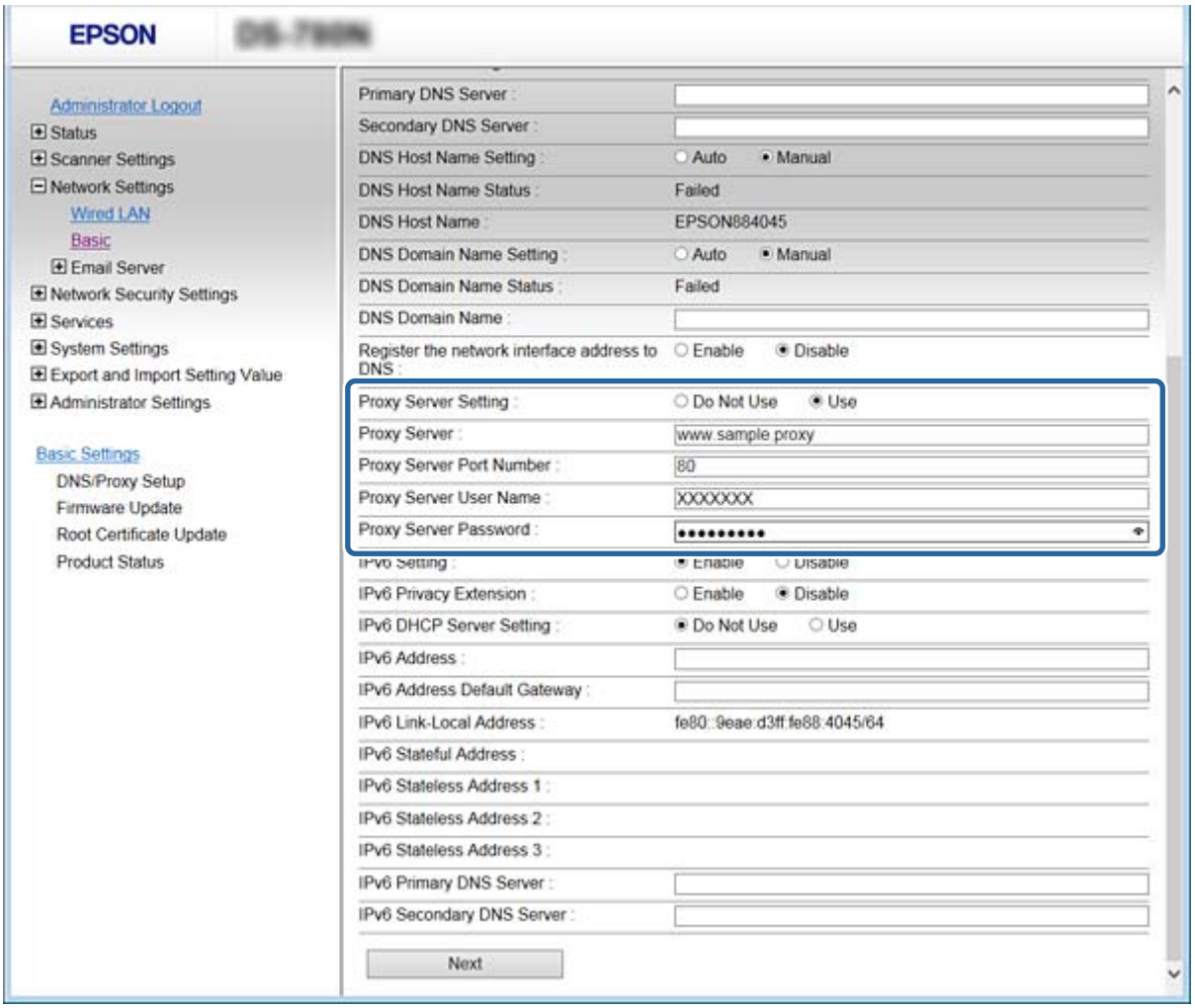
Angi proxy-server

Proxy-serveren kan ikke angis på panelet. Konfigurer ved hjelp av Web Config.

1. Gå inn på Web Config og velg **Network Settings** > **Basic**.
2. Velg **Use** i **Proxy Server Setting**.
3. Angi proxy-server i IPv4-adresse eller FQDN-format i **Proxyserver**, og angi deretter portnummeret i **Proxy Server Port Number**.

   For proxy-servere som krever godkjenning, angi Proxy-server autentiseringsbrukernavn og Proxy-server autentiseringspassord.

4. Klikk på **Next**-knappen.



5. Bekreft innstillingene, og klikk deretter **Innst.**.

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23

Koble til nettverket ved å bruke installasjonsprogrammet

Vi anbefaler bruk av installasjonsprogrammet for å koble skanneren til en datamaskin. Du kan kjøre installasjonsprogrammet ved å bruke en av metodene nedenfor.

❏ Konfigurere fra nettstedet

Gå til følgende nettside og tast inn produktnavnet. Gå til **Oppsett**, og start deretter konfigurasjonen.

http://epson.sn

❏ Konfigurere ved hjelp av programvareplaten (kun for modeller som ble levert med programvareplate og for brukere med datamaskiner med diskstasjon.)

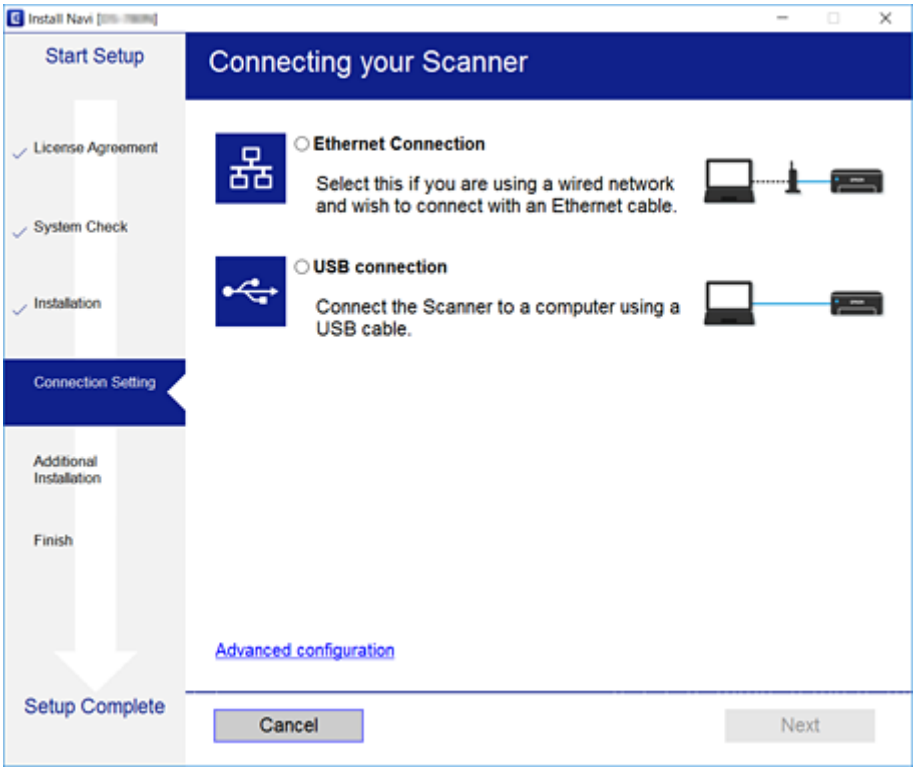
Sett inn programvareplaten i datamaskinen, og følg deretter instruksjonene på skjermen.

Velge tilkoblingsmetoder

Følg instruksjonene på skjermen inntil følgende skjerm vises, hvor du velger tilkoblingsmetode for å koble skanneren til datamaskinen.

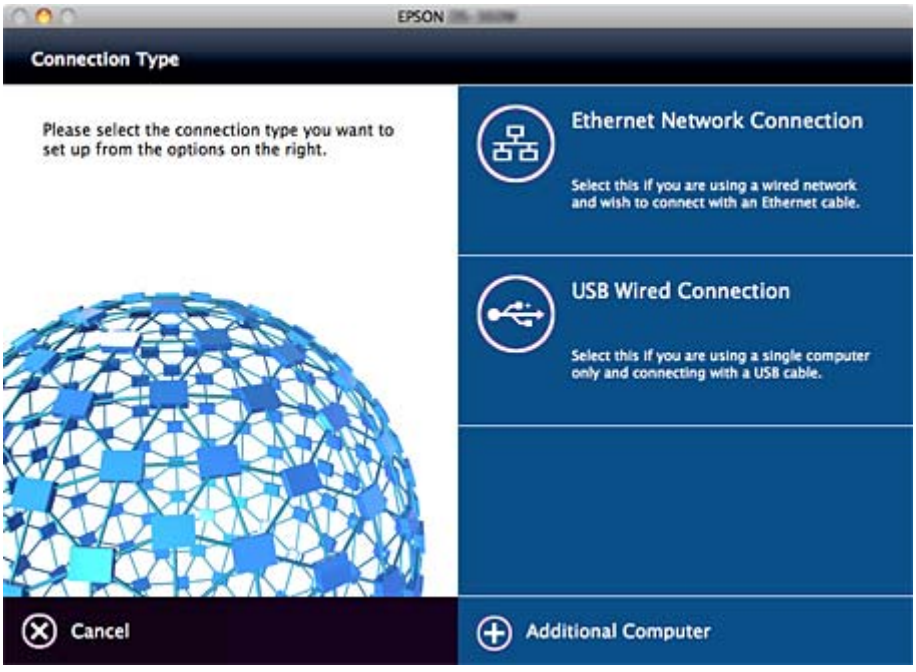
❏ Windows

Velg tilkoblingsmetode og klikk deretter **Neste**.



❏ Mac OS

Velg tilkoblingstype.



Tilkobling

Følg instruksjonene på skjermen. Påkrevd programvare er installert.

Innstillinger av funksjoner

Dette kapittelet forklarer førstegangsinnstillinger som må foretas for å kunne bruke hver funksjon på enheten.

Programvare for innstilling

I dette emnet forklares prosedyren for å foreta innstillinger fra administratorens datamaskin ved bruk av Web Config.

Web Config (websiden for enheten)

Om Web Config

Web Config er et nettleserbasert program for å konfigurere skannerens innstillinger.

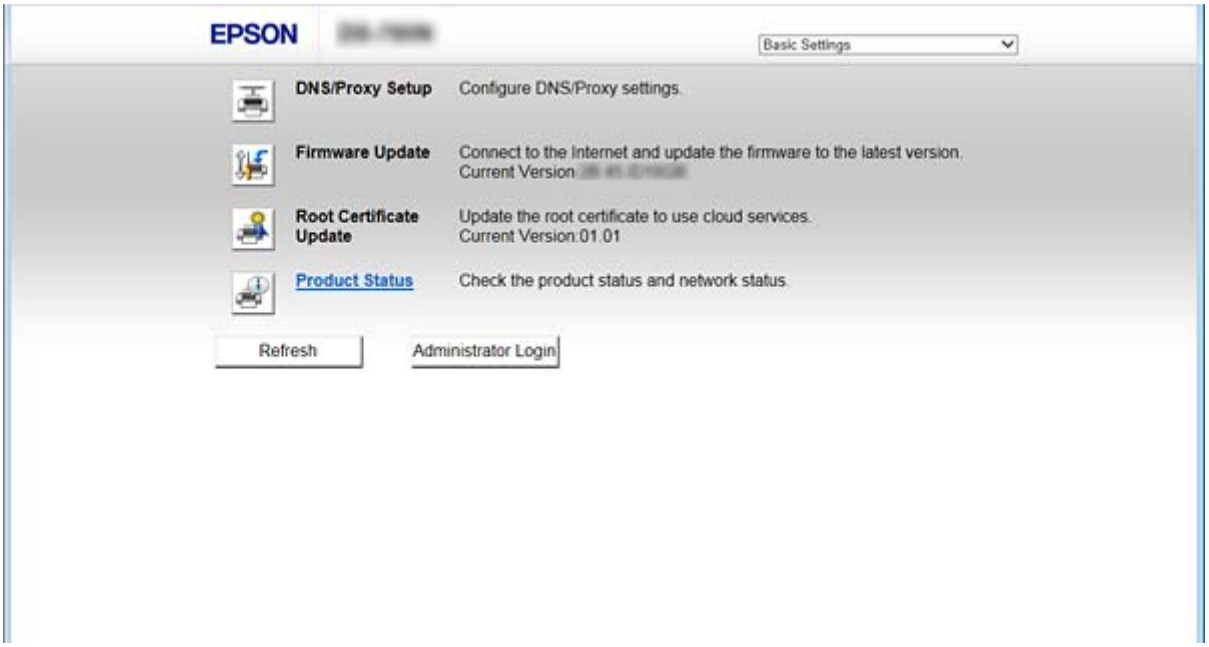
Vil du ha tilgang til Web Config, må du først ha tilordnet en IP-adresse til skanneren.

Merknad:
Du kan låse innstillingene ved å konfigurere administratorpassordet til skanneren.

Nedenfor finner du to innstillingssider.

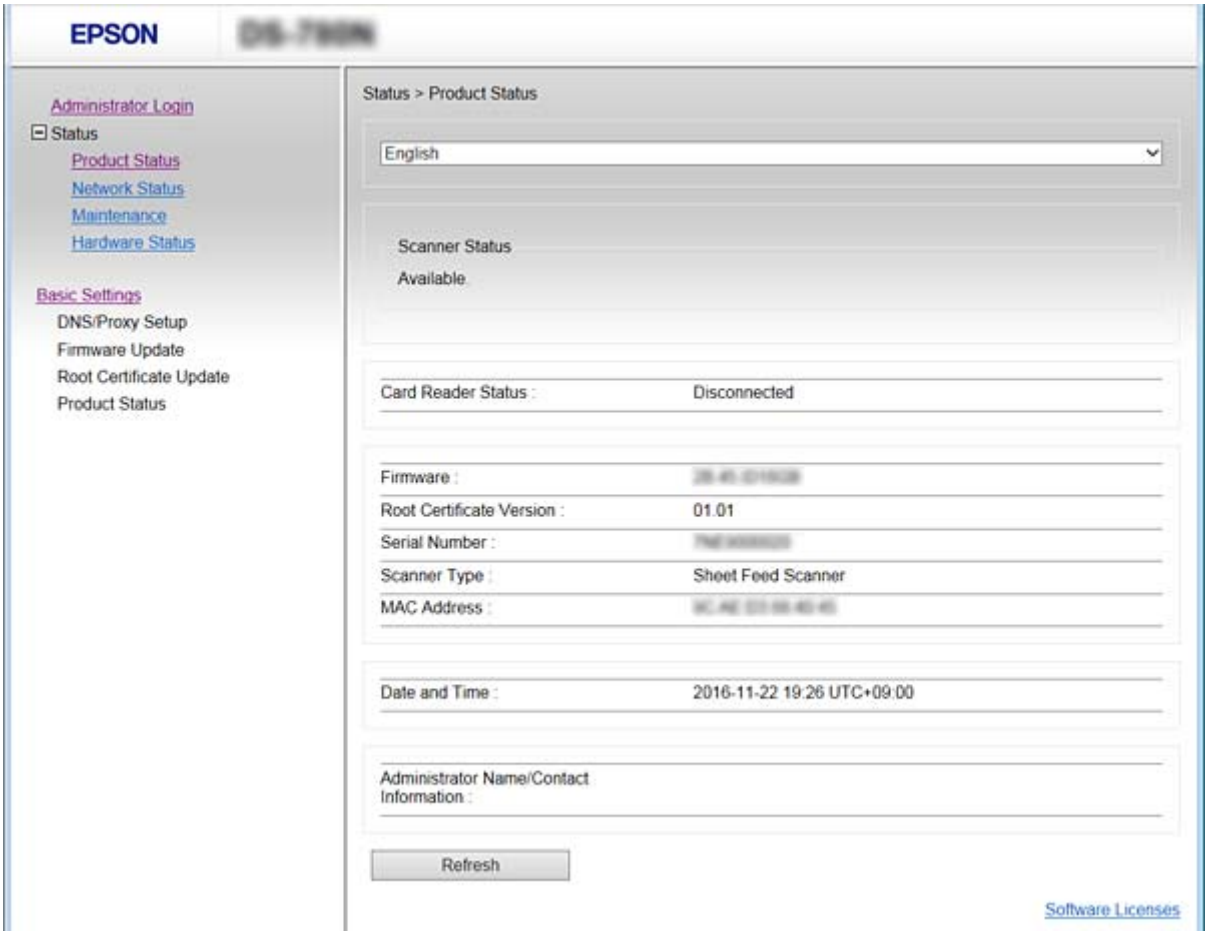
❏ **Basic Settings**

Du kan konfigurere grunnleggende innstillinger for skanneren.



❏ **Advanced Settings**

Du kan konfigurere avanserte innstillinger for skanneren. Denne siden er i hovedsak beregnet på administratorer.



Få tilgang til Web Config

Skriv inn skannerens IP-adresse i en nettleser. JavaScript må være aktivert. Når du går inn på Web Config via HTTPS vil en advarsel vises i nettleseren, da et selv-signert sertifikat, lagret i skanneren, blir brukt.

❏ Få tilgang via HTTPS

IPv4: https://<skannerens IP-adresse> (uten < >)

IPv6: https://[skannerens IP-adresse]/ (med [ ])

❏ Få tilgang via HTTP

IPv4: http://<skannerens IP-adresse> (uten < >)

IPv6: http://[skannerens IP-adresse]/ (med [ ])

Merknad:

❏ *Eksempler*

IPv4:

https://192.0.2.111/

http://192.0.2.111/

IPv6:

https://[2001:db8::1000:1]/

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

❏ *Hvis skannernavnet er registrert med DNS-serveren, kan du bruke skannernavnet i stedet for skannerens IP-adresse.*

Relatert informasjon

➡ "SSL/TLS-kommunikasjon med skanneren" på side 63

➡ "Om digital sertifisering" på side 63

Bruke skannefunksjoner

Avhengig av hvordan du bruker skanneren, må du installere følgende programvare og foreta innstillinger ved hjelp av den.

❏ **Skanne fra datamaskinen**

- ❏ Bekreft gyldigheten av nettverksskanningstjeneste med Web Config (gyldig ved fabrikkforsendelse).
- ❏ Installer Epson Scan 2 på datamaskinen og angi IP-adressen
- ❏ Når du skanner ved hjelp av jobber, installer Document Capture Pro (Document Capture) og angi jobbinnstillinger.

❏ **Skanne fra betjeningspanelet**

- ❏ Når du bruker Document Capture Pro eller Document Capture Pro Server:

  Installer Document Capture Pro eller Document Capture Pro Server

  DCP-innstilling (server-modus, klientmodus).
- ❏ Ved bruk av WSD-protokollen:

  Bekreft gyldigheten av WSD på Web Config eller betjeningspanelet (gyldig ved fabrikkforsendelse)

  Andre enhetsinnstillinger (Windows-datamaskin).

Skanning fra en datamaskin

Installer programvaren og kontroller at nettverksskanning-tjenesten via et nettverk fra datamaskinen.

Relatert informasjon

➡ "Programvare som må installeres" på side 25

➡ "Aktiver nettverksskanning" på side 25

Programvare som må installeres

❏ Epson Scan 2

Dette er en skannerdriver. Hvis du bruker enheten fra en datamaskin, installerer du driveren på hver av klientdatamaskinene. Hvis Document Capture Pro/Document Capture er installert, kan du utføre handlingene som er tildelt knappene på enheten.

Med EpsonNet SetupManager, kan skriverdrivere også bli distribuert sammen i pakker.

❏ Document Capture Pro (Windows)/Document Capture (Mac OS)

Installer på klientdatamaskinen. Du kan hente opp og utføre jobber som er registrert på en datamaskin med Document Capture Pro/Document Capture installert på nettverket fra datamaskinen og skannerens betjeningspanel.

Du kan også skanne fra datamaskinen via nettverket. Epson Scan 2 kreves for å skanne.

Relatert informasjon

➡ "EpsonNet SetupManager" på side 56

Sett skannerens IP-adresse til Epson Scan 2

Angi IP-adressen til skanneren slik at skanneren kan brukes i nettverket.

1. Start **Epson Scan 2 Utility** fra **Start** > **Alle programmer** > **EPSON** > **Epson Scan 2**.

   Hvis en annen skanner allerede er registrert, går du til trinn 2.

   Hvis den ikke er registrert, gå til trinn 4.

2. Klikk ▼ på **Skanner**.
3. Klikk på **Innst.**.
4. Klikk **Aktiver redigering** og klikk deretter **Legg til**.
5. Velg skannerens modellnavn fra **Modell**.
6. Velg IP-adressen til skanneren som skal brukes fra **Adresse** i **Søk etter nettverk**.

   Klikk  og klikk  for å oppdatere listen. Hvis du ikke kan finne IP-adressen til skanneren, velg **Skriv inn adresse** og angi IP-adressen.

7. Klikk på **Legg til**.
8. Klikk på **OK**.

Aktiver nettverksskanning

Du kan stille inn nettverksskanningtjenesten når du skanner fra en klientdatamaskin over nettverket. Standarinnstillingen er aktivert.

1. Åpne Web Config og velg **Services** > **Network Scan**.

2. Kontroller at **Enable scanning** av **EPSON Scan** er valgt.

   Hvis det er krysset av, er oppgaven fullført. Lukk Web Config.

   Hvis det ikke er valgt, velg det og gå til neste trinn.

3. Klikk på **Next**.

4. Klikk på **OK**.

   Nettverksforbindelsen gjenopprettes og innstillingene aktiveres.

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23

Skanning ved bruk av kontrollpanelet

Skann til mappe-funksjonen og skanning til e-post-funksjonen ved hjelp av skannerens kontrollpanel, samt overføring av skanningsresultater til e-post, mapper, etc. utføres ved å kjøre en jobb fra datamaskinen.

Ved overføring av skanneresultater, sett opp jobben med Document Capture Pro Server eller Document Capture Pro.

For mer informasjon om innstillinger og sette opp jobben, se dokumentasjonen eller hjelp for Document Capture Pro Server eller Document Capture Pro.

Relatert informasjon

➡ "Document Capture Pro Server/Document Capture Pro innstillinger" på side 26

➡ "Innstilling av servere og mapper" på side 27

Programvare å installere på datamaskinen

❏ **Document Capture Pro Server**

Dette er server-versjonen av Document Capture Pro. Installer det på en Windows-server. Flere enheter og jobber kan styres sentralt av serveren. Jobber kan kjøres samtidig fra flere skannere.

Ved å bruke den sertifiserte versjonen av Document Capture Pro Server, kan du administrere jobber og skannehistorikk knyttet til brukere og grupper.

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

❏ **Document Capture Pro (Windows)/Document Capture (Mac OS)**

Akkurat som skanning fra en datamaskin, kan du hente opp jobbene som er registrert på maskinen fra kontrollpanelet og utføre dem. Det er ikke mulig å kjøre datajobber samtidig fra flere skannere.

Document Capture Pro Server/Document Capture Pro innstillinger

Foreta innstillinger for å bruke skannefunksjonen fra skannerens betjeningspanel.

1. Gå inn på Web Config og velg **Services** > **Document Capture Pro**.

2. Velg **Driftsmodus**.

   ❏ Server Mode:

   Velg dette når du bruker Document Capture Pro Server eller når du bruker Document Capture Pro bare for jobber som er angitt for en bestemt datamaskin.

   ❏ Client Mode:

   Angi dette når du velger jobb-innstillingene av Document Capture Pro (Document Capture) installert på hver klientmaskin i nettverket uten å spesifisere datamaskinen.

3. Angi følgende i henhold til den valgte modusen.

   ❏ Server Mode:

   I **Server Address**, angi serveren som Document Capture Pro Server er installert på. Det kan være 2 til 252 tegn i IPv4, IPv6, vertsnavn, FQDN-format. I FQDN-format, US-ASCII-bokstaver, tall, alfabeter og bindestrek (unntatt ledende og etterfølgende) kan brukes.

   ❏ Client Mode:

   Angi **Group Settings** for å bruke en skannergruppen spesifisert fra Document Capture Pro (Document Capture).

4. Klikk på **Innst.**.

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23

Innstilling av servere og mapper

Document Capture Pro og Document Capture Pro Server lagrer de skannede dataene til serveren eller klientmaskinen en gang og bruker overføringsfunksjonen til å utføre funksjonen skann til mappe og skann til e-post-funksjonen.

Du trenger rettigheter og informasjon til å overføre fra datamaskinen der Document Capture Pro, Document Capture Pro Server er installert på datamaskinen eller skytjenesten.

Forbered informasjonen om den funksjonen du vil bruke, og viser til følgende.

Du kan foreta innstillinger for disse funksjonene ved hjelp av Document Capture Pro eller Document Capture Pro Server. For mer informasjon om innstillingene, se dokumentasjonen eller hjelp for Document Capture Pro Server eller Document Capture Pro.

Navn	Innstillinger	Krav
Skann til nettverksmappe (SMB)	Opprett og konfigurer deling av lagringsmappen	Den administrative brukerkontoen til datamaskinen som oppretter lagringsmappene.
	Destinasjon for Skann til nettverksmappe (SMB)	Brukernavn og passord for å logge deg på datamaskinen som lagringsmappen er installert på, og tillatelse til å oppdatere lagringsmappen.
Skann til nettverksmappe (FTP)	Innstilling av FTP-serverinnlogging	Innloggingsinformasjon for FTP-serveren og tillatelse til å oppdatere lagringsmappen.

Navn	Innstillinger	Krav
Skann til e-post	Innstilling av e-postserver	Innstillingsinformasjon for e-postserver
Skann til Document Capture Pro (ved bruk av Document Capture Pro Server)	Oppsett for å logge på nettskytjenester	Internett-tilkoblingsmiljø Registrering av konto for skytjenester

Bruk WSD-skann (bare Windows)

Hvis datamaskinen bruker Windows Vista eller nyere, kan du bruke WSD-skann.

Når WSD-protokollen kan brukes, vil **Datamaskin (WSD)**-menyen vises på skannerens kontrollpanel.

1. Gå inn på Web Config og velg **Services** > **Protocol**.
2. Kontroller at **Enable WSD** er krysset av i **WSD Settings**.
   Hvis det er krysset av, er din oppgave fullført og du kan lukke Web Config.
   Hvis det ikke er krysset av, kryss det av og gå videre til neste trinn.
3. Klikk på **Next**-knappen.
4. Bekreft innstillingene, og klikk **Innst.**.

Foreta systemendringer

Foreta systeminnstillinger på kontrollpanelet

Angi lysstyrken på skjermen

Angi lysstyrken på LCD-skjermen.

1. Trykk **Innst.** på startsiden.
2. Trykk **Felles innstillinger** > **LCD-lysstyrke**.
3. Trykk  eller  for å justere lysstyrken.
   Du kan justere fra 1 til 9.
4. Trykk **OK**.

Angi lyd

Angi panelbetjeningslyd og feillyd.

1. Trykk **Innst.** på startsiden.
2. Trykk **Felles innstillinger** > **Lyd**.
3. Angi de følgende alternativene etter behov.
   - ❏ Driftslyd
     Angi volumet på betjeningslyden på betjeningspanelet.
   - ❏ Feillyd
     Angi volumet på feillyden.
4. Trykk **OK**.

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23

Oppdag dobbeltmating av original

Bestem funksjonen for å oppdage dobbeltmating av dokumentet som skal skannes, og for å stoppe skanningen når det oppstår flere matinger.

For å skanne originaler som anses å være fler-matet, for eksempel konvolutter eller papir med klistremerker, sett dem til off.

Merknad:
Det kan også angis fra Web Config eller Epson Scan 2.

1. Trykk **Innst.** på startsiden.
2. Trykk **Eksterne skanneinnstillinger** > **Ultrasonisk registr. av dobbeltmating**.
3. Trykk **Ultrasonisk registr. av dobbeltmating** for å slå den av eller på.
4. Trykk **Lukk**.

Angi lav hastighetsmodus

Angi til å skanne ved lav hastighet slik at det ikke oppstår papirstopp når du skanner tynne dokumenter som slips.

1. Trykk **Innst.** på startsiden.
2. Trykk **Eksterne skanneinnstillinger** > **Sakte**.
3. Trykk **Sakte** for å slå den av eller på.
4. Trykk **Lukk**.

Foreta systemendringer med Web Config

Strømsparingsinnstillinger ved inaktivitet

Foreta innstillinger av strømsparing for perioder når skanneren ikke brukes. Angi tidspunkt avhengig av bruksmiljøet ditt.

Merknad:
Du kan også foreta strømsparingsinnstillinger på skannerens kontrollpanel.

1. Gå inn på Web Config og velg **System Settings** > **Power Saving**.
2. Angi tidspunkt for når **Sleep Timer** skal gå i strømsparingsmodus ved inaktivitet.

   Du kan angi opptil 240 minutter med inkrementer på hele minutter.
3. Velg slukningstid for **Power Off Timer**.
4. Klikk på **OK**.

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23

Innstilling av kontrollpanelet

Konfigurasjon av skannerens kontrollpanel. Du kan konfigurere på følgende vis.

1. Gå inn på Web Config og velg **System Settings** > **Control Panel**.
2. Angi de følgende alternativene etter behov.
   - ❏ Language

     Velg språk for kontrollpanelet.
   - ❏ Panel Lock

     Hvis du velger **ON**, vil administratorpassord kreves når du utfører en handling som krever administratorens godkjenning. Hvis administratorpassord ikke er angitt, vil panellåsen være deaktivert.
   - ❏ Operation Timeout

     Hvis du velger **ON**, vil du automatisk bli avlogget og sendes til startskjermen dersom ingen aktivitet registreres i en viss periode mens du er pålogget som administrator.

     Du kan angi mellom 10 sekunder og 240 minutter med inkrementer på ett sekund.
3. Klikk på **OK**.

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23

Angi begrensning av eksternt grensesnitt

Du kan begrense USB-porten for tilkobling av datamaskin. Angi det til å begrense skanning annet enn via nettverket.

1. Gå inn på Web Config og velg **System Settings** > **External Interface**.
2. Velg **Enable** eller **Disable**.

   For å begrense, velg **Disable**.
3. Trykk **OK**.

Synkronisering av dato og klokkeslett med tidsserveren

Hvis du bruker CA-sertifikat kan du forhindre at det oppstår problemer med tidsinnstillingen.

1. Gå inn på Web Config og velg **System Settings** > **Date and Time** > **Time Server**.
2. Velg **Use** ved **Use Time Server**.
3. Angi tidsserveradresse for **Time Server Address**.

   Du kan bruke IPv4-, IPv6- eller FQDN-format. Skriv inn maksimalt 252 tegn. Hvis du ikke angir dette, lar du det stå tomt.
4. Skriv inn **Update Interval (min)**.

   Du kan angi opptil 10 800 minutter med inkrementer på hele minutter.
5. Klikk på **OK**.

   Merknad:
   *Du kan sjekke tilkoblingsstatus på tidsserveren på **Time Server Status**.*

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23

Grunnleggende sikkerhetsinnstillinger

Dette kapittelet forklarer de grunnleggende sikkerhetsinnstillingene som ikke krever et spesielt miljø.

Introduksjon til de grunnleggende sikkerhetsfunksjonene

Vi introduserer de grunnleggende sikkerhetsfunksjonene på Epson-enheter.

Funksjonsnavn	Funksjonstype	Hva skal stilles inn	Hva skal forebygges
Konfigurasjon av administratorpassord	Lås innstillinger knyttet til systemet, for eksempel nettverks- og USB-tilkoblingsinnstillingene, slik at de ikke kan endres med unntak av administratoren.	En administrator angir et passord for enheten. Konfigurasjoner og oppdateringer er tilgjengelig fra hvor som helst via Web Config, kontrollpanelet Epson Device Admin og EpsonNet Config.	Unngå ulovlig lesing og endring av informasjon som er lagret på enheten, slik som ID, passord, nettverksinnstillinger og kontakter. Reduser også et bredt spekter av sikkerhetsrisikoer som lekkasje av informasjon til nettverksmiljøet eller sikkerhetspolitikk.
SSL/TLS-kommunikasjon	Når du åpner en Epson-server på Internett fra en enhet, for eksempel kommunikasjon med en datamaskin via en nettleser eller fastvareoppdatering, er kommunikasjons innhold kryptert med SSL/TLS-kommunikasjon.	Få tak i et CA-signert sertifikat, og deretter importer det til skanneren.	Fjerning av en identifikasjon for enheten gjennom CA-signerte sertifikater forhindrer etterligning og uautorisert tilgang. I tillegg er kommunikasjonsinnholdet SSL/TLS-beskyttet, noe som forhindrer lekkasje av innholdet for utskriftsdata og installasjonsdata.
Kontrollprotokoller	Kontrollprotokoller brukes til kommunikasjon mellom enheter og datamaskiner, og aktiverer/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.

Relatert informasjon

➡ “Om Web Config” på side 22
➡ “EpsonNet Config” på side 55
➡ “Epson Device Admin” på side 55
➡ “Konfigurere administratorpassordet” på side 33
➡ “Kontrollprotokoller” på side 35

Konfigurere administratorpassordet

Når du angir administratorpassord vil andre brukere enn administrator kunne endre innstillingene for systemadministrasjon. Du kan angi og endre administratorpassord ved å bruke enten Web Config, skannerens kontrollpanel eller programvaren (Epson Device Admin eller EpsonNet Config). Når du bruker programvaren kan du se dokumentasjonen for hver programvare.

Relatert informasjon

➡ "Konfigurere administratorpassord fra kontrollpanelet" på side 33

➡ "Konfigurere administratorpassordet ved å bruke Web Config" på side 33

➡ "EpsonNet Config" på side 55

➡ "Epson Device Admin" på side 55

Konfigurere administratorpassord fra kontrollpanelet

Du kan angi administratorpassord fra skannerens kontrollpanel.

1. Trykk **Innst.** på startsiden.
2. Trykk **Systemadministrasjon** > **Administratorinnstillinger**.

   Hvis elementet ikke vises, vender du skjermen opp for å se det.
3. Trykk **Adminpassord** > **Registrer**.
4. Skriv inn et nytt passord og velg deretter **OK**.
5. Skriv inn passordet på nytt og velg deretter **OK**.
6. Trykk **OK** på bekreftelsesskjermen.

   Skjermen for administratorinnstillinger vises.
7. Trykk **Låsinnstilling** og trykk så **OK** på bekreftelsesskjermen.

   Låsinnstilling er satt til **På**, og administratorpassordet vil måtte oppgis når du bruker et låst menyelement.

Merknad:

❏ *Hvis du angir **Innst.** > **Felles innstillinger** > **Tidsavbrudd for handling** til **På**, vil skanneren logge av etter en viss periode uten registrert aktivitet på kontrollpanelet.*

❏ *Du kan endre eller slette administratorpassordet ved å velge **Endre** eller **Tilbakestill** på skjermen **Adminpassord**, og deretter angi administratorpassord.*

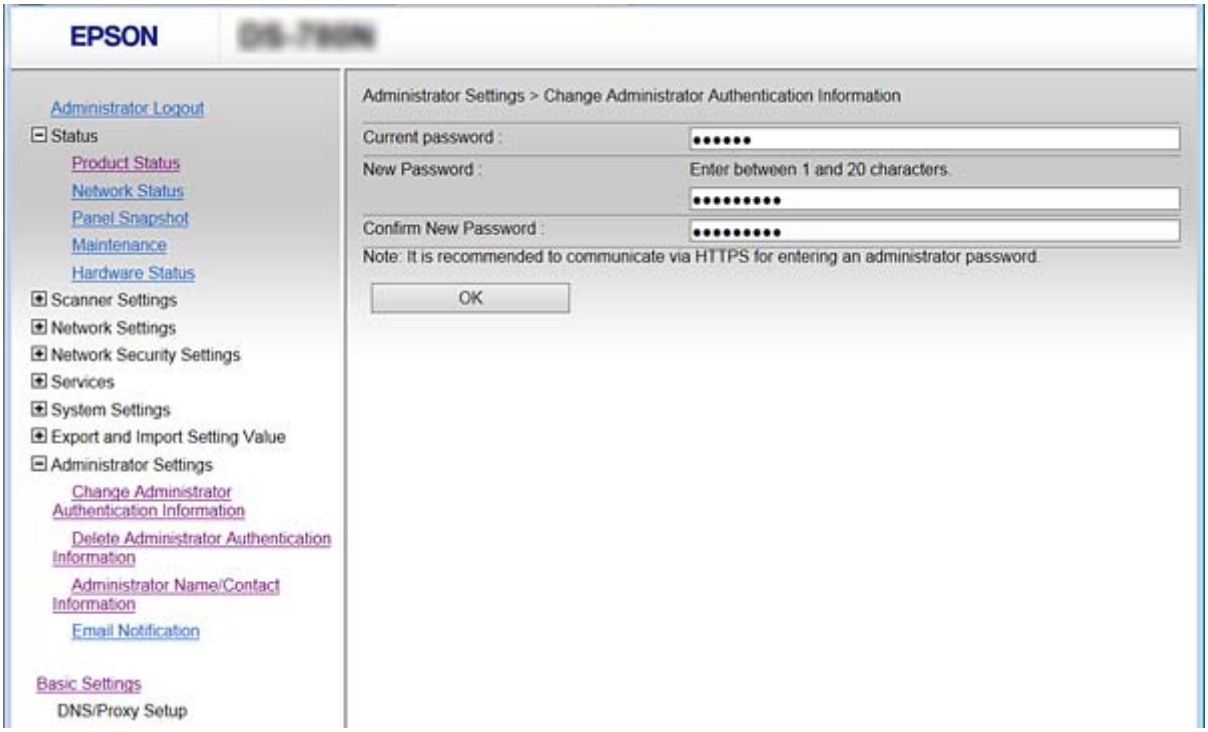
Konfigurere administratorpassordet ved å bruke Web Config

Du kan angi administratorpassord ved å bruke Web Config.

1. Gå inn på Web Config og velg **Administrator Settings** > **Change Administrator Authentication Information**.

2. Skriv inn et passord i **New Password** og **Confirm New Password**. Angi brukernavn om nødvendig.

   Hvis du vil endre til et nytt passord, skriv inn nåværende passord.



3. Velg **OK**.

   Merknad:

   ❏ *For å angi eller endre en låst meny klikker du **Administrator Login** og angir deretter administratorpassordet.*

   ❏ *For å slette administratorpassordet klikker du **Administrator Settings** > **Delete Administrator Authentication Information**, og angir deretter administratorpassordet.*

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23

Elementer som skal låses av administratorpassord

Administratorer har tilgang til å stille inn og endre innstillinger for alle enhetens funksjoner.

Og, hvis du angir passord på enheten, kan du låse den slik at du ikke kan endre elementer knyttet til enhetsbehandling.

Følgende elementer kan administratorer styre.

Artikkel	Beskrivelse
Skannerinnstillinger	Innstilling av dobbeltmating og lav hastighetsmodus.
Innstillinger for Ethernet-tilkobling	Endre navnet på enhetene og IP-adressen, still inn DNS-serveren eller proxy-server, og endringer av innstillinger for nettverkstilkoblinger.

Artikkel	Beskrivelse
Innstilling av brukertjenester	Konfigurasjon for å kontrollere kommunikasjonsprotokoller, nettverksskanning og Document Capture Pro-tjenester.
Innstilling av e-postserver	Konfigurasjon av en e-postserver som kommuniserer direkte med enhetene.
Sikkerhetsinnstilling	Innstillinger for nettverkssikkerhet, slik som SSL/TLS-kommunikasjon, IPsec/IP-filtrering og IEEE802.1X.
Oppdatering av rotsertifikat	Oppdatering av rotsertifikater som kreves for Document Capture Pro Server-godkjenning og fastvareoppdatering fra Web Config.
Fastvareoppdatering	Sjekk og oppdater fastfaren for enheter.
Tids- og timerinnstilling	Overgangstid for hvilemodus, automatisk slukning, dato/klokkeslett, timer for inaktivitet, andre timer-relaterte innstillinger.
Tilbakestill alle standardinnstillinger	Innstilling for tilbakestilling av skanneren til fabrikkinnstillinger.
Administratorinnstilling	Innstilling av administratorlås eller administratorpassord.
Innstilling av sertifisert enhet	ID-innstilling av godkjent enhet. Angi når du bruker skanneren på et godkjenningssystem som støtter godkjenningsenheter.

Kontrollprotokoller

Du kan skanne via ulike baner og protokoller. Du kan skanne ved hjelp av nettverksskanning fra et uspesifisert antall datamaskiner i nettverket. For eksempel er skanning med bare angitte baner og protokoller tillatt. Du kan redusere utilsiktede sikkerhetsrisikoer ved å begrense skanning via bestemte baner eller ved å kontrollere de tilgjengelige funksjonene.

Konfigurer protokollinnstillinger.

1. Gå inn på Web Config og velg **Services** > **Protocol**.
2. Konfigurer hvert element.
3. Klikk på **Next**.
4. Klikk på **OK**.

   Innstillingene brukes på skanneren.

Relatert informasjon

➡ “Få tilgang til Web Config” på side 23

➡ “Protokoller du kan Aktivere eller Deaktivere” på side 36

➡ “Innstillingselementer for protokoll” på side 37

Protokoller du kan Aktivere eller Deaktivere

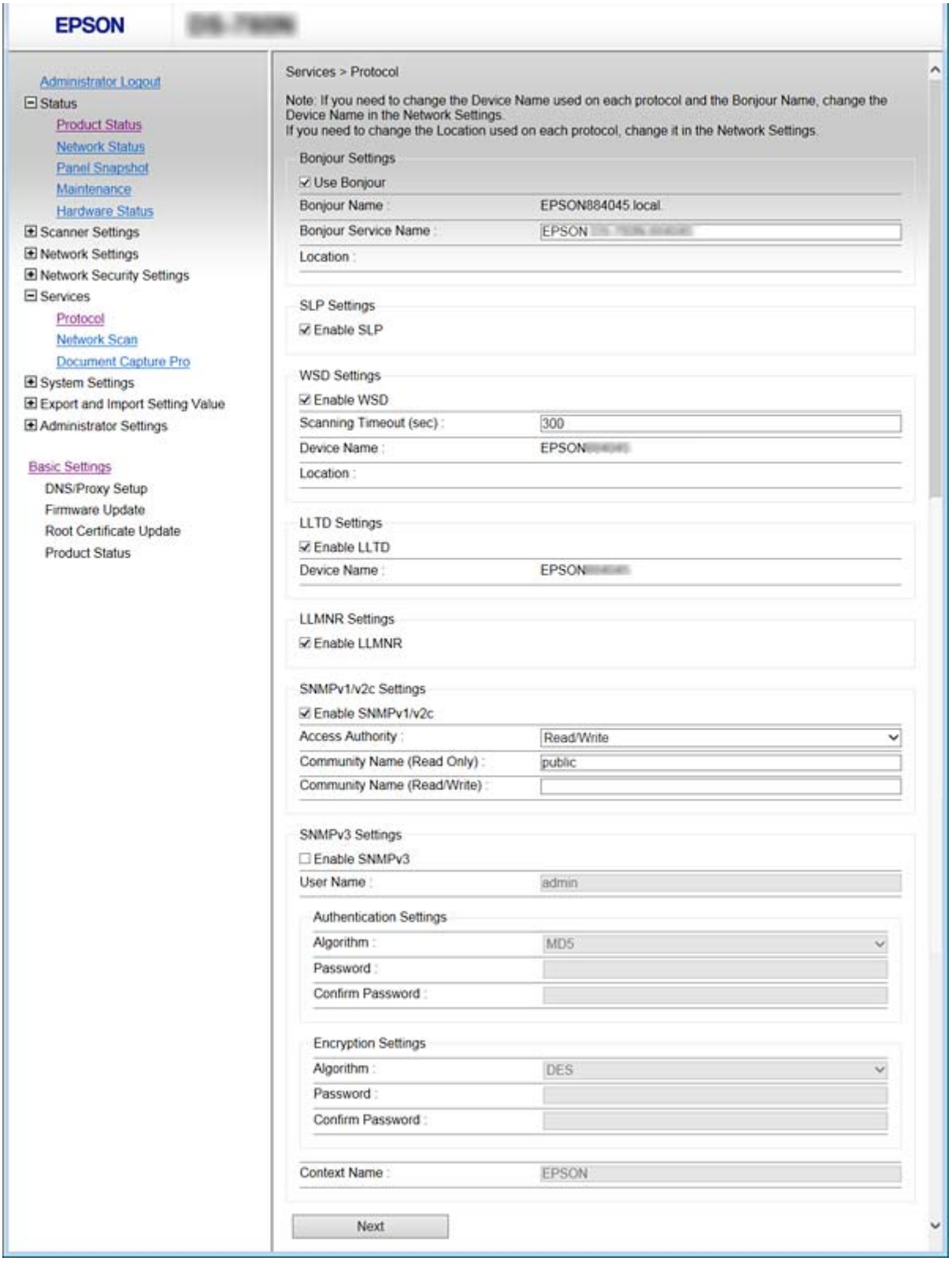
Protokoll	Beskrivelse
Bonjour Settings	Du kan angi om du vil bruke Bonjour. Bonjour brukes til å søke etter enheter, skanne, og så videre.
SLP Settings	Du kan aktivere eller deaktivere SLP-funksjonen. SLP anvendes for Epson Scan 2, og nettverkssøking i EpsonNet Config.
WSD Settings	Du kan aktivere eller deaktivere WSD-funksjonen. Når denne er aktivert, kan du legge til WSD-enheter eller skanne via WSD-porten.
LLTD Settings	Du kan aktivere eller deaktivere LLTD-funksjonen. Når denne er aktivert, vises den på nettverkskartet i Windows.
LLMNR Settings	Du kan aktivere eller deaktivere LLMNR-funksjonen. Når denne er aktivert, kan du bruke navneløsing uten NetBIOS selv om du ikke kan bruke DNS.
SNMPv1/v2c Settings	Du kan angi om du vil aktivere SNMPv1/v2c. Dette brukes til å sette opp enheter, overvåking og så videre.
SNMPv3 Settings	Du kan angi om du vil aktivere SNMPv3. Dette brukes til å sette opp krypterte enheter, overvåking, osv.

Relatert informasjon

➡ “Kontrollprotokoller” på side 35

➡ “Innstillingselementer for protokoll” på side 37

Innstillingselementer for protokoll



Artikler	Innstillingsverdi og beskrivelse
Bonjour Settings	

Grunnleggende sikkerhetsinnstillinger

Artikler	Innstillingsverdi og beskrivelse
Use Bonjour	Marker her for å søke etter eller bruke enheter via Bonjour.
Bonjour Name	Viser Bonjour-navn.
Bonjour Service Name	Du kan vise og angi Bonjour-tjenestenavnet.
Location	Viser Bonjour-plasseringsnavn.
SLP Settings	
Enable SLP	Velg dette for å aktivere SLP-funksjonen. Den brukes for nettverksgjenkjenning i Epson Scan 2 og EpsonNet Config.
WSD Settings	
Enable WSD	Velg dette for å aktivere tillegging av enheter ved hjelp av WSD og utskrift og skanning via WSD-porten.
Scanning Timeout (sec)	Skriv inn verdi for tidsavbrudd av kommunikasjon for WSD-skanning mellom 3 og 3600 sekunder.
Device Name	Viser WSD-enhetsnavn.
Location	Viser WSD-plasseringsnavn.
LLTD Settings	
Enable LLTD	Velg dette for å aktivere LLTD. Skanneren vises på Windows-nettverkskartet.
Device Name	Viser LLTD-enhetsnavn.
LLMNR Settings	
Enable LLMNR	Velg dette for å aktivere LLMNR. Du kan bruke navneløsing uten NetBIOS selv om du ikke kan bruke DNS.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	Velg for å aktivere SNMPv1/v2c. Bare skannere som støtter SNMPv3 vises.
Access Authority	Definer tilgangsrettigheter når SNMPv1/v2c er aktivert. Velg **Read Only** eller **Read/Write**.
Community Name (Read Only)	Skriv inn 0 til 32 ASCII-tegn (0x20 til 0x7E).
Community Name (Read/Write)	Skriv inn 0 til 32 ASCII-tegn (0x20 til 0x7E).
SNMPv3 Settings	
Enable SNMPv3	SNMPv3 er aktivert når boksen er krysset av.
User Name	Skriv inn mellom 1 og 32 tegn ved hjelp av 1-biters tegn.
Authentication Settings	
Algorithm	Velg en algorytme for autentisering for SNMPv3.

Grunnleggende sikkerhetsinnstillinger

Artikler	Innstillingsverdi og beskrivelse
Password	Velg et passord for autentisering for SNMPv3. Skriv inn mellom 8 og 32 tegn i ASCII (0x20–0x7E). Hvis du ikke angir dette, lar du det stå tomt.
Confirm Password	Skriv inn passordet du konfigurerte som bekreftelse.
Encryption Settings	
Algorithm	Velg en algorytme for kryptering for SNMPv3.
Password	Velg et passord for kryptering for SNMPv3. Skriv inn mellom 8 og 32 tegn i ASCII (0x20–0x7E). Hvis du ikke angir dette, lar du det stå tomt.
Confirm Password	Skriv inn passordet du konfigurerte som bekreftelse.
Context Name	Skriv inn maksimalt 32 tegn i Unicode (UTF-8). Hvis du ikke angir dette, lar du det stå tomt. Antall tegn som kan angis varierer avhengig av språket som er brukt.

Relatert informasjon

➡ “Kontrollprotokoller” på side 35
➡ “Protokoller du kan Aktivere eller Deaktivere” på side 36

Drifts- og administrasjonsinnstillinger

Dette kapittelet forklarer aspekter relatert til daglig drift og administrasjon av enheten.

Bekreft informasjonen om en enhet

Du kan sjekke følgende informasjon om enheten fra **Status** ved å bruke Web Config.

❏ Product Status

Sjekk språk, stratus, produktnummer, MAC-adresse, osv.

❏ Network Status

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

❏ Panel Snapshot

Vis et øyeblikksbilde som vises på kontrollpanelet på enheten.

❏ Maintenance

Sjekk startdato, skanneinformasjon, osv.

❏ Hardware Status

Kontroller statusen for skanneren.

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23

Administrere enheter (Epson Device Admin)

Du kan administrere og styre mange enheter ved å bruke Epson Device Admin. Epson Device Admin lar deg administrere enheter som tilhører andre nettverk. Det følgende skisserer hovedfunksjonene for administrasjon.

For mer informasjon om funksjoner og bruk av programvaren kan du se dokumentasjonen eller hjelpedelen på Epson Device Admin.

❏ Oppdagelse av enheter

Du kan registrere enheter på nettverket og registrere dem på en liste. Hvis Epson-enheter som skrivere og skannere er koblet til samme nettverkssegment som administratorens datamaskin, kan du finne dem selv om de ikke har blitt tilordnet en IP-adresse.

Du kan også registrere enheter som er koblet til datamaskiner på nettverket med USB-kabler. Du må installere Epson Device USB Agent på datamaskinen.

❏ Innstilling av enheter

Du kan lage en mal som inneholder innstillingselementer som nettverksgrensesnitt og papirkilde, og bruke den på andre enheter som delte innstillinger. Når den er koblet til nettverket, kan du tilordne en IP-adresse til en enhet som ikke har blitt tildelt en IP-adresse før.

❏ Overvåking av enheter

Du kan regelmessig se status og detaljert informasjon for enheter på nettverket. Du kan også overvåke enheter som er koblet til datamaskiner på nettverket via USB-kabler og enheter fra andre selskaper som er registrert i enhetslisten. For å overvåke enheter som er koblet til med USB-kabler, må du installere Epson Device USB Agent.

❏ Administrere varsler

Du kan overvåke varsler for status for enheter og andre forbruksvarer. Systemet sender automatisk e-postvarsler til administratoren basert på faste forhold.

❏ Administrere rapporter

Du kan lage regelmessige rapporter fra systemet som samler data på enheten om bruk og forbruksvarer. Du kan deretter lagre disse opprettede rapportene og sende dem via e-post.

Relatert informasjon

➡ "Epson Device Admin" på side 55

Motta e-postvarslinger når det skjer hendelser

Om e-postvarsler

Du kan bruke denne funksjonen for å motta varsler på e-post når hendelser oppstår. Du kan registrere opptil 5 e-postadresser og velge hvilke hendelser du vil motta varsel for.

E-postserveren må konfigureres for å bruke denne funksjonen.

Relatert informasjon

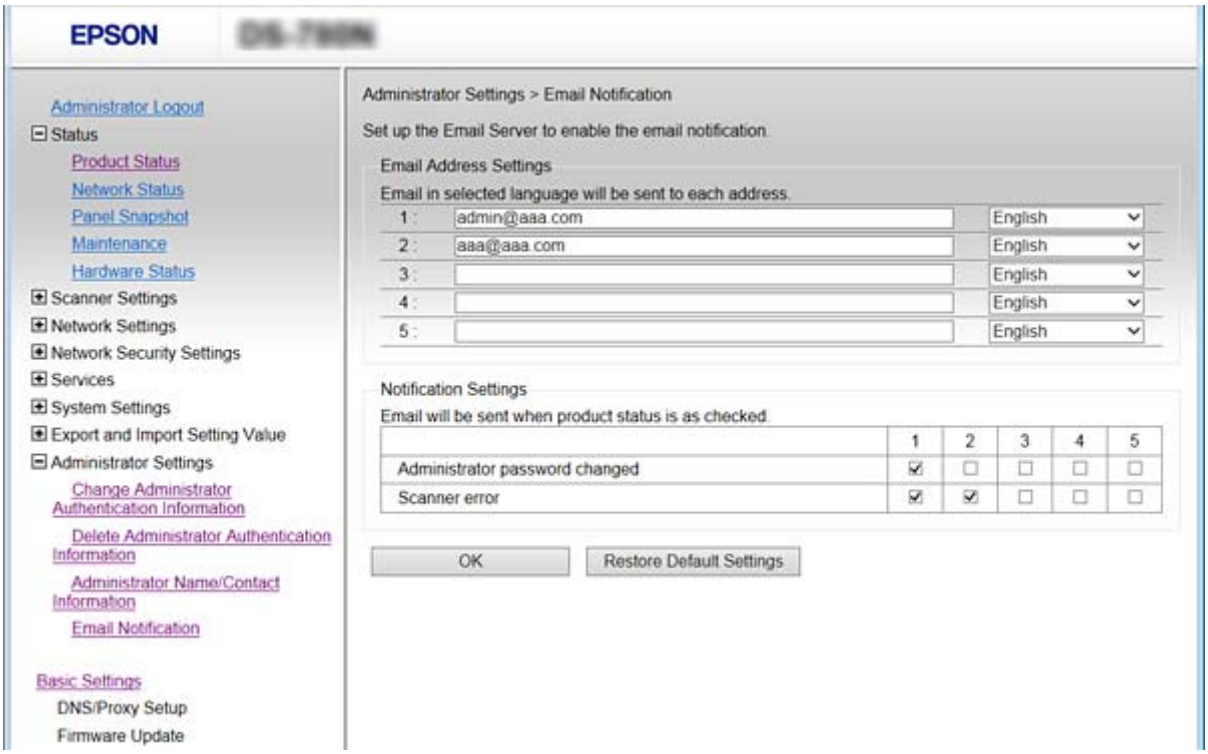
➡ "Konfigurere en e-postserver" på side 42

Konfiguere e-postvarsel

For å bruke denne funksjonen må du konfigurere en e-postserver.

1. Gå inn på Web Config og velg **Administrator Settings** > **Email Notification**.
2. Skriv inn en e-postadresse du vil skal motta e-postvarsler.
3. Velg språk for e-postvarsler.

4. Huk av boksene for varslene du ønsker å motta.



5. Klikk **OK**.

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23
➡ "Konfigurere en e-postserver" på side 42

Konfigurere en e-postserver

Sjekk følgende før du konfigurerer.

❏ Skanneren er koblet til et nettverk.

❏ Datamaskinens e-postserverinformasjon.

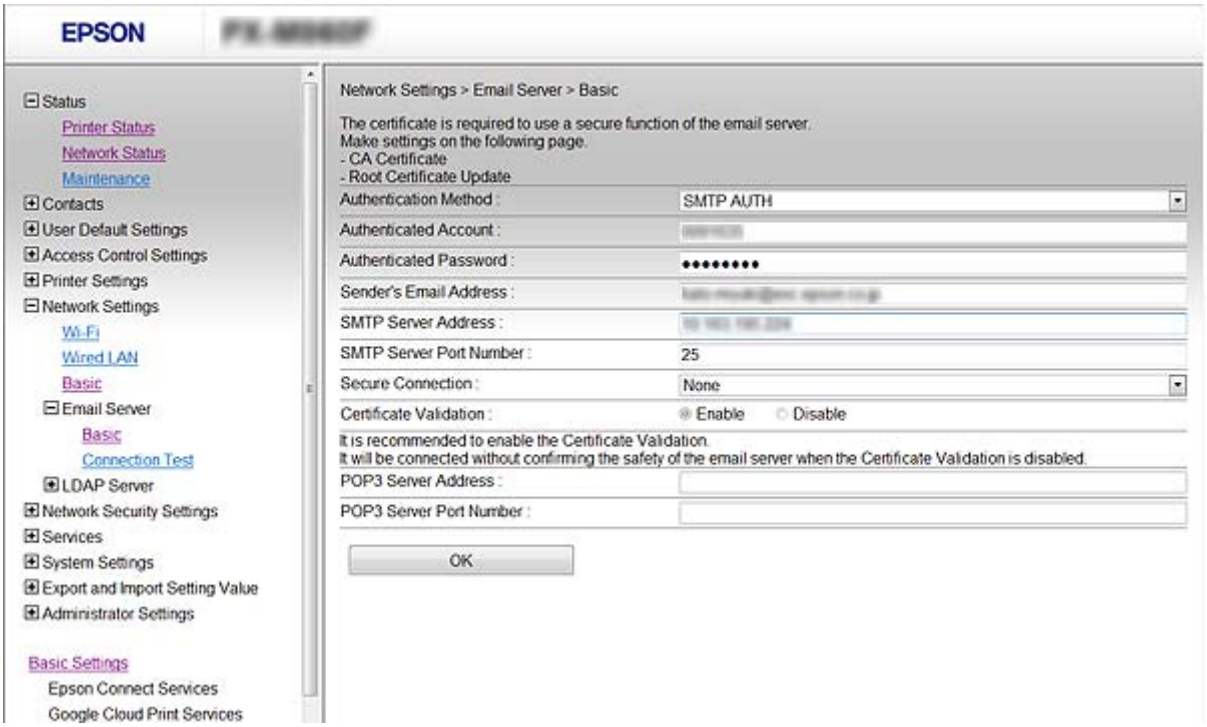
1. Gå inn på Web Config og velg **Network Settings** > **Email Server** > **Basic**.
2. Angi en verdi for hvert element.
3. Velg **OK**.

   Valgte innstillinger viser.

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23
➡ "Innstillingselementer for e-postserver" på side 43

Innstillingselementer for e-postserver



Elementer	Innstillinger og forklaring	
Authentication Method	Angi godkjenningsmetoden for skanneren som skal få tilgang til e-postserveren.	
	Off	Autentifisering er deaktivert under kommunikasjon med en e-postserver.
	SMTP AUTH	Krever at en e-postserver støtter SMTP-autentifisering.
	POP before SMTP	Konfigurer POP3-serveren når du velger denne metoden.
Authenticated Account	Hvis du velger **SMTP AUTH** eller **POP before SMTP** som **Authentication Method**, skriver du inn det autentiserte kontonavnet på mellom 0 og 255 tegn i ASCII (0x20 til 0x7E).	
Authenticated Password	Hvis du velger **SMTP AUTH** eller **POP before SMTP** som **Authentication Method**, skriver du inn det autentiserte kontonavnet på mellom 0 og 20 tegn ived å bruke A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.	
Sender's Email Address	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 ".".	
SMTP Server Address	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 Port Number	Skriv inn et tall mellom 1 og 65535.	

Elementer	Innstillinger og forklaring	
Secure Connection	Spesifiser sikker tilkobling metode for e-postserveren.	
	None	Hvis du velger **POP before SMTP** i **Authentication Method**, blir tilkoblingsmetoden satt til **None**.
	SSL/TLS	Dette er tilgjengelig når **Authentication Method** er satt til **Off** eller **SMTP AUTH**.
	STARTTLS	Dette er tilgjengelig når **Authentication Method** er satt til **Off** eller **SMTP AUTH**.
Certificate Validation	Sertifikatet er validert når dette er aktivert. Vi anbefaler at dette settes til **Enable**.	
POP3 Server Address	Hvis du velger **POP before SMTP** som **Authentication Method**, 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 Port Number	Hvis du velger **POP before SMTP** som **Authentication Method**, skriver du inn et nummer mellom 1 og 65535 tegn.	

Relatert informasjon

➡ "Konfigurere en e-postserver" på side 42

Kontrollere e-postservertilkoblingen

1. Gå inn på Web Config og velg **Network Settings** > **Email Server** > **Connection Test**.
2. Velg **Start**.

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

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23
➡ "Testreferanser for e-postservertilkobling" på side 44

Testreferanser for e-postservertilkobling

Meldinger	Forklaring
Connection test was successful.	Denne meldingen vises når tilkoblingen med serveren er vellykket.
SMTP server communication error. Check the following. - Network Settings	Denne meldingen vises når ❏ Skanneren ikke er koblet til nettverket ❏ SMTP-serveren er nede ❏ Nettverkstilkoblingen er frakoblet under kommunikasjon ❏ Ufullstendige data er mottatt

Drifts- og administrasjonsinnstillinger

Meldinger	Forklaring
POP3 server communication error. Check the following. - Network Settings	Denne meldingen vises når ❏ Skanneren ikke er koblet til nettverket ❏ POP3-serveren er nede ❏ Nettverkstilkoblingen er frakoblet under kommunikasjon ❏ Ufullstendige data er mottatt
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Denne meldingen vises når ❏ Tilkobling til en DNS-server mislyktes ❏ Navneoppslag for en SMTP-server mislyktes
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Denne meldingen vises når ❏ Tilkobling til en DNS-server mislyktes ❏ Navneoppslag for en POP3-server mislyktes
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Denne meldingen vises når SMTP-serverautentisering mislyktes.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Denne meldingen vises når POP3-serverautentisering mislyktes.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Denne meldingen vises når du prøver å kommunisere med protokoller som ikke støttes.
Connection to SMTP server failed. Change Secure Connection to None.	Denne meldingen vises når SMTP ikke samsvarer mellom en server og en klient eller når serveren ikke støtter sikker SMTP-tilkobling (SSL-tilkobling).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Denne meldingen vises når SMTP ikke samsvarer mellom en server og en klient eller når serveren ber om å bruke en SSL/TLS-tilkobling for en sikker SMTP-tilkobling.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Denne meldingen vises når SMTP ikke samsvarer mellom en server og en klient eller når serveren ber om å bruke en STARTTLS-tilkobling for en sikker SMTP-tilkobling.
The connection is untrusted. Check the following. - Date and Time	Denne meldingen vises når skannerens dato og klokkeslett er feil eller sertifikatet er utløpt.
The connection is untrusted. Check the following. - CA Certificate	Denne meldingen vises når skanneren ikke har et rotsertifikat som tilsvarer serveren eller en CA Certificate ikke har blitt importert.
The connection is not secured.	Denne meldingen vises når det sertifikat som ble hentet er skadet.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Denne meldingen vises når en autentiseringsmetode ikke samsvarer mellom en server og en klient. Serveren støtter SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Denne meldingen vises når en autentiseringsmetode ikke samsvarer mellom en server og en klient. Serveren støtter ikke SMTP AUTH.

Meldinger	Forklaring
Sender's Email Address is incorrect. Change to the email address for your email service.	Denne meldingen vises når den angitte avsenders e-postadresse er feil.
Cannot access the product until processing is complete.	Denne meldingen vises når skanneren er opptatt.

Relatert informasjon

➡ “Kontrollere e-postservertilkoblingen” på side 44

Oppdatere fastvaren

Oppdatere fastvaren ved hjelp av Web Config

Oppdaterer fastvaren ved å bruke Web Config. Denne enheten må være koblet til Internett.

1. Gå inn på Web Config og velg **Basic Settings** > **Firmware Update**.
2. Klikk på **Start**.

   Fastvarekontrollen starter, og fastvareinformasjonen vises dersom oppdatert fastvare finnes.
3. Klikk **Start** og følg instruksjonene på skjermen.

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

➡ “Få tilgang til Web Config” på side 23
➡ “Epson Device Admin” på side 55

Oppdatere fastvaren ved å bruke Epson Firmware Updater

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.

1. Gå inn på Epson-nettstedet og last ned fastvaren.
2. Koble datamaskinen som fastvaren ble lastet ned på til enheten ved å bruke en USB-kabel.
3. Dobbeltklikk på den nedlastede .exe-filen.

   Epson Firmware Updater starter.
4. Følg instruksjonene på skjermen.

Sikkerhetskopier innstillingene

Ved å eksportere innstillingselementene på Web Config, kan du kopiere elementene til andre skannere.

Eksportere innstillingene

Eksporter hver innstilling for skanneren.

1. Gå inn på Web Config, og velg deretter **Export and Import Setting Value** > **Export**.
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 filen som eksporteres.

   Du trenger da passordet for å importere filen. La dette stå tomt hvis du ikke vil kryptere filen.
4. Klikk **Export**.

> ***Forsiktighetsregel:***
>
> *Hvis du vil eksportere nettverksinnstillingene til skanneren, som skannernavnet og IP-adresse, velger du **Enable to select the individual settings of device** og velger flere elementer. Bruk bare de valgte verdiene for skanneren som utskiftes.*

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23

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. Hvis IP-adressene overlapper, vil ikke skanneren reflektere verdien.*

1. Gå inn på Web Config, og velg deretter **Export and Import Setting Value** > **Import**.
2. Velg den eksporterte filen, og angi krypteringspassordet.
3. Klikk **Next**.
4. Velg innstillingene du vil importere, og klikk deretter **Next**.
5. Klikk **OK**.

Innstillingene brukes på skanneren.

Drifts- og administrasjonsinnstillinger

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23

Problemløsing

Tips for å løse problemer

Du finner mer informasjon i følgende håndbok.

❏ Brukerhåndbok

Gir instruksjoner om bruk av skriveren, vedlikehold og problemløsing.

Sjekke loggen for server- og nettverksenhet

Ved problemer med nettverkstilkobling, kan det være mulig å finne årsaken ved å bekrefte loggen av e-postserveren, LDAP-serveren, etc., sjekke status ved hjelp av nettverksloggen av systemutstyrslogger og kommandoer, for eksempel rutere.

Åpne nettverksinnstillinger

Gjenopprette nettverksinnstillingene fra kontrollpanelet

Du kan gjenopprette alle nettverksinnstillinger til standardene.

1. Trykk **Innst.** på startsiden.
2. Trykk **Systemadministrasjon** > **Gjenopprett standardinnst.** > **Nettverksinnstillinger**.
3. Les meldingen, og trykk deretter **Ja**.
4. Trykk **Lukk** når det vises en melding om at oppsettet er fullført.

   Skjermen lukkes automatisk etter en viss tid hvis du ikke trykker **Lukk**.

Sjekke kommunikasjonen mellom enheter og datamaskiner

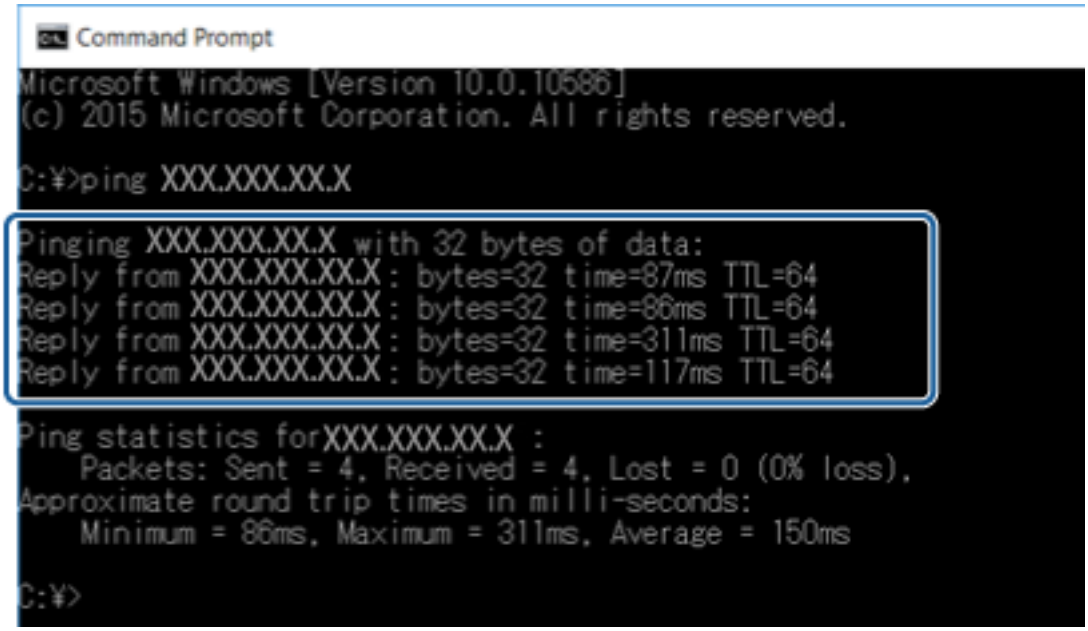
Kontrollere tilkoblingen med Ping-kommando — Windows

Du kan bruke en Ping-kommando for å kontrollere at datamaskinen er koblet til en skanner. Følg stegene under for å sjekke tilkoblingen med en Ping-kommando.

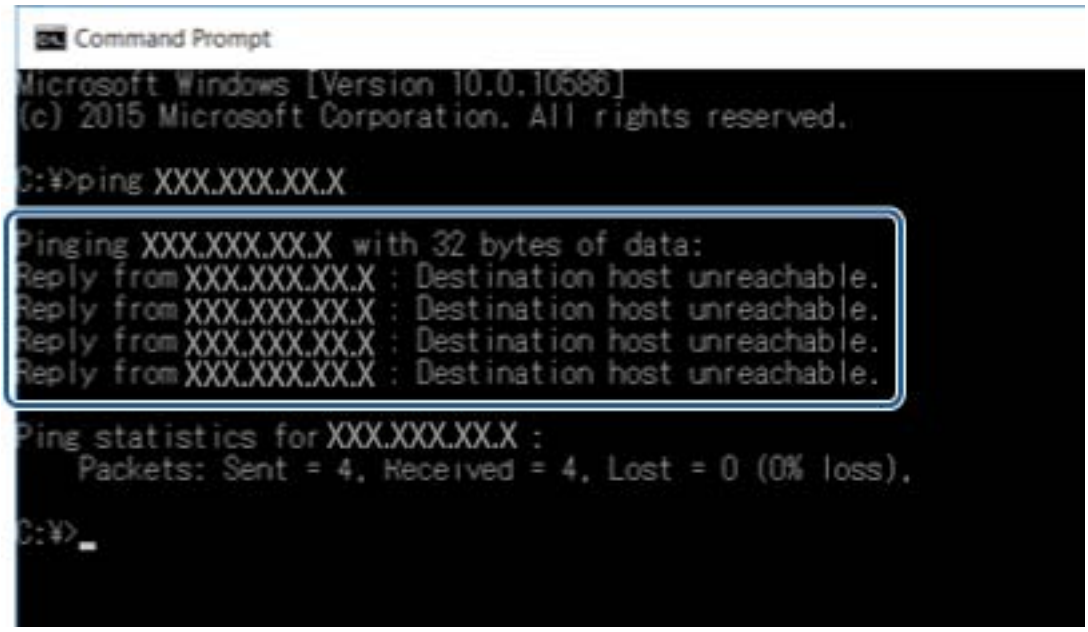
1. Kontroller skannerens IP-adresse for tilkoblingen du vil kontrollere.

   Du kan sjekke dette ved å bruke Epson Scan 2.

2. Vis datamaskinens skjermbilde for ledetekst.
   - ❏ Windows 10
     Høyreklikk på startknappen eller klikk og hold den inne, og velg deretter **Ledetekst**.
   - ❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
     Vis programskjermen, og velg deretter **Ledetekst**.
   - ❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 eller tidligere
     Klikk startknappen, velg **Alle programmer** eller **Programmer** > **Tilbehør** > **Ledetekst**.
3. Skriv inn «ping xxx.xxx.xxx.xxx», og trykk deretter Enter.
   Skriv inn skannerens IP-adresse for xxx.xxx.xxx.xxx.
4. Kontroller kommunikasjonsstatusen.
   Meldingen nedenfor vises hvis skanneren og datamaskinen kommuniserer.



Meldingen nedenfor vises hvis skanneren og datamaskinen ikke kommuniserer.



Kontrollere tilkoblingen med Ping-kommando — Mac OS

Du kan bruke en Ping-kommando for å kontrollere at datamaskinen er koblet til en skanner. Følg stegene under for å sjekke tilkoblingen med en Ping-kommando.

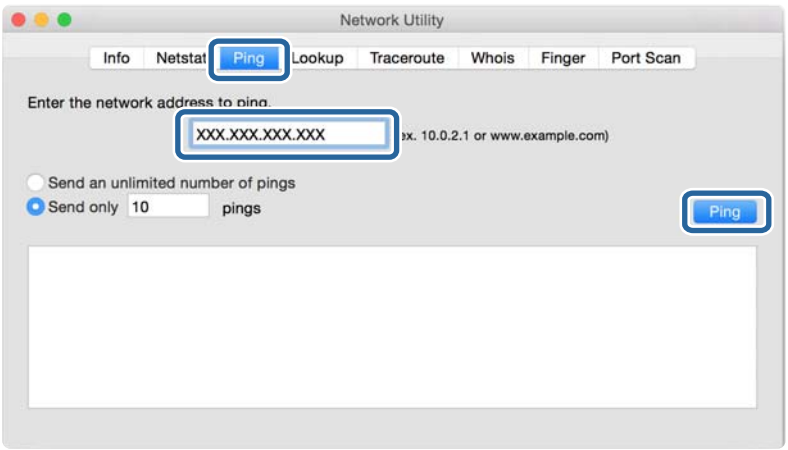
1. Kontroller skannerens IP-adresse for tilkoblingen du vil kontrollere.

   Du kan sjekke dette ved å bruke Epson Scan 2.

2. Kjør Network Utility.

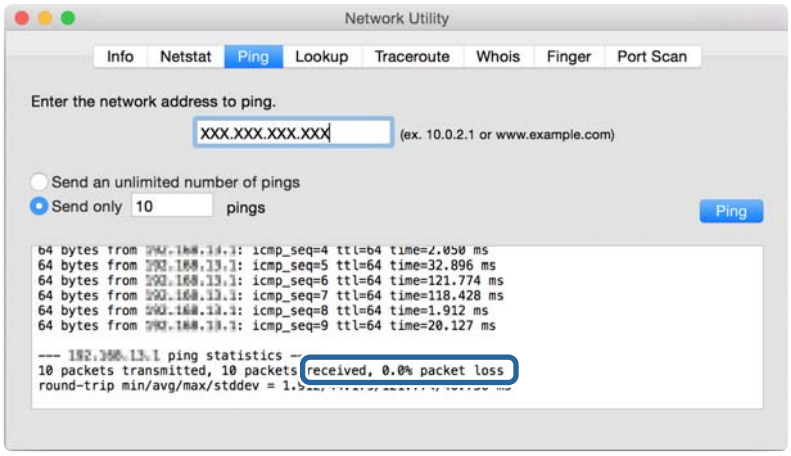
   Skriv inn "Network Utility" i **Spotlight**.

3. Klikk kategorien **Ping**, skriv inn IP-adressen du kontrollerte i trinn 1, og klikk deretter **Ping**.

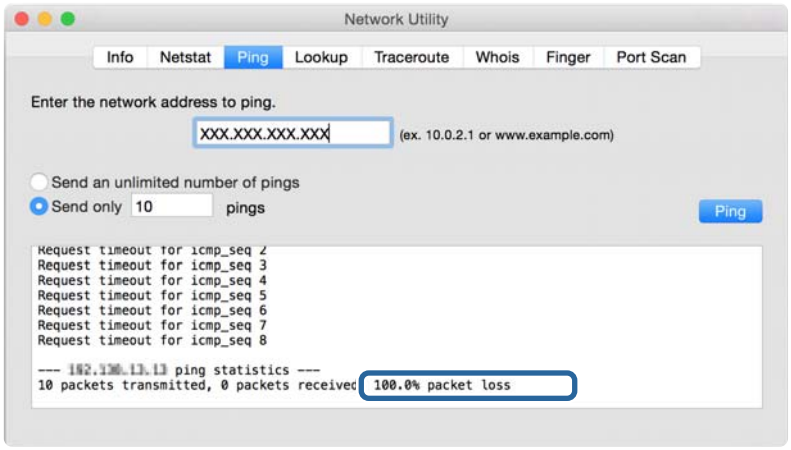


4. Kontroller kommunikasjonsstatusen.

   Meldingen nedenfor vises hvis skanneren og datamaskinen kommuniserer.



   Meldingen nedenfor vises hvis skanneren og datamaskinen ikke kommuniserer.



Problemer med bruk av nettverksprogrammer

Får ikke tilgang til Web Config

Er IP-adressen til skanneren riktig konfigurert?

Konfigurer IP-adressen ved hjelp av Epson Device Admin eller EpsonNet Config.

Støtter nettleseren din bulkkrypteringer for Encryption Strength for SSL/TLS?

Bulkkrypteringene for Encryption Strength for SSL/TLS er som følger. Du kan kun få tilgang til Web Config i en nettleser som støtter følgende bulkkrypteringer. Kontroller nettleserens krypteringsstøtte.

- ❏ 80bit: AES256/AES128/3DES
- ❏ 112bit: AES256/AES128/3DES
- ❏ 128bit: AES256/AES128

❏ 192bit: AES256

❏ 256bit: AES256

Meldingen «Foreldet» vises når du åpner Web Config ved hjelp av SSL-kommunikasjon (https).

Hvis sertifikatet er foreldet, må du hente sertifikatet på nytt. Hvis meldingen vises før utløpsdatoen, kontrollerer du at skannerens dato er riktig konfigurert.

Meldingen «Navnet på sikkerhetssertifikatet samsvarer ikke···» vises når du åpner Web Config ved hjelp av SSL-kommunikasjon (https).

Skannerens IP-adresse som er angitt for **Common Name** for å opprette et selvsignert sertifikat eller en CSR, samsvarer ikke med adressen som er skrevet inn i nettleseren. Hent og importer et sertifikat på nytt, eller endre navnet på skanneren.

Skanneren åpnes via en proxy-server.

Hvis du bruker en proxy-server sammen med skanneren, må du konfigurere nettleserens proxy-innstillinger.

❏ 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 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

Relatert informasjon

➡ “Få tilgang til Web Config” på side 23

➡ “Tilordne IP-adressen” på side 15

➡ “Tilordne IP-adresse ved å bruke EpsonNet Config” på side 56

Modellnavn og/eller IP-adresse vises ikke på EpsonNet Config

Valgte du Blokker, Avbryt eller Avslutt da det ble vist en melding fra Windows sikkerhetsskjerm eller brannmuren?

Hvis du velger **Blokker**, **Avbryt** eller **Avslutt**, vises ikke IP-adressen og modellnavnet på EpsonNet Config eller EpsonNet Setup.

Du korrigerer dette ved å registrere EpsonNet Config som unntak ved hjelp av Windows-brannmuren og vanlig sikkerhetsprogramvare. Hvis du bruker et antivirus- eller sikkerhetsprogram, må du lukke det og deretter åpne EpsonNet Config.

Er innstillingen for tidsavbrudd ved kommunikasjonsfeil for kort?

Kjør EpsonNet Config, og velg **Tools** > **Options** > **Timeout**, og deretter øker du tiden i innstillingen for **Communication Error**. Merk at dette kan føre til at EpsonNet Config vil kjøre saktere.

Relatert informasjon

➡ “Løping EpsonNet Config — Windows” på side 56

➡ “Løping EpsonNet Config — Mac OS” på side 56

Tillegg

Introduksjon til nettverksprogramvaren

Følgende beskriver programvaren som konfigurerer og styrer enheter.

Epson Device Admin

Epson Device Admin er et program som lar deg installere enheter på nettverket og så konfigurere og administrere tjenestene. Du kan hente frem detaljert informasjon om enheter, slik som status og forbruk, sending av meldinger og varsler, samt opprette rapporter for enhetsbruk. Du kan også lage en mal som inneholder innstillingselement og bruke den på andre enheter som delte innstillinger. Du kan laste ned Epson Device Admin fra nettstedet for Epson kundestøtte. Du finner mer informasjon i dokumentasjonen eller hjelpen til Epson Device Admin.

Kjører kun Epson Device Admin (Windows)

Velg **Alle Programmer** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**.

Merknad:
Hvis det vises et brannmurvarsel, skal du tillate tilgang for Epson Device Admin.

EpsonNet Config

EpsonNet Config gir administratorer tilgang til å konfigurere skannerens nettverksinnstillinger, slik som å tilordne IP-adresse og endre tilkoblingsmodus. Funksjonen for satsvis innstilling støttes på Windows. Du finner mer informasjon i dokumentasjonen eller hjelpen til EpsonNet Config.

Løping EpsonNet Config — Windows

Velg **Alle programmer** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

Merknad:
Hvis det vises et brannmurvarsel, skal du tillate tilgang for EpsonNet Config.

Løping EpsonNet Config — Mac OS

Velg **Gå** > **Programmer** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

EpsonNet SetupManager

EpsonNet SetupManager er et program for å lage en pakke til en enkel skannerinstallasjon, slik som å installere skannerdriveren og installere Document Capture Pro. Med denne programvaren kan administrator lage unike programvarepakker og distribuere dem blant grupper.

For mer informasjon gå inn på ditt lokale Epson-nettsted.

Tilordne IP-adresse ved å bruke EpsonNet Config

Du kan tilordne en IP-adresse til skanneren ved å bruke EpsonNet Config. EpsonNet Config gjør det mulig å tilordne en IP-adresse til en skanner som ikke har blitt tilordnet en adresse etter tilkobling med en Ethernet-kabel.

Tildele IP-adresse med satsvise innstillinger

Opprette en fil for satsvise innstillinger

Ved å bruke MAC-adresse og modellnavn som nøkler kan du opprette en ny SYLK-fil for å konfigurere IP-adresse.

1. Åpne et regnearksprogram (slik som Microsoft Excel) eller et tekstbehandlingsprogram.
2. Skriv inn "Info_MACAddress", "Info_ModelName", og "TCPIP_IPAddress" i den første raden når innstillingselementet skifter navn.

   Angi innstillingselementene for følgende tekststrenger. For å skille mellom store/små bokstaver og dobbelt-/enkeltbytetegn, hvis bare ett tegn er forskjellig, vil elementet ikke bli gjenkjent.

   Angi innstillingselementets navn slik det står beskrevet ovenfor. Ellers kan ikke EpsonNet Config gjenkjenne innstillingselementene.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. Skriv inn en MAC-adresse, modellnavn og IP-adresse for hvert nettverksgrensesnitt.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

0000XXXX0001	ALC-XXXXX	192.168.100.102
0000XXXX0002	ALC-XXXXX	192.168.100.103
0000XXXX0003	ALC-XXXXX	192.168.100.104

4. Skriv inn et navn og lagre som SYLK-fil (*.slk).

Foreta satsvise innstillinger ved å bruke konfigurasjonsfilen

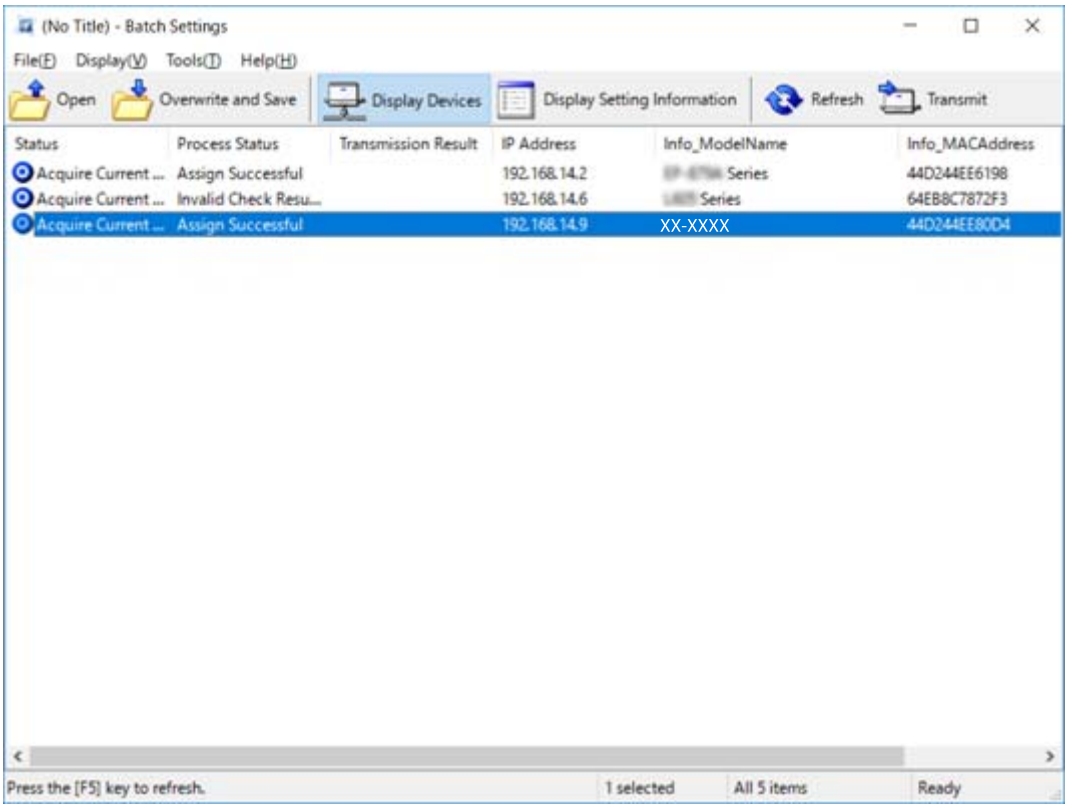
Tilordne IP-adresser i konfigurasjonsfilen (SYLK-fil) samtidig. Du må opprette konfigurasjonsfilen før tilordningen skjer.

1. Koble alle enheter til nettverket med Ethernet-kabler.
2. Slå av skanneren.
3. Start EpsonNet Config.

   En liste over skannere på nettverket vises. Det kan ta noe tid før disse vises.
4. Klikk på **Tools** > **Batch Settings**.
5. Klikk på **Open**.
6. På filvelgerskjermen velger du SYLK-filen (*.slk) som inneholder innstillingene og klikker så **Open**.

7. Velg enhetene du vil utføre satsvise innstillinger av med **Status**-kolonnen satt til **Unassigned** og **Process Status** satt til **Assign Successful**.

   Når flere valg skal gjøres, trykker du Ctrl eller Shift og klikker eller drar musen.



8. Klikk på **Transmit**.

9. Når passordvinduet vises, skriv inn passordet, og klikk deretter **OK**.

   Overfør innstillingene.

   Merknad:
   Informasjonen blir sendt til nettverksgrensesnittet inntil fremdriftsmåleren er ferdig. Ikke slå av enheten eller trådløst nettverkskort, og ikke send data til enheten.

10. På **Transmitting Settings**-skjermen klikker du **OK**.

11. Sjekk status for enheten du vil stille inn.

    For enheter som viser  eller  , sjekker du innholdet for innstillingsfilen og kontrollerer at enheten omstartet normalt.

Ikon	Status	Process Status	Forklaring
	Setup Complete	Setup Successful	Installasjonen ble fullført normalt.
	Setup Complete	Rebooting	Når informasjonen har blitt overført, trenger hver enhet å omstartes for at innstillingene skal tre i kraft. En sjekk utføres for å avgjøre hvorvidt enheten kan kobles til etter omstart.
	Setup Complete	Reboot Failed	Kan ikke bekrefte enheten etter endring av overføringsinnstillinger. Kontroller at enheten er påslått og har omstartet som normalt.
	Setup Complete	Searching	Søker etter enheten indikert i innstillingsfilen.*
	Setup Complete	Search Failed	Kan ikke sjekke enheter som allerede har blitt installert. Kontroller at enheten er påslått og har omstartet som normalt.*

    * Kun når innstillingsinformasjon vises.

Relatert informasjon

➡ "Løping EpsonNet Config — Windows" på side 56
➡ "Løping EpsonNet Config — Mac OS" på side 56

Tilordne en unik IP-adresse til hver enkelte enhet

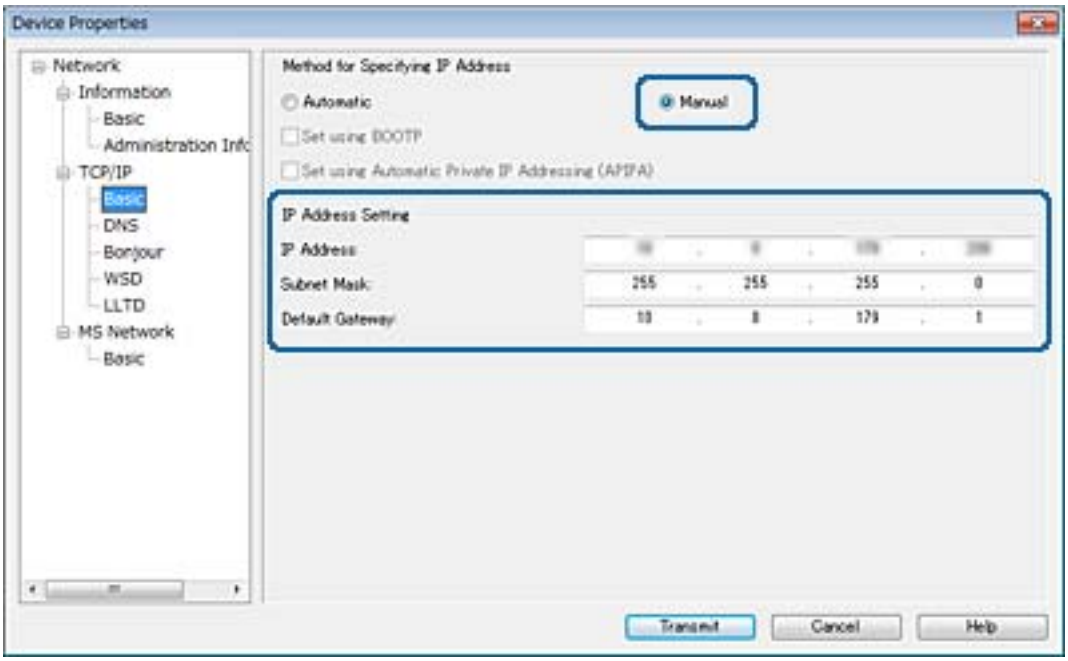
Tilordne en IP-adresse til skanneren ved å bruke EpsonNet Config.

1. Slå av skanneren.
2. Koble skanneren til et nettverk med en Ethernet-kabel.
3. Start EpsonNet Config.

   En liste over skannere på nettverket vises. Det kan ta noe tid før disse vises.
4. Dobbeltklikk skanneren du vil tilordne til.

   Merknad:
   Hvis du har koblet til flere skannere på samme modell, kan du finne skanneren ved å bruke MAC-adressen.
5. Velg **Network** > **TCP/IP** > **Basic**.

6. Skriv inn adresser for **IP Address**, **Subnet Mask**, og **Default Gateway**.



Merknad:
Angi en statisk adresse når du kobler skanneren til et sikkert nettverk.

7. Klikk på **Transmit**.

   Skjermen som bekrefter overføring av informasjon vises.

8. Klikk på **OK**.

   Overføring ferdig-skjermbildet vises.

   Merknad:
   Informasjonen sendes til enheten, og deretter vises meldingen "Konfigurasjonen er fullført" vises. Ikke slå av enheten, og ikke send data til tjenesten.

9. Klikk på **OK**.

Relatert informasjon

➡ "Løping EpsonNet Config — Windows" på side 56
➡ "Løping EpsonNet Config — Mac OS" på side 56

Bruke porten for skanneren

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

Tillegg

Avsender (klient)	Bruk	Destinasjon (server)	Protokoll	Portnummer
Skanner	E-postsending (E-postvarsling)	SMTP-server	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	POP før SMTP-tilkobling (E-postvarsling	POP-server	POP3 (TCP)	110
	Control WSD	Klientdatamaskin	WSD (TCP)	5357
	Søk på datamaskinen ved push-skanning fra Document Capture Pro	Klientdatamaskin	Registrering av nettverkspush-skann	2968
	Henter jobbinformasjon ved push-skanning fra Document Capture Pro	Klientdatamaskin	Nettverkspush-skann	2968
Klientdatamaskin	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
	Videresender skannedata fra Document Capture Pro	Skanner	Nettverksskann (TCP)	1865

Avanserte sikkerhetsinnstillinger for bedrift

I dette kapittelet beskriver vi de avanserte sikkerhetsfunksjonene.

Sikkerhetsinnstillinger og forebygging av farlige situasjoner

Når en enhet er koblet til et nettverk, kan du få tilgang til den eksternt. I tillegg kan flere personer dele enheten, 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 enheten i et miljø hvor det er tilgang til Internett er risikoen enda høyere.

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

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

Navn	Funksjonstype	Hva skal stilles inn	Hva skal forebygges
SSL/TLS-kommunikasjon	Kommunikasjonsbanen til en datamaskin og en enhet er kryptert med SSL/TLS-kommunikasjon. Innholdet i kommunikasjon fra en nettleser er beskyttet.	Angi et CA-sertifikat for serveren som er signert av en CA (Certificate Authority) til enheten.	Forhindre lekkasje av innstillingsinformasjon samt innholdet i overført data til skanneren fra datamaskinen. Tilgangen til Epson-serveren via Internett fra enheten kan også beskyttes ved hjelp av en fastvareoppdatering, el.l.
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 skanneprotokoll.	Opprett grunnleggende retningslinjer og individuelle retningslinjer for å angi hvilke klienter eller typer data som kan få tilgang til enheten.	Beskytt uautorisert tilgang og tukling og avskjæring av kommunikasjonsdata til enheten.
SNMPv3	Funksjoner er lagt til, som for eksempel overvåking av tilkoblede enheter i nettverket, integritet av SNMP-protokollens data som skal styres, kryptering, brukerautentisering, osv.	Aktiver SNMPv3, og angi deretter autentiserings- og krypteringsmetode.	Sørg for å endre innstillinger via nettverket, konfidensialitet for statlig overvåking.
IEEE802.1X	Tillater kun at en bruker som er godkjent for Ethernet kan koble til. Tillater kun at en bruker med godkjenning bruker enheten.	Godkjenningsinnstilling av RADIUS-serveren (godkjenningsserver).	Beskytt mot uautorisert tilgang og bruk av enheten.

Navn	Funksjonstype	Hva skal stilles inn	Hva skal forebygges
Les ID-kort	Du kan bruke enheten ved å holde et ID-kort over en godkjent tilkoblet enhet. Du kan begrense tilgangen til logger for hver bruker og enhet, og begrense bruken av enheter og de tilgjengelige funksjonene til hver bruker og gruppe.	Koble en godkjenningsenhet til enheten og angi deretter informasjon om en bruker i godkjenningssystemet.	Forhindre uautorisert bruk og forfalskning av enheten.

Relatert informasjon

➡ "SSL/TLS-kommunikasjon med skanneren" på side 63
➡ "Kryptert kommunikasjon ved bruk av IPsec/IP-filtrering" på side 71
➡ "Bruke SNMPv3-protokollen" på side 82
➡ "Koble skanneren til et IEEE802.1X-nettverk" på side 84

Innstilling av sikkerhetsfunksjoner

Ved innstilling av IPsec/IP-filtrering eller IEEE802.1X, anbefales det at du går inn på Web Config ved å bruke SSL/TLS for å kommunisere innstillingsinformasjon, for å redusere faren for sikkerhetsbrudd slik som manipulering eller avskjæring.

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.

Om digital sertifisering

❏ Sertifikat signert av en CA

Et sertifikat som er signert av en CA (sertifiseringsinstans) må hentes fra en sertifiseringsinstans. Du kan sørge for sikker kommunikasjon ved å bruke et CA-signert sertifikat. Du kan bruke et CA-signert sertifikat for hver enkelt sikkerhetsfunksjon.

❏ CA-sertifikat

Et CA-sertifikat angir at en tredjepart har bekreftet identiteten til en server. Dette er en viktig del innen klarert nettsikkerhet. Du må hente et CA-sertifikat for servergodkjenning fra en CA som utsteder slike.

❏ Selvsignert sertifikat

Selvsignert sertifikat er et sertifikat som skanneren utsteder og signerer selv. Dette sertifikatet er upålitelig og kan ikke forhindre forfalskning. Hvis du bruker dette sertifikatet som SSL/TLS-sertifikat, kan det vises en sikkerhetsadvarsel i nettleseren. Du kan bare bruke dette sertifikatet for SSL/TLS-kommunikasjon.

Relatert informasjon

➡ "Hente og importere et CA-signert sertifikat" på side 64

➡ "Slette et CA-signert sertifikat" på side 67
➡ "Oppdatere et selvsignert sertifikat" på side 68

Hente og importere 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 **Network Security Settings**. Deretter velger du **SSL/TLS** > **Certificate** eller **IPsec/IP Filtering** > **Client Certificate** eller **IEEE802.1X** > **Client Certificate**.

2. Klikk **Generate** 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 **OK**.

   Det vises en fullføringsmelding.

5. Velg **Network Security Settings**. Deretter velger du **SSL/TLS** > **Certificate**, eller **IPsec/IP Filtering** > **Client Certificate** eller **IEEE802.1X** > **Client Certificate**.

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-signed Certificate.*

7. Send CSR-en til en sertifiseringsinstans, og hent et CA-signed Certificate.

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

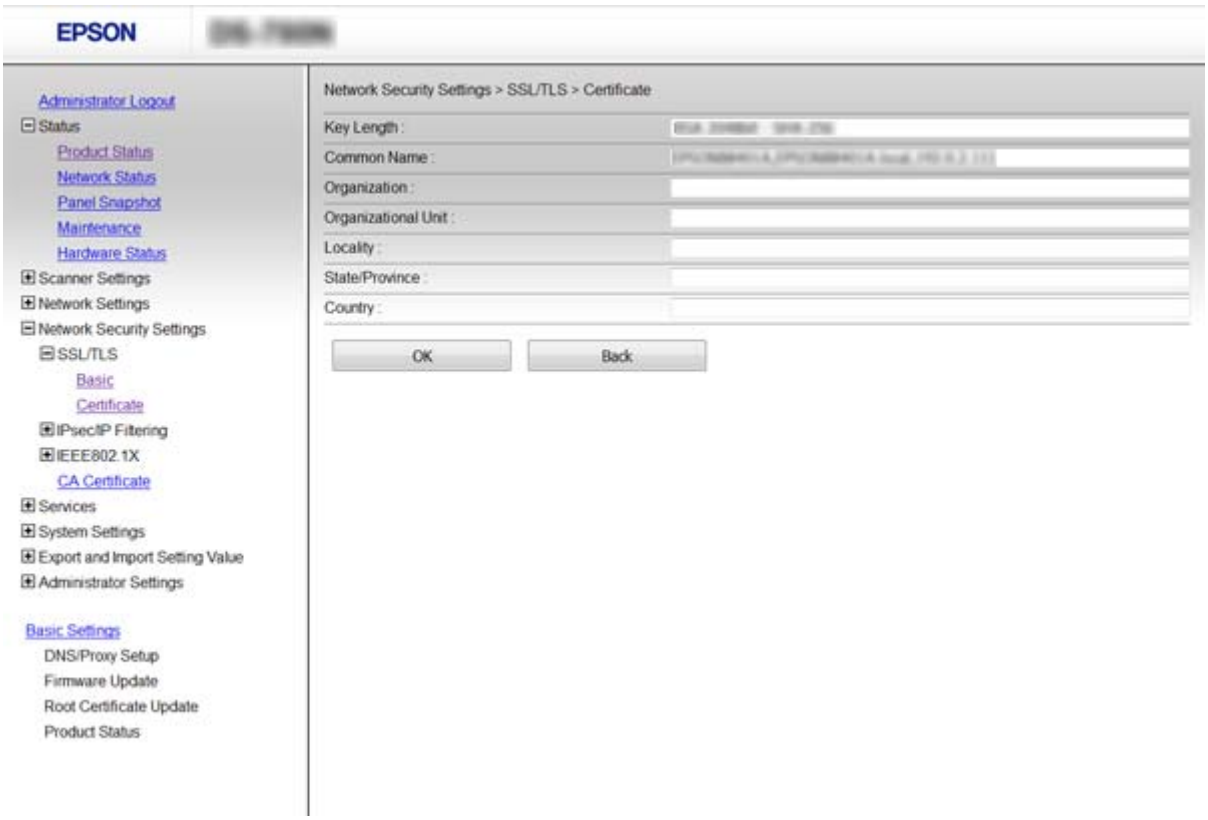
8. Lagre utstedt CA-signed Certificate på en datamaskin som er koblet til skanneren.

   Hentingen av et CA-signed Certificate er fullført når du lagrer sertifikatet et sted.

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23
➡ "Innstillingselementer for CSR" på side 65
➡ "Importere et CA-signert sertifikat" på side 65

Innstillingselementer for CSR



Artikler	Innstillinger og forklaring
Key Length	Velg en nøkkellengde for en CSR.
Common Name	Du kan skrive inn mellom 1 og 128 tegn. Hvis dette er en IP-adresse, bør det være en statisk IP-adresse. Eksempel: URL for å få tilgang til Web Config: https://10.152.12.225 Fellesnavn: 10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	Du kan skrive inn mellom 0 og 64 tegn i ASCII (0x20–0x7E). Du kan skille forskjellige navn med komma.
Country	Skriv inn en tosifret landskode angitt av ISO-3166.

Relatert informasjon

➡ “Hente et CA-signert sertifikat” på side 64

Importere et CA-signert sertifikat

Forsiktighetsregel:

❏ *Kontroller at skannerens dato og klokkeslett er riktig innstilt.*

❏ *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 **Network Security Settings**. Deretter velger du **SSL/TLS** > **Certificate**, eller **IPsec/IP Filtering** > **Client Certificate** eller **IEEE802.1X** > **Client Certificate**.

2. Klikk **Import**.

   Det åpnes en side for import av sertifikatet.

3. Angi en verdi for hvert element.

   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
     - ❏ **Private Key**: Må ikke konfigureres fordi skanneren inneholder en privattast.
     - ❏ **Password**: Skal ikke konfigureres.
     - ❏ **CA Certificate 1/CA Certificate 2**: Valgfritt
   - ❏ Et sertifikat med PEM/DER-format som er hentet fra datamaskinen
     - ❏ **Private Key**: Må angis.
     - ❏ **Password**: Skal ikke konfigureres.
     - ❏ **CA Certificate 1/CA Certificate 2**: Valgfritt
   - ❏ Et sertifikat med PKCS#12-format som er hentet fra datamaskinen
     - ❏ **Private Key**: Skal ikke konfigureres.
     - ❏ **Password**: Valgfritt
     - ❏ **CA Certificate 1/CA Certificate 2**: Skal ikke konfigureres.

4. Klikk **OK**.

   Det vises en fullføringsmelding.

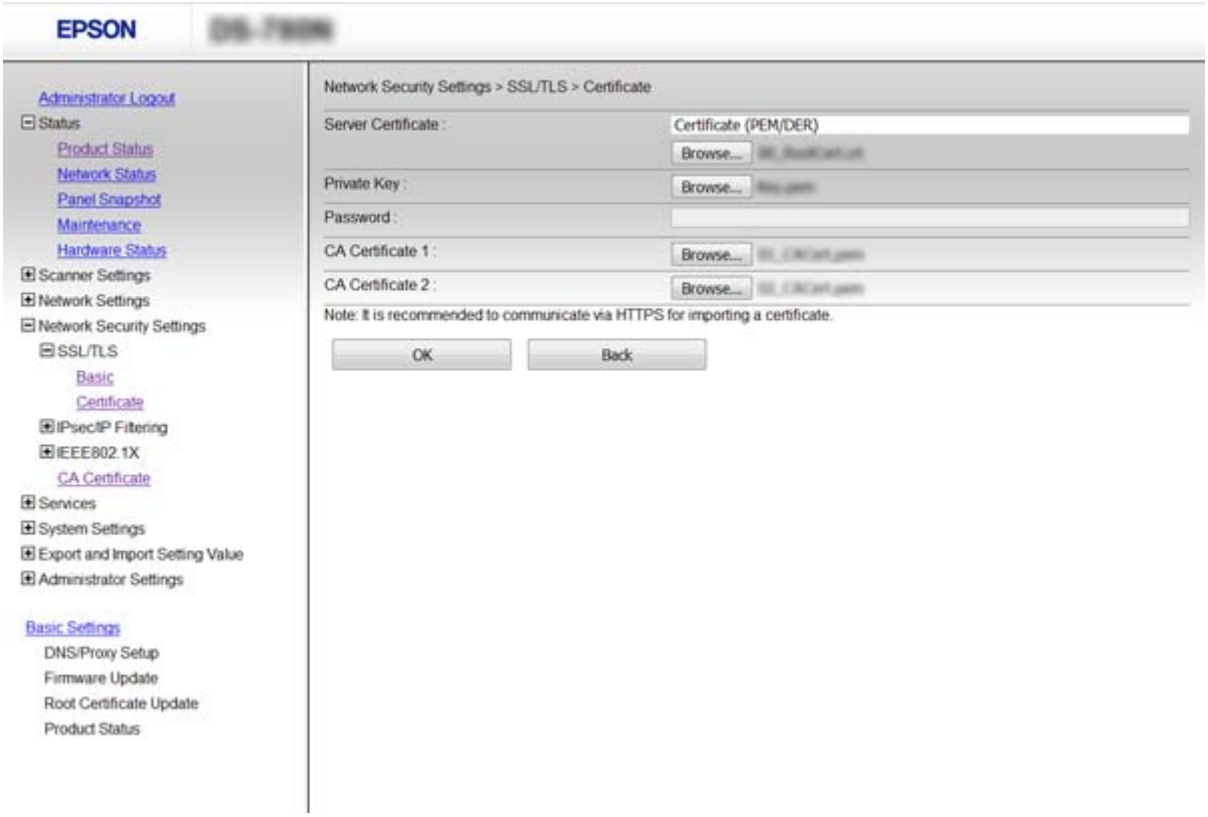
Merknad:
*Klikk **Confirm** for å bekrefte sertifikatinformasjonen.*

Relatert informasjon

➡ “Få tilgang til Web Config” på side 23

➡ “Innstillingselementer for import av CA-signert sertifikat” på side 67

Innstillingselementer for import av CA-signert sertifikat



Elementer	Innstillinger og forklaring
Server Certificate eller Client Certificate	Velg format for sertifikatet.
Private Key	Hvis du henter et sertifikat med PEM/DER-format ved hjelp av en CSR som er opprettet fra en datamaskin, angir du filen for privatnøkkelen som samsvarer med sertifikatet.
Password	Skriv inn et passord for å kryptere en privatnøkkel.
CA Certificate 1	Hvis sertifikatets format er **Certificate (PEM/DER)**, importerer du et sertifikat fra en sertifiseringsinstans som utsteder serversertifikater. Angi en fil om nødvendig.
CA Certificate 2	Hvis sertifikatets format er **Certificate (PEM/DER)**, importerer du et sertifikat fra en sertifiseringsinstans som utsteder **CA Certificate 1**. Angi en fil om nødvendig.

Relatert informasjon

➡ “Importere et CA-signert sertifikat” på side 65

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 **Network Security Settings**. Deretter velger du **SSL/TLS** > **Certificate**, eller **IPsec/IP Filtering** > **Client Certificate** eller **IEEE802.1X** > **Client Certificate**.
2. Klikk på **Delete**.
3. Bekreft at du vil slette sertifikatet i meldingen som vises.

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23

Oppdatere et selvsignert sertifikat

Hvis skanneren støtter HTTPS-serverfunksjonen, kan du oppdatere et selvsignert sertifikat. Det vises en advarsel når du åpner Web Config med et selvsignert sertifikat.

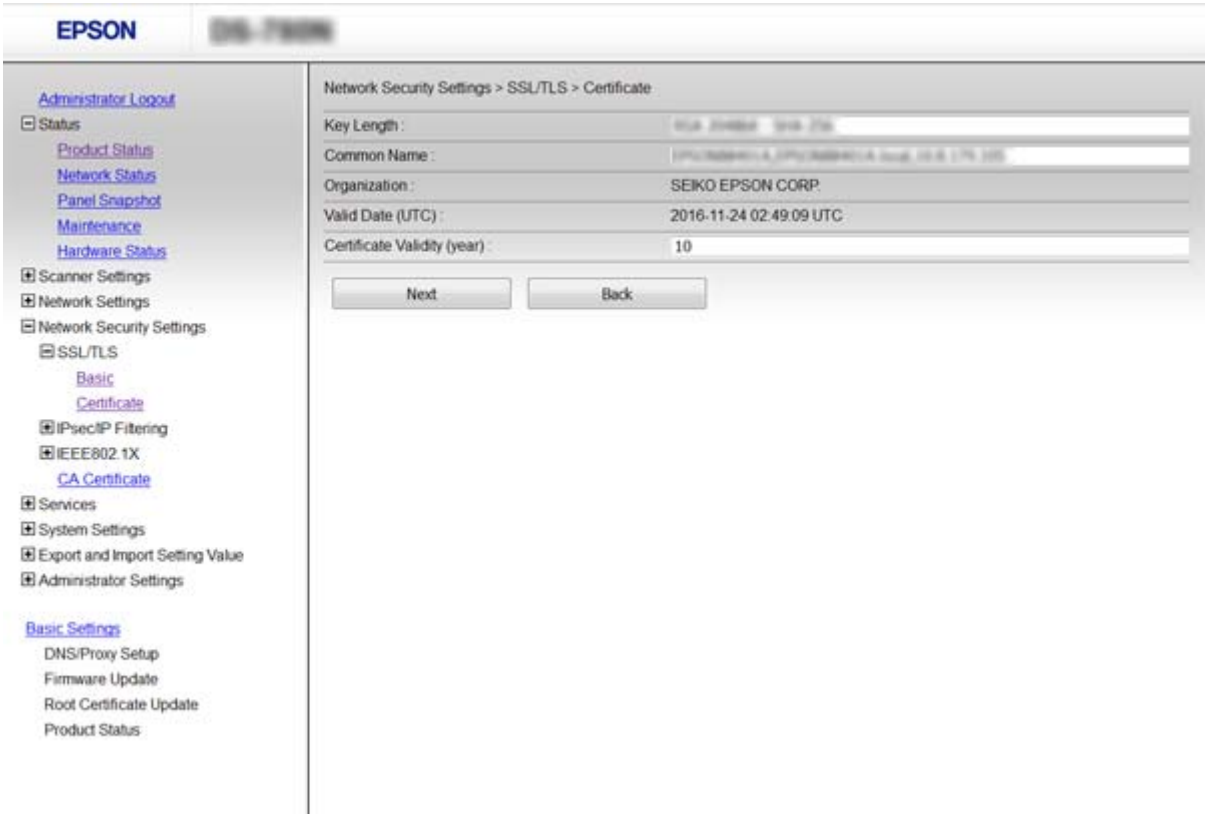
Bruk et selvsignert sertifikat midlertidig til du har hentet og importert et CA-signert sertifikat.

1. Gå inn på Web Config og velg **Network Security Settings** > **SSL/TLS** > **Certificate**.
2. Klikk på **Update**.
3. Skriv inn **Common Name**.

   Skriv inn en IP-adresse, eller en identifikator, slik som et FQDN-navn for skanneren. Du kan skrive inn mellom 1 og 128 tegn.

   Merknad:
   Du kan skille forskjellige navn (CN) med komma.

4. Angi en gyldighetsperiode for sertifikatet.



5. Klikk på **Next**.

   Det vises en bekreftelsesmelding.

6. Klikk på **OK**.

   Skanneren er oppdatert.

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

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23

Konfigurere CA Certificate

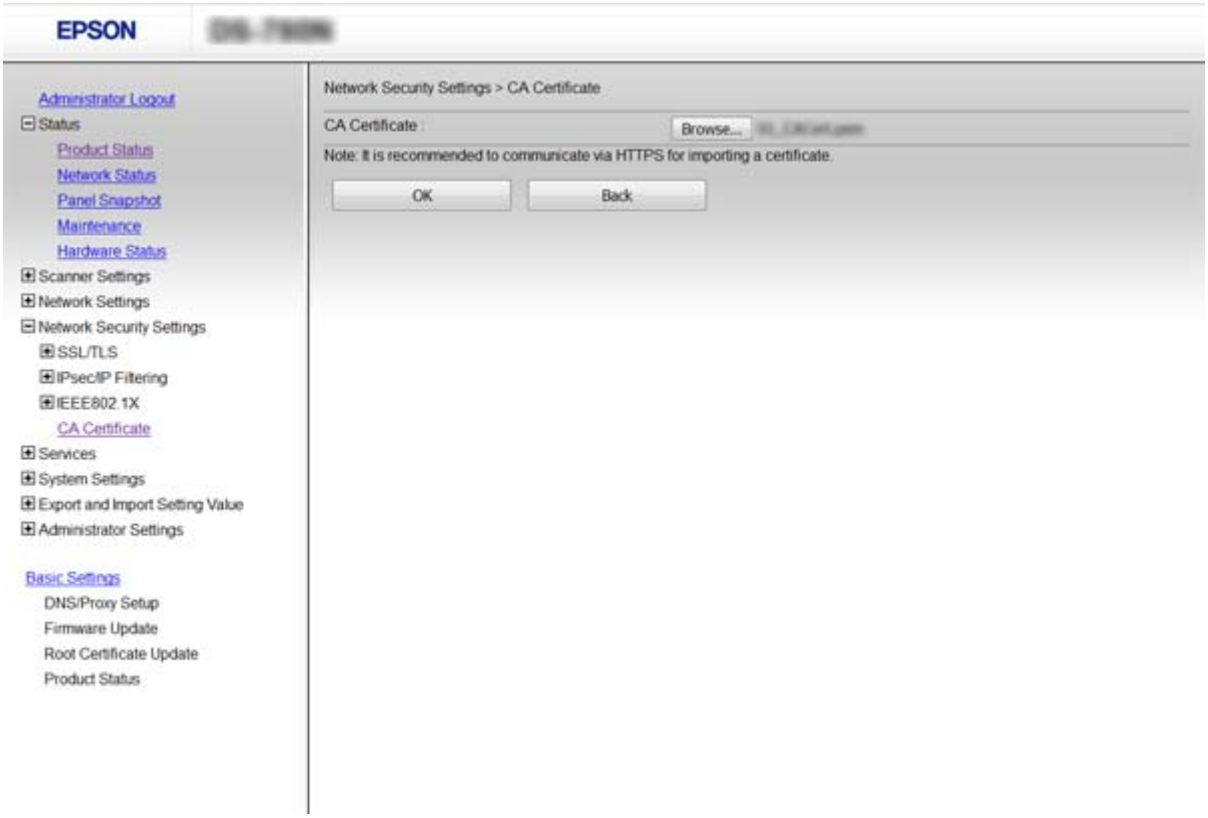
Du kan importere, vise eller slette et CA Certificate.

Importere et CA Certificate

1. Gå inn på Web Config og velg deretter**Network Security Settings** > **CA Certificate**.

2. Klikk **Import**.

3. Velg CA Certificate du vil importere.



4. Klikk **OK**.

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

Relatert informasjon

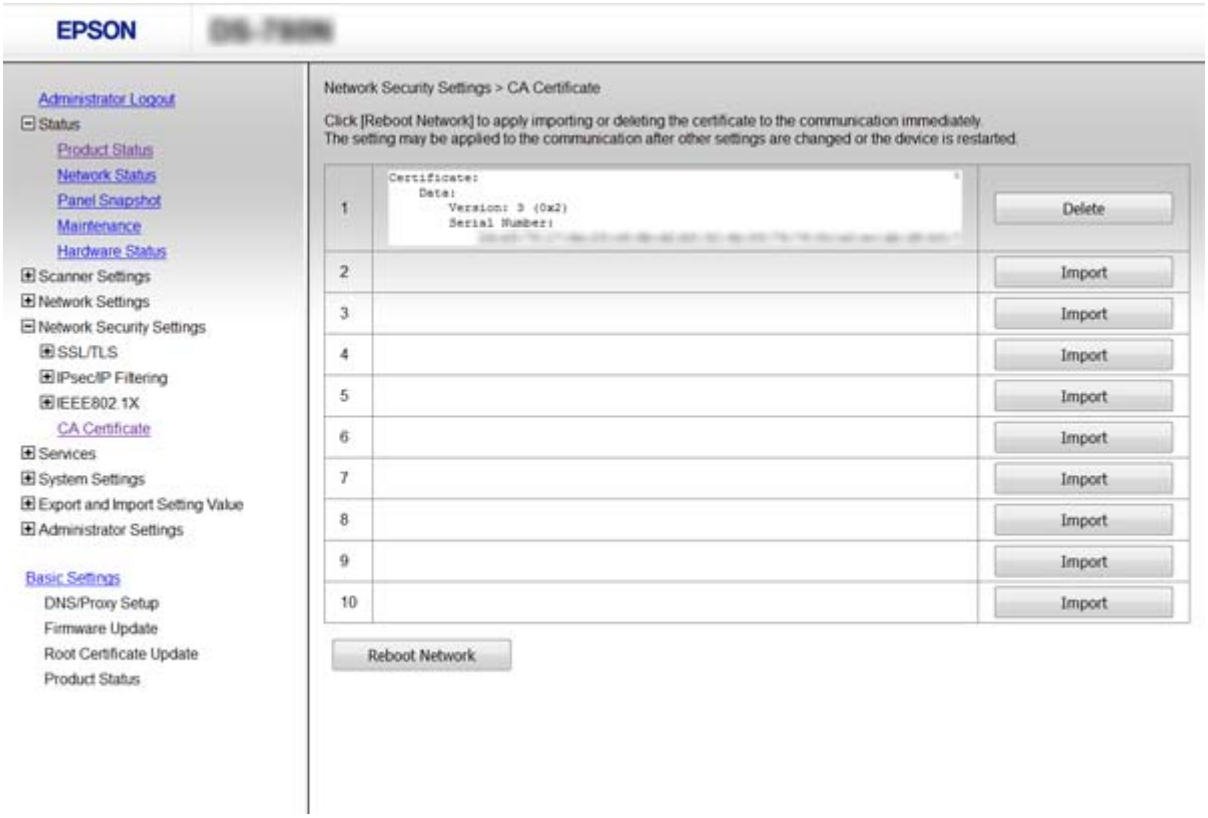
➡ "Få tilgang til Web Config" på side 23

Slette et CA Certificate

Du kan slette et importert CA Certificate.

1. Gå inn på Web Config og velg deretter**Network Security Settings** > **CA Certificate**.

2. Klikk **Delete** ved siden av CA Certificate du vil slette.



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

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23

Kryptert kommunikasjon ved bruk av IPsec/IP-filtrering

Om IPsec/IP Filtering

Hvis skanneren støtter IPsec/IP-filtrering, kan du filtrere trafikk basert på IP-adresser, tjenester og port. 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.

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. 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.

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

Konfigurere Default Policy

1. Gå inn på Web Config og velg **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Angi en verdi for hvert element.
3. Klikk **Next**.

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

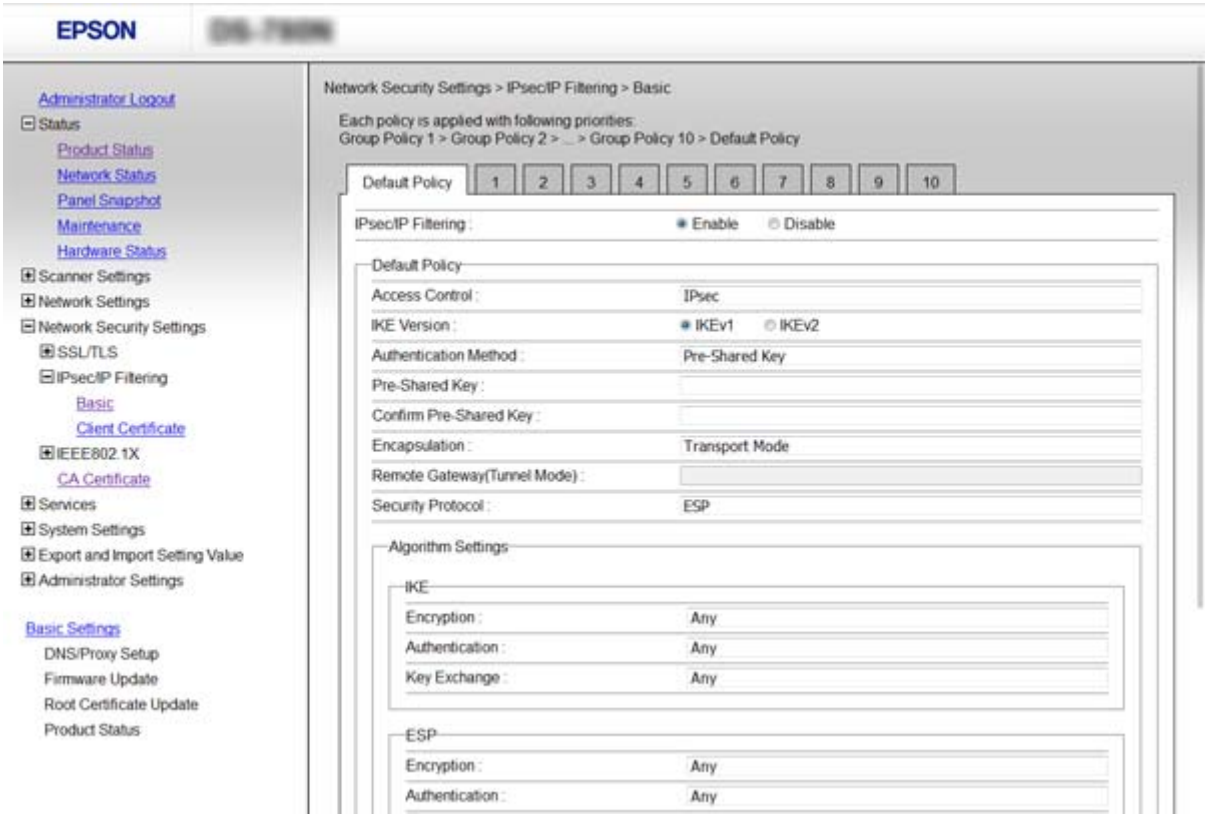
   Skanneren er oppdatert.

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23

➡ "Innstillingselementer for Default Policy" på side 72

Innstillingselementer for Default Policy



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

Avanserte sikkerhetsinnstillinger for bedrift

Artikler	Innstillinger og forklaring	
Access Control	Konfigurer en kontrollmetode for trafikk av IP-pakker.	
	Permit Access	Velg dette for å tillate at konfigurerte IP-pakker passerer.
	Refuse Access	Velg dette for å hindre at konfigurerte IP-pakker passerer.
	IPsec	Velg dette for å tillate at konfigurerte IPsec-pakker passerer.
IKE Version	Velg IKEv1 eller IKEv2 som IKE-versjon. Velg en av dem avhengig av hvilken enhet skanneren er koblet til.	
IKEv1	Følgende elementer vises når du velger **IKEv1** for **IKE Version**.	
	Authentication Method	Vil du velge **Certificate**, må du på forhånd hente og importere et CA-signert sertifikat.
	Pre-Shared Key	Hvis du velger **Pre-Shared Key** for **Authentication Method**, skriver du inn en forhåndsdelt tast på opptil 127 tegn.
	Confirm Pre-Shared Key	Skriv inn tasten du konfigurerte for bekreftelse.
IKEv2	Følgende elementer vises når du velger **IKEv2** for **IKE Version**.	
Local	Authentication Method	Vil du velge **Certificate**, må du på forhånd hente og importere et CA-signert sertifikat.
	ID Type	Velg type ID for skanneren.
	ID	Angi skannerens ID, som samsvarer med ID-typen. Du kan ikke bruke "@", "#" eller "=" som første tegn. **Distinguished Name**: Skriv inn 1 til 128 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde "=". **IP Address**: 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 (.). **Email Address**: Skriv inn 1 til 128 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde "@". **Key ID**: Skriv inn 1 til 128 enkeltbyte ASCII-tegn (0x20 til 0x7E).
	Pre-Shared Key	Hvis du velger **Pre-Shared Key** for **Authentication Method**, skriver du inn en forhåndsdelt tast på opptil 127 tegn.
	Confirm Pre-Shared Key	Skriv inn tasten du konfigurerte for bekreftelse.

Avanserte sikkerhetsinnstillinger for bedrift

Artikler	Innstillinger og forklaring	
Remote	Authentication Method	Vil du velge **Certificate**, må du på forhånd hente og importere et CA-signert sertifikat.
	ID Type	Velg ID-type for enheten du vil godkjenne.
	ID	Angi skannerens ID, som samsvarer med ID-type. Du kan ikke bruke "@", "#" eller "=" som første tegn. **Distinguished Name**: Skriv inn 1 til 128 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde "=". **IP Address**: 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 (.). **Email Address**: Skriv inn 1 til 128 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde "@". **Key ID**: Skriv inn 1 til 128 enkeltbyte ASCII-tegn (0x20 til 0x7E).
	Pre-Shared Key	Hvis du velger **Pre-Shared Key** for **Authentication Method**, skriver du inn en forhåndsdelt tast på opptil 127 tegn.
	Confirm Pre-Shared Key	Skriv inn tasten du konfigurerte for bekreftelse.
Encapsulation	Velger du **IPsec** for **Access Control**, må du konfigurere en innkapslingsmodus.	
	Transport Mode	Velg dette hvis du bare bruker skanneren på samme LAN. IP-pakker med lag 4 eller nyere blir kryptert.
	Tunnel Mode	Hvis du bruker skanneren på et nettverk som kan kobles til Internett, slik som IP-sec-VPN, velg dette alternativet. Toppteksten og dataene i IP-pakkene blir kryptert.
Remote Gateway(Tunnel Mode)	Hvis du velger **Tunnel Mode** for **Encapsulation**, skriver du inn en gateway-adresse på mellom 1 og 39 tegn.	
Security Protocol	**IPsec** for **Access Control**, velg et alternativ.	
	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.
Algorithm Settings		
IKE	Encryption	Velg krypteringsalgoritme for IKE. Elementene vil variere avhengig av IKE-versjon.
	Authentication	Velg godkjenningsalgoritme for IKE.
	Key Exchange	Velg nøkkelendringsalgoritme for IKE. Elementene vil variere avhengig av IKE-versjon.

Artikler	Innstillinger og forklaring	
ESP	Encryption	Velg krypteringsalgoritme for ESP. Dette er tilgjengelig når **ESP** er valgt for **Security Protocol**.
	Authentication	Velg autorisasjonsalgoritme for ESP. Dette er tilgjengelig når **ESP** er valgt for **Security Protocol**.
AH	Authentication	Velg krypteringsalgoritme for AH. Dette er tilgjengelig når **AH** er valgt for **Security Protocol**.

Relatert informasjon

➡ “Konfigurere Default Policy” på side 72

Konfigurere Group Policy

1. Gå inn på Web Config og velg **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Klikk på en numerert tast du vil konfigurere.
3. Angi en verdi for hvert element.
4. Klikk **Next**.

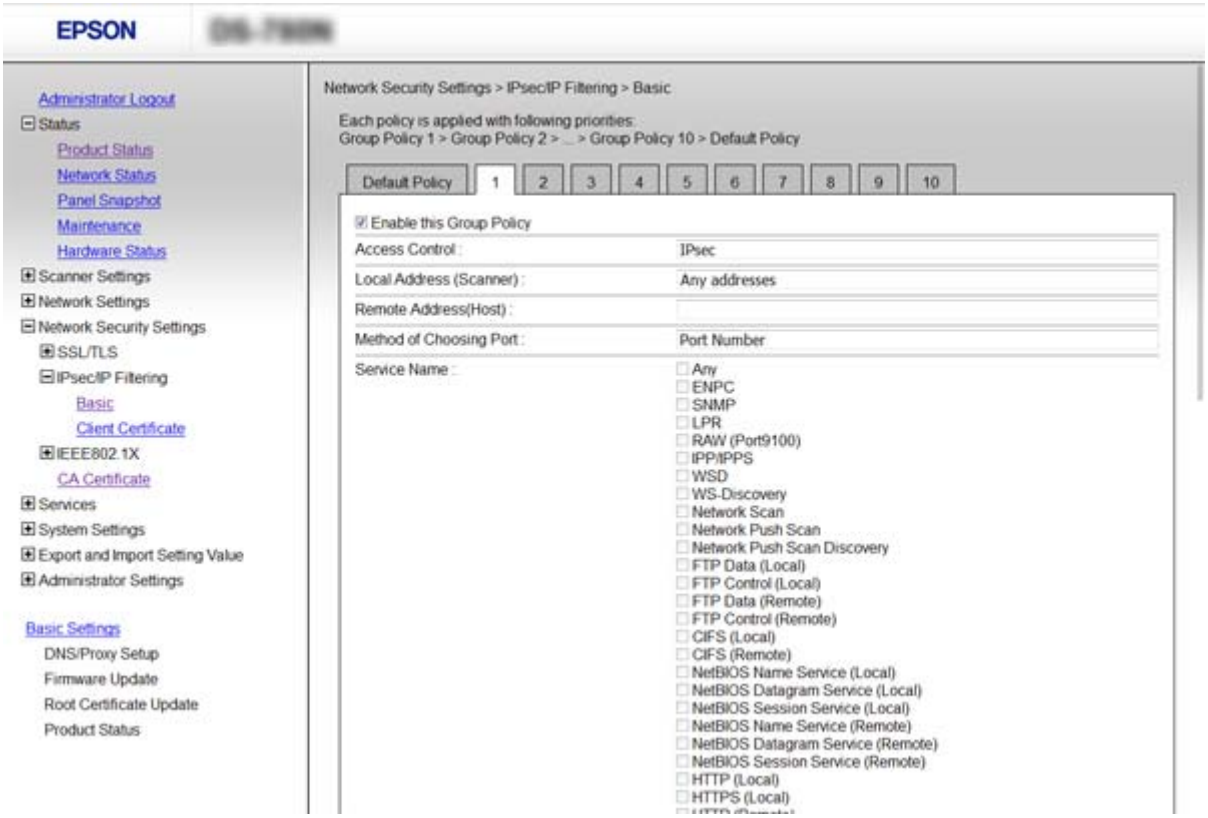
   Det vises en bekreftelsesmelding.
5. Klikk **OK**.

   Skanneren er oppdatert.

Relatert informasjon

➡ “Få tilgang til Web Config” på side 23
➡ “Innstillingselementer for Group Policy” på side 76

Innstillingselementer for Group Policy



Artikler	Innstillinger og forklaring	
Enable this Group Policy	Du kan aktivere eller deaktivere en gruppepolicy.	
Access Control	Konfigurer en kontrollmetode for trafikk av IP-pakker.	
	Permit Access	Velg dette for å tillate at konfigurerte IP-pakker passerer.
	Refuse Access	Velg dette for å hindre at konfigurerte IP-pakker passerer.
	IPsec	Velg dette for å tillate at konfigurerte IPsec-pakker passerer.
Local Address (Scanner)	Velg en IPv4-adresse eller IPv6-adresse som matcher ditt nettverksmiljø. Hvis en IP-adresse er gitt automatisk, kan du velge **Use auto-obtained IPv4 address**.	
Remote Address(Host)	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.*	
Method of Choosing Port	Velg en metode for å spesifisere porter.	
Service Name	Velg et alternativ hvis du velger **Service Name** for **Method of Choosing Port**.	

Avanserte sikkerhetsinnstillinger for bedrift

Artikler	Innstillinger og forklaring	
Transport Protocol	Velger du **Port Number** for **Method of Choosing Port**, må du konfigurere en innkapslingsmodus.	
	Any Protocol	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.
Local Port	Hvis du velger **Port Number** for **Method of Choosing Port** og hvis du velger **TCP** eller **UDP** for **Transport Protocol**, 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.	
Remote Port	Hvis du velger **Port Number** for **Method of Choosing Port** og hvis du velger **TCP** eller **UDP** for **Transport Protocol**, 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 Version	Velg IKEv1 eller IKEv2 som IKE-versjon. Velg en av dem avhengig av hvilken enhet skanneren er koblet til.	
IKEv1	Følgende elementer vises når du velger **IKEv1** for **IKE Version**.	
	Authentication Method	Velg et alternativ hvis du velger **IPsec** for **Access Control**. Brukt sertifikat er det samme som standardpolicyen.
	Pre-Shared Key	Hvis du velger **Pre-Shared Key** for **Authentication Method**, skriver du inn en forhåndsdelt tast på opptil 127 tegn.
	Confirm Pre-Shared Key	Skriv inn tasten du konfigurerte for bekreftelse.
IKEv2	Følgende elementer vises når du velger **IKEv2** for **IKE Version**.	

Avanserte sikkerhetsinnstillinger for bedrift

Artikler	Innstillinger og forklaring	
Local	Authentication Method	Velg et alternativ hvis du velger **IPsec** for **Access Control**. Brukt sertifikat er det samme som standardpolicyen.
	ID Type	Velg type ID for skanneren.
	ID	Angi skannerens ID, som samsvarer med ID-type. Du kan ikke bruke "@", "#" eller "=" som første tegn. **Distinguished Name**: Skriv inn 1 til 128 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde "=". **IP Address**: 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 (.). **Email Address**: Skriv inn 1 til 128 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde "@". **Key ID**: Skriv inn 1 til 128 enkeltbyte ASCII-tegn (0x20 til 0x7E).
	Pre-Shared Key	Hvis du velger **Pre-Shared Key** for **Authentication Method**, skriver du inn en forhåndsdelt tast på opptil 127 tegn.
	Confirm Pre-Shared Key	Skriv inn tasten du konfigurerte for bekreftelse.
Remote	Authentication Method	Velg et alternativ hvis du velger **IPsec** for **Access Control**. Brukt sertifikat er det samme som standardpolicyen.
	ID Type	Velg ID-type for enheten du vil godkjenne.
	ID	Angi skannerens ID, som samsvarer med ID-type. Du kan ikke bruke "@", "#" eller "=" som første tegn. **Distinguished Name**: Skriv inn 1 til 128 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde "=". **IP Address**: 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 (.). **Email Address**: Skriv inn 1 til 128 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde "@". **Key ID**: Skriv inn 1 til 128 enkeltbyte ASCII-tegn (0x20 til 0x7E).
	Pre-Shared Key	Hvis du velger **Pre-Shared Key** for **Authentication Method**, skriver du inn en forhåndsdelt tast på opptil 127 tegn.
	Confirm Pre-Shared Key	Skriv inn tasten du konfigurerte for bekreftelse.
Encapsulation	Velger du **IPsec** for **Access Control**, må du konfigurere en innkapslingsmodus.	
	Transport Mode	Velg dette hvis du bare bruker skanneren på samme LAN. IP-pakker med lag 4 eller nyere blir kryptert.
	Tunnel Mode	Hvis du bruker skanneren på et nettverk som kan kobles til Internett, slik som IP-sec-VPN, velg dette alternativet. Toppteksten og dataene i IP-pakkene blir kryptert.

Artikler	Innstillinger og forklaring	
Remote Gateway(Tunnel Mode)	Hvis du velger **Tunnel Mode** for **Encapsulation**, skriver du inn en gateway-adresse på mellom 1 og 39 tegn.	
Security Protocol	Velg et alternativ hvis du velger **IPsec** for **Access Control**.	
	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.
Algorithm Settings		
IKE	Encryption	Velg krypteringsalgoritme for IKE. Elementene vil variere avhengig av IKE-versjon.
	Authentication	Velg godkjenningsalgoritme for IKE.
	Key Exchange	Velg nøkkelendringsalgoritme for IKE. Elementene vil variere avhengig av IKE-versjon.
ESP	Encryption	Velg krypteringsalgoritme for ESP. Dette er tilgjengelig når **ESP** er valgt for **Security Protocol**.
	Authentication	Velg autorisasjonsalgoritme for ESP. Dette er tilgjengelig når **ESP** er valgt for **Security Protocol**.
AH	Authentication	Velg godkjenningsalgoritme for AH. Dette er tilgjengelig når **AH** er valgt for **Security Protocol**.

Relatert informasjon

➡ “Konfigurere Group Policy” på side 75

➡ “Kombinasjon av Local Address (Scanner) og Remote Address(Host) på Group Policy” på side 79

➡ “Referanser for tjenestenavn på gruppepolicy” på side 80

Kombinasjon av Local Address (Scanner) og Remote Address(Host) på Group Policy

		Innstilling av Local Address (Scanner)		
		IPv4	IPv6*2	Any addresses*3
Innstilling av Remote Address(Host)	IPv4*1	✓	–	✓
	IPv6*1*2	–	✓	✓
	Tom	✓	✓	✓

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

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

*3 Utenom IPv6-link-lokal-adresser.

Referanser for tjenestenavn på gruppepolicy

Merknad:
Utilgjengelige tjenester vil vises men kan ikke velges.

Tjenestenavn	Protokolltype	Lokalt portnummer	Eksternt portnummer	Kontrollerte funksjoner
Any	–	–	–	Alle tjenester
ENPC	UDP	3289	Hvilken som helst port	Søker etter en skanner fra programmer slik som EpsonNet Config og så en skannerdriver
SNMP	UDP	161	Hvilken som helst port	Henter og konfigurerer MIB fra programmer slik som EpsonNet Config og Epson-skannerdriveren
WSD	TCP	Hvilken som helst port	5357	Kontrollerer WSD
WS-Discovery	UDP	3702	Hvilken som helst port	Søker etter en skanner fra WSD
Network Scan	TCP	1865	Hvilken som helst port	Videresender skannerdata fra Document Capture Pro
Network Push Scan Discovery	UDP	2968	Hvilken som helst port	Søke etter en datamaskin fra skanneren.
Network Push Scan	TCP	Hvilken som helst port	2968	Henter jobbinformasjon for push-skanning fra Document Capture Pro eller Document Capture
HTTP (Local)	TCP	80	Hvilken som helst port	HTTP(S)-server (videresender data fra Web Config og WSD)
HTTPS (Local)	TCP	443	Hvilken som helst port	
HTTP (Remote)	TCP	Hvilken som helst port	80	HTTP(S)-klient (kommunikasjon mellom oppdatere fastvare og oppdatere rotsertifikat)
HTTPS (Remote)	TCP	Hvilken som helst port	443	

Eksempler på IPsec/IP Filtering

Mottar kun IPsec-pakker

Dette eksemplet viser kun hvordan du konfigurerer en standardpolicy.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **IPsec**

❏ **Authentication Method**: **Pre-Shared Key**

❏ **Pre-Shared Key**: Skriv inn opptil 127 tegn.

Group Policy:

Skal ikke konfigureres.

Akseptere skanning ved hjelp Epson Scan 2 og skannerinnstillinger

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

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **Refuse Access**

Group Policy:

❏ **Enable this Group Policy**: Merk av for dette alternativet.

❏ **Access Control**: **Permit Access**

❏ **Remote Address(Host)**: IP-adresse til en klient

❏ **Method of Choosing Port**: **Service Name**

❏ **Service Name**: Huk av boksen for **ENPC**, **SNMP**, **Network Scan**, **HTTP (Local)** og **HTTPS (Local)**.

Få tilgang kun fra en angitt IP-adresse

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

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**:**Refuse Access**

Group Policy:

❏ **Enable this Group Policy**: Merk av for dette alternativet.

❏ **Access Control**: **Permit Access**

❏ **Remote Address(Host)**: IP-adresse til en administrators klient

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

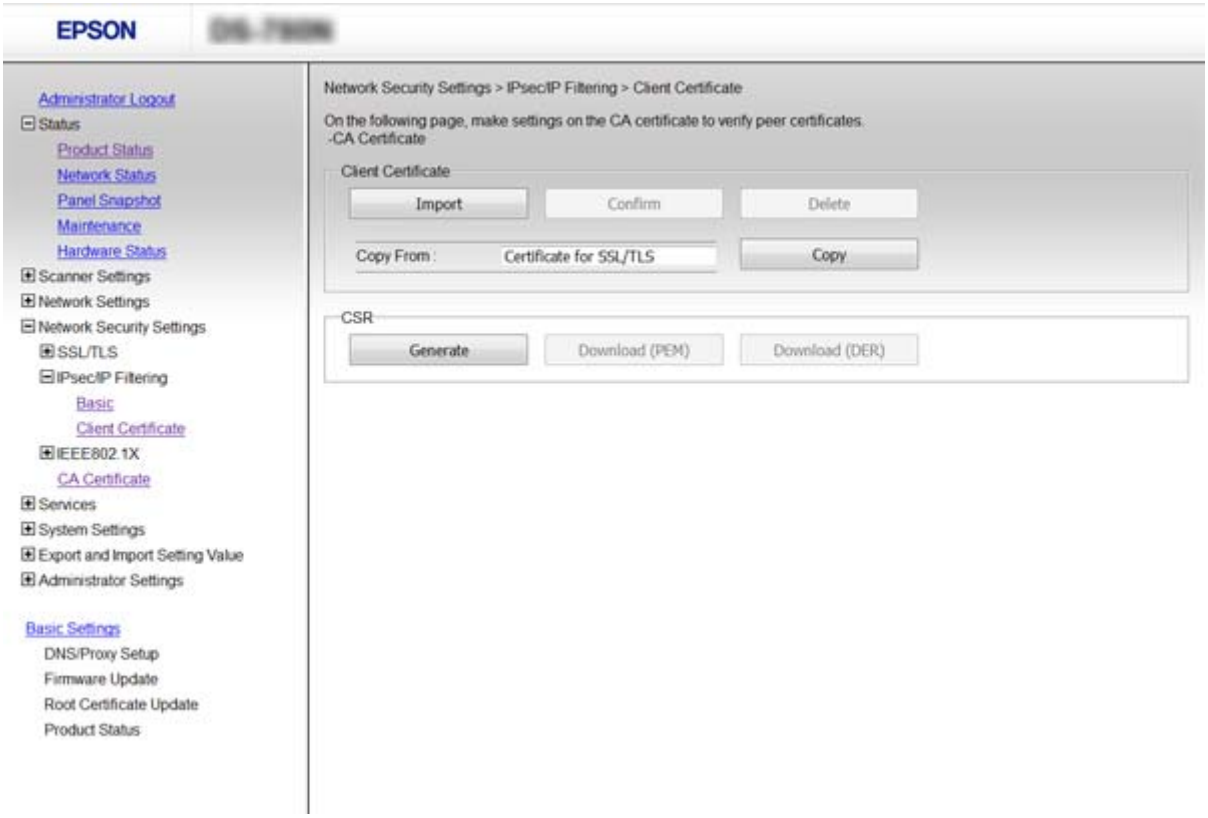
Konfigurere et sertifikat for IPsec/IP Filtering

Konfigurer klientsertifikat for IPsec/IP-filtrering. Hvis du vil konfigurere sertifiseringsinstans, går du til **CA Certificate**.

1. Gå inn på Web Config og velg **Network Security Settings** > **IPsec/IP Filtering** > **Client Certificate**.

2. Importer sertifikatet i **Client Certificate**.

   Hvis du allerede har importert et sertifikat utgitt av en sertifiseringsinstans i IEEE802.1X eller SSL/TLS, kan du kopiere sertifikatet og bruke det til IPsec/IP-filtrering. Slik kopierer du det: Velg sertifikatet fra **Copy From**, og klikk deretter **Copy**.



Relatert informasjon

➡ "Få tilgang til Web Config" på side 23

➡ "Hente og importere et CA-signert sertifikat" på side 64

Bruke SNMPv3-protokollen

Om SNMPv3

SNMP er en protokoll som utfører overvåking og kontroll for å samle informasjon om enhetene som kobles til nettverket. SNMPv3 er administrasjonssikkerhetsfunksjon-versjonen som har blitt forbedret.

Når du bruker SNMPv3, kan statlig overvåking og innstillingsendringer av SNMP-kommunikasjon (pakke) godkjennes og krypteres for å beskytte SNMP-kommunikasjon (pakke) fra nettverksrisiko, for eksempel telefonavlytting, etterligning og manipulering.

Konfigurere SNMPv3

Hvis skanneren støtter SNMPv3-protokollen kan du overvåke og kontrollere tilganger til skriveren.

1. Gå inn på Web Config og velg **Services** > **Protocol**.
2. Angi en verdi for hvert element av **SNMPv3 Settings**.
3. Klikk **Next**.

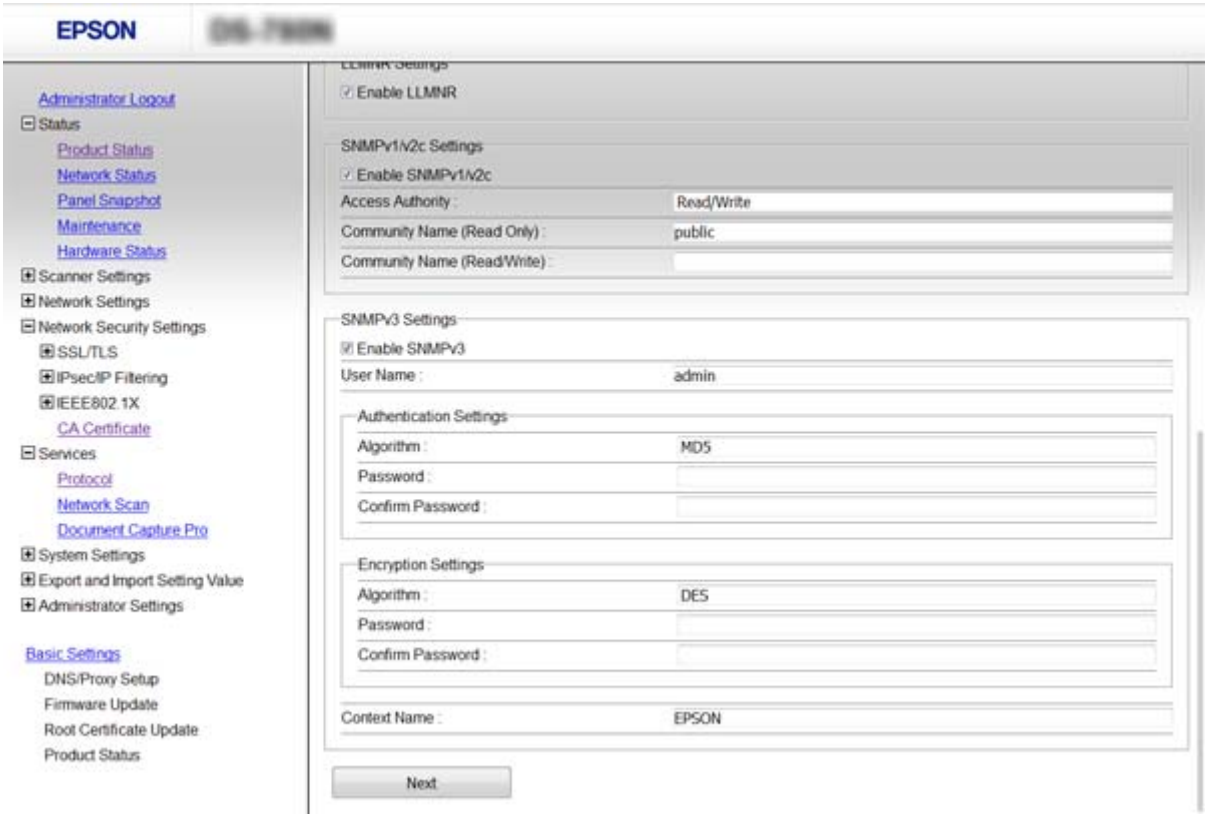
   Det vises en bekreftelsesmelding.
4. Klikk **OK**.

   Skanneren er oppdatert.

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23
➡ "Innstillingselementer for SNMPv3" på side 83

Innstillingselementer for SNMPv3



Elementer	Innstillinger og forklaring
Enable SNMPv3	SNMPv3 er aktivert når det er merket av for alternativet.
User Name	Skriv inn mellom 1 og 32 tegn ved hjelp av 1-byte-tegn.
Authentication Settings	
Algorithm	Velg en algoritme for godkjenning.

Elementer	Innstillinger og forklaring
Password	Skriv inn mellom 8 og 32 tegn i ASCII (0x20-0x7E).
Confirm Password	Skriv inn passordet du konfigurerte for bekreftelse.
Encryption Settings	
Algorithm	Velg en algoritme for kryptering.
Password	Skriv inn mellom 8 og 32 tegn i ASCII (0x20-0x7E).
Confirm Password	Skriv inn passordet du konfigurerte for bekreftelse.
Context Name	Skriv inn mellom 1 og 32 tegn ved hjelp av 1-byte-tegn.

Relatert informasjon

➡ “Konfigurere SNMPv3” på side 82

Koble skanneren til et IEEE802.1X-nettverk

Konfigurere et IEEE802.1X-nettverk

Hvis skanneren støtter IEEE802.1X, kan du bruke skriveren på et nettverk med godkjenning som er koblet til en RADIUS-server og en hub som godkjenner.

1. Gå inn på Web Config og velg **Network Security Settings** > **IEEE802.1X** > **Basic**.
2. Angi en verdi for hvert element.
3. Klikk på **Next**.

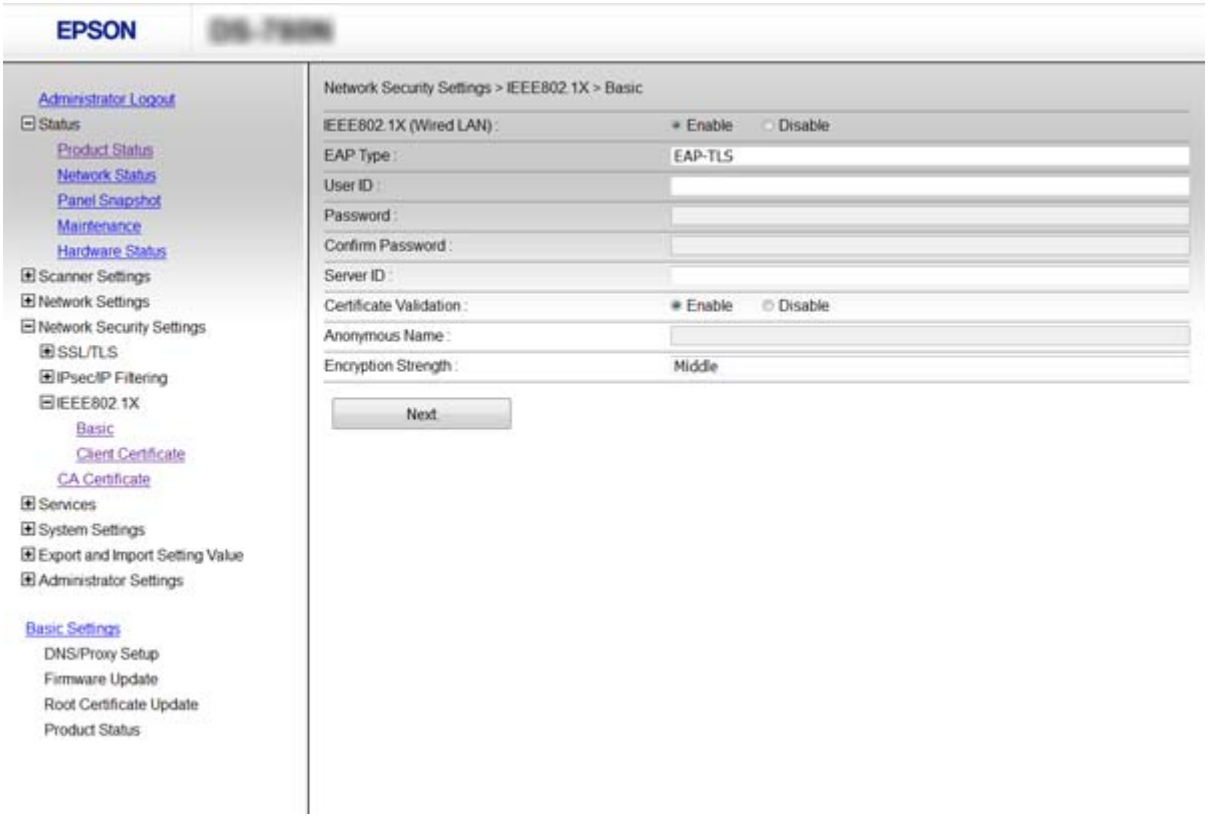
   Det vises en bekreftelsesmelding.
4. Klikk på **OK**.

   Skanneren er oppdatert.

Relatert informasjon

➡ “Få tilgang til Web Config” på side 23
➡ “Innstillingselementer for IEEE802.1X-nettverk” på side 85
➡ “Får ikke tilgang til skriveren eller skanneren etter konfigurering av IEEE802.1X” på side 89

Innstillingselementer for IEEE802.1X-nettverk



Artikler	Innstillinger og forklaring	
IEEE802.1X (Wired LAN)	Du kan aktivere eller deaktivere innstillingene på siden (**IEEE802.1X** > **Basic**) for IEEE802.1X (kablet LAN).	
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.
User ID	Konfigurer en ID som skal brukes som godkjenning av en RADIUS-server. Skriv inn 1 til 128 enkeltbyte ASCII-tegn (0x20 til 0x7E).	
Password	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.	
Confirm Password	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).	
Certificate Validation	Du kan stille inn sertifikatvalidering uavhengig av autentiseringsmetode. Importer sertifikatet i **CA Certificate**.	

Artikler	Innstillinger og forklaring	
Anonymous Name	Hvis du velger **PEAP-TLS** eller **PEAP/MSCHAPv2** for **Authentication Method**, 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).	
Encryption Strength	Du kan velge én av følgende.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Relatert informasjon

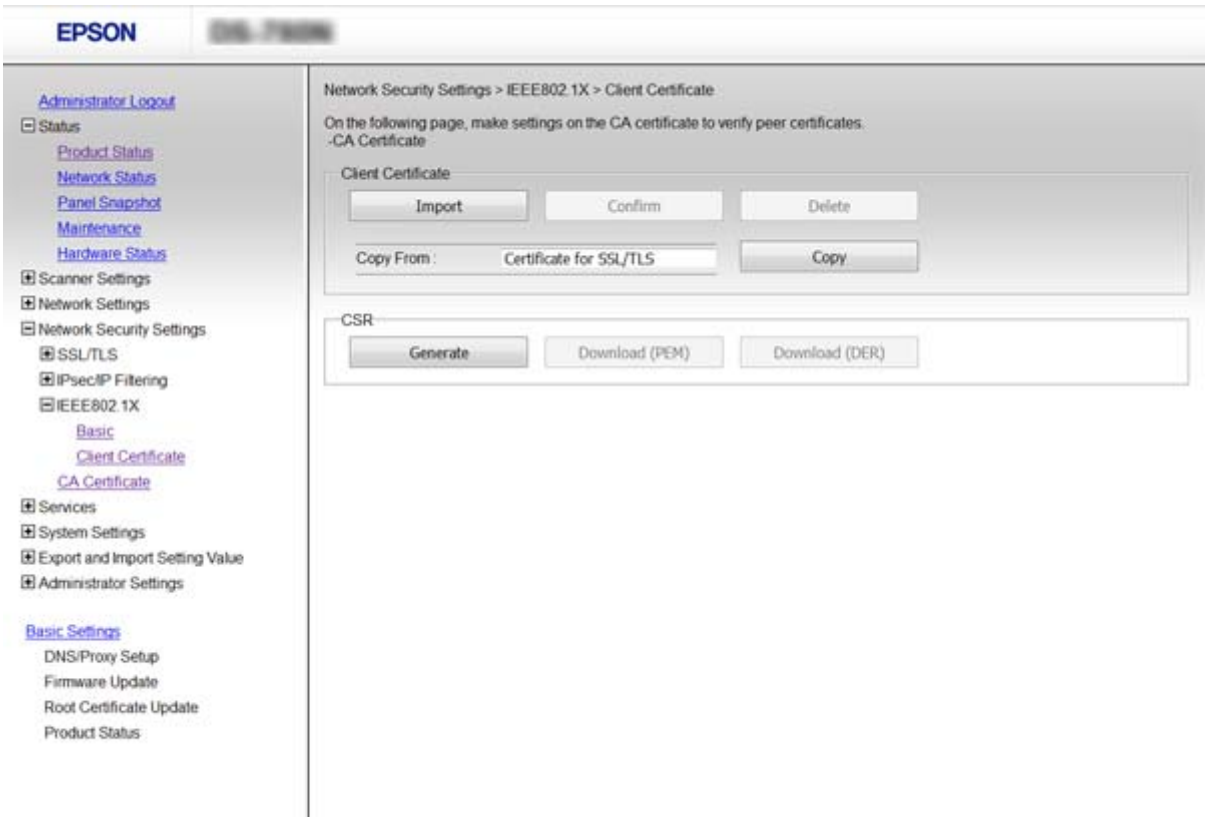
➡ "Konfigurere et IEEE802.1X-nettverk" på side 84

Konfigurere et sertifikat for IEEE802.1X

Konfigurer klientsertifikat for IEEE802.1X. Hvis du vil konfigurere sertifiseringsinstanssertifikatet, går du til **CA Certificate**.

1. Gå inn på Web Config og velg **Network Security Settings** > **IEEE802.1X** > **Client Certificate**.
2. Angi et sertifikat i **Client Certificate**.

   Du kan kopiere sertifikatet hvis det er publisert av en sertifiseringsinstans. Slik kopierer du det: Velg sertifikatet fra **Copy From**, og klikk deretter **Copy**.



Relatert informasjon

➡ "Få tilgang til Web Config" på side 23

➡ "Hente og importere et CA-signert sertifikat" på side 64

Løse problemer med avanserte sikkerhetsinnstillinger

Gjenopprette sikkerhetsinnstillingene

Når du oppretter et svært sikkert miljø slik som IPsec/IP-filtrering eller IEEE802.1X, 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 fra kontrollpanelet

Du kan deaktivere IPsec/IP-filtrering eller IEEE802.1X fra skannerens kontrollpanel.

1. Trykk **Innst.** > **Nettverksinnstillinger**.
2. Trykk **Endre innstillinger**.
3. Trykk på elementene du vil deaktivere.
   - ❏ **IPsec/IP-filtrering**
   - ❏ **IEEE802.1X**
4. Trykk **Forts.** når det vises en melding om at oppsettet er fullført.

Gjenoppretting av sikkerhetsfunksjon ved hjelp av Web Config

For IEEE802.1X vil enheter kanskje ikke bli oppdaget av nettverket. I dette tilfellet må du deaktivere funksjonen ved å bruke skannerens kontrollpanel.

For IPsec/IP-filtrering kan du deaktivere funksjonen dersom du får tilgang til enheten fra datamaskinen.

Deaktivere IPsec/IP-filtrering med Web Config

1. Gå inn på Web Config og velg **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Velg **Disable** for **IPsec/IP Filtering** i **Default Policy**.
3. Klikk **Next**, og slett deretter **Enable this Group Policy** for alle grupperegler.
4. Klikk på **OK**.

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23

Problemer ved bruk av funksjoner for nettverkssikkerhet

Glemt en forhåndsdelt tast

Konfigurer tasten på nytt med Web Config.

For å endre tasten,gå inn på Web Config og velg **Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Default Policy** eller **Group Policy**.

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

Relatert informasjon

➡ "Få tilgang til Web Config" på side 23

Kan ikke kommunisere med IPsec-kommunikasjon

Bruker du en algoritme som ikke støttes i innstillingene for datamaskinen?

Skanneren støtter følgende algoritmer.

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-gruppe 1, DH-gruppe 2, DH-gruppe 5, DH-gruppe 14, DH-gruppe 15, DH-gruppe 16, DH-gruppe 17, DH-gruppe 18, DH-gruppe 19, DH-gruppe 20, DH-gruppe 21, DH-gruppe 22, DH-gruppe 23, DH-gruppe 24, DH-gruppe 25, DH-gruppe 26, DH-gruppe 27*, DH-gruppe 28*, DH-gruppe 29*, DH-gruppe 30*
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 71

Kan plutselig ikke kommunisere

Er skannerens IP-adresse ugyldig eller er den blitt endret?

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 (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**) kanskje ikke bli oppdaget.

Bruk en statisk IP-adresse.

Er datamaskinens IP-adresse ugyldig eller er den blitt endret?

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 (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) kanskje ikke bli oppdaget.

Bruk en statisk IP-adresse.

Relatert informasjon

➡ “Få tilgang til Web Config” på side 23

➡ “Kryptert kommunikasjon ved bruk av IPsec/IP-filtrering” på side 71

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

Den innstilte verdien kan være 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 71

Får ikke tilgang til skriveren eller skanneren etter konfigurering av IEEE802.1X

Innstillingene kan være feil.

Deaktiver IEEE802.1X fra skannerens kontrollpanel. Koble til skanneren og en datamaskin, og konfigurer deretter IEEE802.1X igjen.

Relatert informasjon

➡ “Konfigurere et IEEE802.1X-nettverk” på side 84

Problemer med å bruke et digitalt sertifikat

Kan ikke importere et CA-signert sertifikat

Samsvarer det CA-signerte sertifikatet og informasjonen på CSR-en?

Hvis det CA-signerte sertifikatet 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.

Er det CA-signerte sertifikatet større enn 5 kB?

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

Er det riktig passord for å importere sertifikatet?

Hvis du glemmer passordet, kan du ikke importere sertifikatet.

Relatert informasjon

➡ "Importere et CA-signert sertifikat" på side 65

Kan ikke oppdatere et selvsignert sertifikat

Er Common Name angitt?

Common Name må være angitt.

Har du angitt tegn som ikke støttes for Common Name? Japansk støttes for eksempel ikke.

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

Er komma eller mellomrom tatt med i Common Name?

Hvis du har skrevet inn et komma, vil **Common Name** 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 68

Kan ikke opprette CSR

Er Common Name angitt?

Common Name må være angitt.

Har du angitt tegn som ikke støttes, under Common Name, Organization, Organizational Unit, Locality, State/Province? Japansk støttes for eksempel ikke.

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

Er komma eller mellomrom tatt med i Common Name?

Hvis du har skrevet inn et komma, vil **Common Name** 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 64

Det vises en advarsel om digitalt sertifikat

Meldinger	Årsak/Dette skal du gjøre
Enter a Server Certificate.	**Årsak:** Du har ikke valgt hvilken fil som skal importeres. **Dette skal du gjøre:** Velg filen, og klikk **Import**.
CA Certificate 1 is not entered.	**Årsak:** CA-sertifikat 1 er ikke angitt, og kun CA-sertifikat 2 er angitt. **Dette skal du gjøre:** Importer CA-sertifikat 1 først.
Invalid value below.	**Årsak:** Filbanen og/eller passordet inneholder tegn som ikke støttes. **Dette skal du gjøre:** Kontroller at tegnene er riktig angitt for elementet.
Invalid date and time.	**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.
Invalid password.	**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
Invalid file.	**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.
Cannot use the Server Certificates that include more than three CA certificates.	**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.
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**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.
Private key is required.	**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
Setup failed.	**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 63

Slette et CA-signert sertifikat ved et uhell

Finnes det en sikkerhetskopifil av 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

➡ “Slette et CA-signert sertifikat” på side 67

➡ “Importere et CA-signert sertifikat” på side 65