EPSON
EXCEED YOUR VISION

Administratorvejledning

NPD5668-00 DA

Indholdsfortegnelse

Copyright

Varemærker

Om denne vejledning

Mærker og symboler. 6
Anvendte beskrivelser i denne vejledning. 6
Henvisninger til operativsystemer. 6

Introduktion

Vejledningskomponent. 8
Definitioner af udtryk, der er anvendt i denne vejledning. 8

Forberedelse

Strøm af scannerindstillinger og styring. 10
Eksempel på netværksmiljø. 11
Eksempel på indstilling af scannerforbindelse. . . 11
Forberedelse af tilslutning til et netværk. 12
Indsamling af oplysninger om indstillinger for forbindelse. 12
Specifikationer for scanner. 12
Brug af portnummer. 13
Typer af tildeling af IP-adresse. 13
DNS-server og proxyserver. 13
Metode til indstilling af netværksforbindelse. . . . 13

Tilslutning

Tilslutning til netværket. 15
Tilslutning til netværket fra kontrolpanelet. 15
Tilslutning til netværket ved hjælp af installationsprogrammet. 19

Funktionsindstillinger

Software til opsætning. 22
Web Config (enhedens hjemmeside). 22
Brug af scanningsfunktioner. 24
Scanning fra en computer. 24
Scanning vha. kontrolpanelet. 26
Overføre systemindstillinger. 28
Systemindstillinger på kontrolpanelet. 28
Systemindstillinger ved hjælp af Web Config. . . . 30

Grundlæggende sikkerhedsindstillinger

Introduktion til grundlæggende sikkerhedsfunktioner. 32
Konfiguration af administratoradgangskode. 32
Konfiguration af administratoradgangskoden fra kontrolpanelet. 33
Konfiguration af administratoradgangskode ved hjælp af Web Config. 33
Elementer, der skal låses med administratoradgangskode. 34
Styring af protokoller. 35
Protokoller, du kan aktivere eller deaktivere. 36
Protokolindstillingselementer. 37

Indstillinger for betjening og administration

Bekræft oplysninger for en enhed. 40
Administration af enheder (Epson Device Admin). .40
Modtagelse af meddelelser med e-mail, når hændelser opstår. 41
Om e-mail-meddelelser. 41
Konfigurere email-meddelelser. 41
Konfiguration af en mailserver. 42
Kontrol af en mailserverforbindelse. 44
Opdatering af firmware. 46
Opdatering af firmware ved hjælp af Web Config. 46
Opdatering af firmware ved hjælp af Epson Firmware Updater. 46
Sikkerhedskopiering af indstillingerne. 47
Eksport af indstillingerne. 47
Import af indstillingerne. 47

Problemløsning

Tip til problemløsning. 49
Kontrol af log for server og netværksenhed. 49
Initialisering af netværksindstillingerne. 49
Gendannelse af netværksindstillingerne fra kontrolpanelet. 49
Kontrol af kommunikation mellem enheder og computere. 49
Kontrol af forbindelse vha. en ping-kommando — Windows. 49

Kontrol af forbindelse vha. en ping-kommando — Mac OS. 51
Problemer med brug af netværkssoftwaren. 52
Kan ikke få adgang til Web Config. 52
Modelnavn og/eller IP-adresse vises ikke på EpsonNet Config. 53

Appendiks

Introduktion til netværkssoftware. 55
Epson Device Admin. 55
EpsonNet Config. 55
EpsonNet SetupManager. 56
Tildeling af en IP-adressen ved hjælp af EpsonNet Config. 56
Tildeling af IP-adresse ved hjælp af batchindstillinger. 56
Tildeling af en IP-adresse til hver enhed. 59
Brug af port til scanneren. 60

Avancerede sikkerhedsindstillinger for virksomheder

Sikkerhedsindstillinger og forebyggelse af fare. 62
Indstillinger for sikkerhedsfunktioner. 63
SSL/TLS-kommunikation med scanneren. 63
Om digitalt certifikat. 63
Hentning og import af et CA-signeret certifikat. . 64
Sletning af et CA-signeret certifikat. 67
Opdatering af et selvsigneret certifikat. 68
Konfiguration af CA Certificate. 69
Krypteret kommunikation ved hjælp af IPsec/IP-filtrering. 71
Om IPsec/IP Filtering. 71
Konfiguration af Default Policy. 72
Konfiguration af Group Policy. 75
Eksempler på konfiguration af IPsec/IP Filtering. 80
Konfiguration af et certifikat til IPsec/IP Filtering. 81
Brug af SNMPv3-protokol. 82
Om SNMPv3. 82
Konfiguration af SNMPv3. 82
Tilslutning af scanneren til et IEEE802.1X-netværk. 84
Konfiguration af et IEEE802.1X-netværk. 84
Konfiguration af et certifikat til IEEE802.1X. . . . 86
Problemløsning for avanceret sikkerhed. 87
Gendannelse af sikkerhedsindstillingerne. 87
Problemer med brug af netværkssikkerhedsfunktioner. 88
Problemer med brug af et digitalt certifikat. 90

Copyright

Varemærker

- ❏ EPSON® er et registreret varemærke, og EPSON EXCEED YOUR VISION eller EXCEED YOUR VISION er et varemærke tilhørende 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.
- ❏ Generel bemærkning: Andre produktnavne, der nævnes heri, anvendes udelukkende til identifikationsformål og kan være varemærker tilhørende deres respektive ejere. Epson frasiger sig alle rettigheder til disse mærker.

Om denne vejledning

Mærker og symboler

> ⚠ ***Forsigtig:***
> *Anvisninger, der skal følges omhyggeligt for at undgå personskader.*

> ***Vigtigt:***
> *Anvisninger, der skal følges for at undgå beskadigelse af udstyret.*

Bemærk:
Anvisninger, der indeholder nyttige tip og begrænsninger vedrørende brug af scanneren.

Relaterede oplysninger

➡ Klik på dette ikon for at se relaterede oplysninger.

Anvendte beskrivelser i denne vejledning

❏ Skærmbillederne af scannerdriveren og Epson Scan 2 (scannerdriveren) er fra Windows 10 eller OS X El Capitan. Det viste skærmindhold varierer afhængigt af modellen og situationen.

❏ Illustrationerne i denne vejledning er vejledende. Selvom der kan være små forskelle afhængigt af modellen, er betjeningsmetoden den samme.

❏ Nogle af menupunkterne på LCD-skærmen varierer afhængigt af modellen og indstillingerne.

Henvisninger til operativsystemer

Windows

I denne vejledning henviser udtryk som "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. Windows bruges desuden til at henvise til alle versioner.

❏ 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 denne manual bruges "Mac OS" til at henvise 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.

Introduktion

Vejledningskomponent

Denne vejledning er til enhedens administrator, der er ansvarlig for at slutte en printer eller scanner til netværket, og den indeholder oplysninger om, hvordan man kan foretage indstillinger for at bruge funktionerne.

Se *Brugervejledning* for oplysninger om funktioner.

Forberedelse

Forklarer administratorens opgaver, hvordan enheder indstilles, og software til styring.

Tilslutning

Forklarer, hvordan man slutter en enhed til et netværk eller en telefonlinje. Den forklarer også netværksmiljøet, f.eks. brug af en port til enheden, DNS og proxyserveroplysninger.

Funktionsindstillinger

Forklarer indstillingerne for hver af enhedens funktioner.

Grundlæggende sikkerhedsindstillinger

Forklarer indstillingerne for hver funktion, såsom udskrivning, scanning og fax.

Indstillinger for betjening og administration

Forklarer betjeningen efter påbegyndelse af brug af enheder, såsom informationskontrol og vedligeholdelse.

Løsning af problemer

Forklarer initialisering af indstillinger og fejlfinding af netværket.

Avancerede sikkerhedsindstillinger for virksomheder

Forklarer indstillingsmetoden til at forbedre enhedens sikkerhed, f.eks. brug af CA-certifikat, SSL/TLS-kommunikation og IPsec/IP-filtrering.

Afhængigt af modellen er nogle af funktionerne i dette kapitel ikke understøttet.

Definitioner af udtryk, der er anvendt i denne vejledning

Følgende udtryk er anvendt i denne vejledning.

Administrator

Den person, der har ansvaret for installation og opsætning af enheden eller netværket på et kontor eller en organisation. I mindre organisationer kan denne person være ansvarlig for både enheds- og netværksadministration. I store organisationer har administratorer autoritet over netværket eller enheder i en

afdelings enhedsgruppe, og netværksadministratorer står for opsætning af virksomhedens eksterne kommunikationsindstillinger, såsom internettet.

Netværksadministrator

Den person, der har ansvaret for at kontrollere netværkskommunikationen. Den person, der konfigurerer router, proxyserver, DNS-server og mailserver til at styre kommunikationen via internettet eller netværket.

Bruger

Den person, der bruger enheder som f.eks. printere og scannere.

Web Config (enhedens hjemmeside)

Den webserver, der er indbygget i enheden. Den kaldes Web Config. Du kan kontrollere og ændre enhedsstatus på den ved hjælp af browseren.

Værktøj

En generisk betegnelse for software til opsætning og styring af en enhed, såsom Epson Device Admin, EpsonNet Config, EpsonNet SetupManager osv.

Push-scanning

En generisk betegnelse for scanning fra enhedens kontrolpanel.

ASCII (American Standard Code for Information Interchange)

En af standardtegnkoderne. 128 tegn er defineret, herunder tegn som alfabetet (a–z, A–Z), arabiske tal (0–9), symboler, blanktegn og kontroltegn. Når "ASCII" er beskrevet i denne vejledning, betyder det 0x20–0x7E (hex-nummer), som er angivet nedenfor, og omfatter ikke kontroltegn.

SP*	!	\"	#	$	%	og	'	(	)	*	+	,	-	.	/
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	{	|	}	~	

* Mellemrumstegn.

Unicode (UTF-8)

En international standardkode, der dækker de store globale sprog. Når "UTF-8" er beskrevet i denne vejledning, betyder det kodningstegn i UTF-8-format.

Forberedelse

Dette kapitel forklarer administratorens rolle og forberedelse før indstillinger.

Strøm af scannerindstillinger og styring

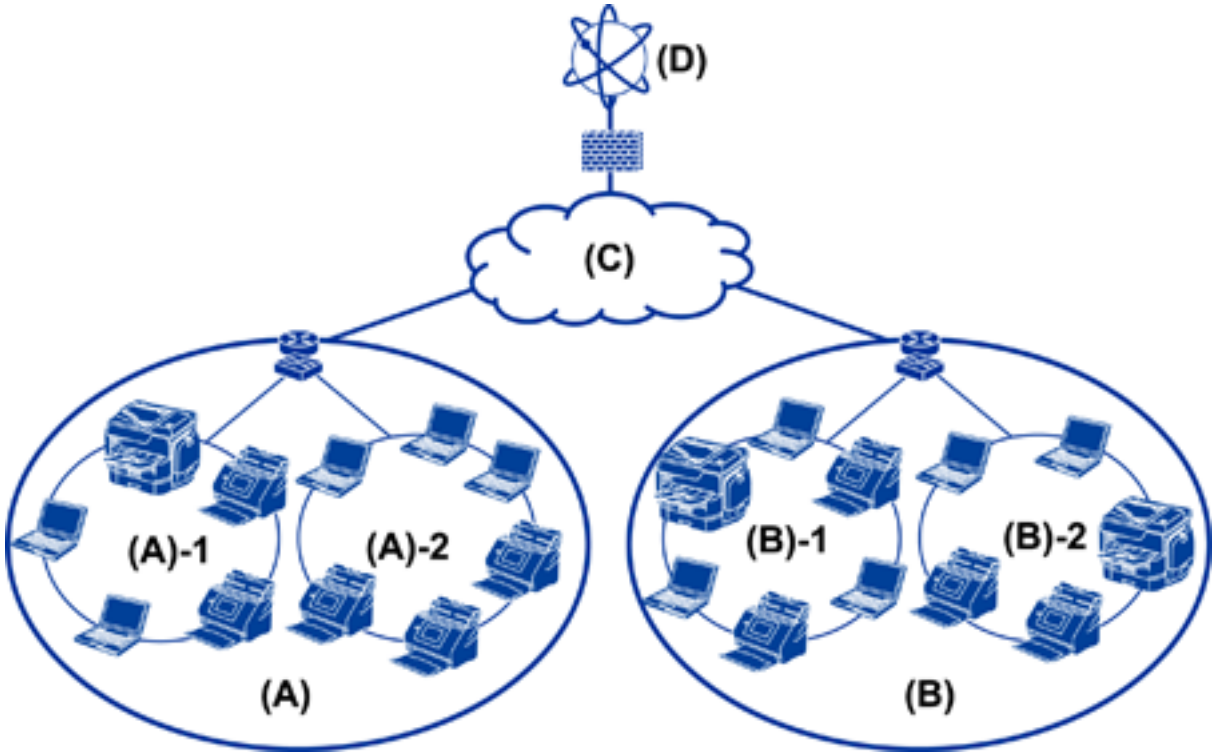
Administratoren foretage indstillingerne for netværksforbindelsen, den indledende opsætning og vedligeholdelse af scanneren, så de kan være til rådighed for brugerne.

1. Klargøring
   - ❏ Indsamling af oplysninger til indstilling af forbindelsen
   - ❏ Afgørelse om tilslutningsmetode
2. Forbinder
   - ❏ Netværksforbindelse fra scannerens kontrolpanel
3. Opsætning af funktioner
   - ❏ Scannerdriverens indstillinger
   - ❏ Andre avancerede indstillinger
4. Sikkerhedsindstillinger
   - ❏ Administratorindstillinger
   - ❏ SSL/TLS
   - ❏ Protokolkontrol
   - ❏ Avancerede sikkerhedsindstillinger (tilbehør)
5. Betjening og styring
   - ❏ Kontrol af enhedens status
   - ❏ Håndtering af hændelser
   - ❏ Sikkerhedskopiering af enhedens indstillinger

Relaterede oplysninger

➡ “Forberedelse” på side 10
➡ “Tilslutning” på side 15
➡ “Funktionsindstillinger” på side 22
➡ “Grundlæggende sikkerhedsindstillinger” på side 32
➡ “Indstillinger for betjening og administration” på side 40

Eksempel på netværksmiljø



(A): Kontor 1

❏ (A) – 1: LAN 1

❏ (A) – 2: LAN 2

(B): Kontor 2

❏ (B) – 1: LAN 1

❏ (B) – 2: LAN 2

(C): WAN

(D): Internet

Eksempel på indstilling af scannerforbindelse

Der er primært to forbindelsestyper, afhængigt af hvordan du bruger scanneren. Begge typer tilslutter scanneren til netværket med computeren via hubben.

❏ Server/klient-forbindelse (scanner ved hjælp af Windows-server, jobadministration)

❏ Peer-to-peer-forbindelse (direkte forbindelse med klientcomputer)

Relaterede oplysninger

➡ “Server/klient-forbindelse” på side 12

➡ “Peer-to-peer-forbindelser” på side 12

Server/klient-forbindelse

Centraliser scanner og jobadministration med Document Capture Pro Server, som er installeret på serveren. Det er bedst egnet til arbejde, der bruger flere scannere til at scanne et stort antal dokumenter i et bestemt format.

Relaterede oplysninger

➡ "Definitioner af udtryk, der er anvendt i denne vejledning" på side 8

Peer-to-peer-forbindelser

Brug en individuel scanner med en scannerdriver såsom Epson Scan 2, som er installeret på klientcomputeren. Når du installerer Document Capture Pro (Document Capture) på klientcomputeren, er det muligt at køre job på scannerens individuelle klientcomputere.

Relaterede oplysninger

➡ "Definitioner af udtryk, der er anvendt i denne vejledning" på side 8

Forberedelse af tilslutning til et netværk

Indsamling af oplysninger om indstillinger for forbindelse

Du skal have en IP-adresse, gateway-adresse osv. til netværksforbindelsen. Kontroller følgende på forhånd.

Afdelinger	Punkter	Bemærk
Enhedens forbindelsesmetode	❏ Ethernet	Brug et kabel af kategori 5e eller højere STP (Shielded Twisted Pair) til Ethernet-forbindelse.
Oplysninger om LAN-forbindelse	❏ IP-adresse ❏ Undernetmaske ❏ Standardgateway	Hvis du automatisk indstiller IP-adressen ved hjælp af routerens DHCP-funktion, er det ikke nødvendigt.
Oplysninger om DNS-information	❏ IP-adresse for primær DNS ❏ IP-adresse for sekundær DNS	Hvis du bruger en statisk IP-adresse som IP-adresse, skal du konfigurere DNS-serveren. Konfigurer, når du tildeler automatisk, ved hjælp af DHCP-funktionen, og når DNS-serveren kan ikke tildeles automatisk.
Oplysninger om proxyserver	❏ Navn på proxyserver ❏ Portnummer	Konfigurer, når du bruger en proxyserver til internetforbindelse, og når du bruger Epson Connect-tjenesten eller firmwaren automatiske opdateringsfunktion.

Specifikationer for scanner

For specifikationer, som scanneren understøtter i standard eller forbindelsestilstand, se *Brugervejledning*.

Brug af portnummer

Se "Bilag" for det portnummer, som scanneren bruger.

Relaterede oplysninger

➡ “Brug af port til scanneren” på side 60

Typer af tildeling af IP-adresse

Der findes to typer af tildeling af en IP-adresse til scanneren.

Statisk IP-adresse:

Tildel forudbestemte unikke IP-adresse til scanneren.

IP-adressen bliver ikke ændret, selv når du slukker for scanneren eller routeren, så du kan styre enheden ved IP-adressen.

Denne type er velegnet til et netværk, hvor mange scannere administreres, såsom et stort kontor eller en skole.

Automatisk tildeling af DHCP-funktion:

Den korrekte IP-adresse tildeles automatisk, når kommunikationen mellem scanneren og routeren, der understøtter DHCP-funktionen, lykkes.

Hvis det er ubelejligt at ændre IP-adressen for en bestemt enhed, kan du reservere IP-adressen på forhånd og derefter tildele den.

DNS-server og proxyserver

Hvis du bruger en internetforbindelsestjeneste, skal du konfigurere DNS-serveren. Hvis du ikke konfigurerer den, skal du angive IP-adressen for at få adgang, fordi navneoversættelsen kan mislykkes.

Proxyserveren er placeret ved porten mellem netværket og internettet, og den kommunikerer til computeren, scanneren og internettet (modsat server) på vegne af hver af dem. Det modsatte server kommunikerer kun til proxyserveren. Derfor kan scanneroplysninger såsom IP-adresse og portnummer ikke læses, og der kan forventes øget sikkerhed.

Du kan forbyde adgang til en bestemt webadresse ved hjælp af filtrering, da proxyserveren kan kontrollere indholdet af kommunikationen.

Metode til indstilling af netværksforbindelse

For forbindelsesindstillinger for scannerens IP-adresse, undernetmaske og standardgateway gøres følgende.

Brug af kontrolpanelet:

Konfigurer indstillingerne ved hjælp af scannerens kontrolpanel for hver scanner. Opret forbindelse til netværket efter at have konfigureret indstillingerne for scannerforbindelsen.

Brug af installationsprogrammet:

Hvis installationsprogrammet anvendes, indstilles scannerens netværk og klientcomputeren automatisk. Indstillingen kan foretages ved at følge anvisningerne i installationsprogrammet, selvom du ikke har indgående kendskab til netværket.

Brug af et værktøj:

Brug et værktøj fra administratorens computer. Du kan finde en scanner og derefter indstille printeren eller oprette en SYLK-fil til at foretage batchindstillinger for scannere. Du kan indstille mange scannere, men de skal være forbundet fysisk med et Ethernet-kabel før indstilling. Derfor anbefales det, at du opretter et Ethernet for indstillingen.

Relaterede oplysninger

➡ “Tilslutning til netværket fra kontrolpanelet” på side 15

➡ “Tilslutning til netværket ved hjælp af installationsprogrammet” på side 19

➡ “Tildeling af en IP-adressen ved hjælp af EpsonNet Config” på side 56

Tilslutning

Dette kapitel forklarer miljøet eller proceduren for at tilslutte scanneren til netværket.

Tilslutning til netværket

Tilslutning til netværket fra kontrolpanelet

Slut scanneren til netværket ved hjælp af scannerens kontrolpanel.

For at gå til scannerens kontrolpanel skal du se *Brugervejledning* for yderligere oplysninger.

Tildeling af IP-adressen

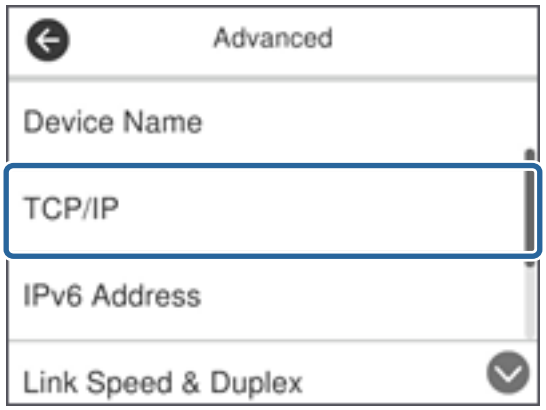
Opsæt de grundlæggende elementer såsom IP-adresse, Subnetmaske og Standard-gateway.

1. Tænd for scanneren.
2. Svip skærmen til venstre på scanneren kontrolpanel, og tryk derefter på **Indstillinger**.

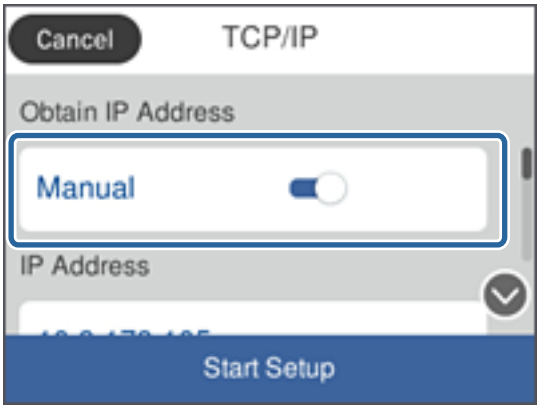
3. Tryk på **Netværksindstillinger** > **Skift indstillinger**.

   Hvis elementet ikke vises, skal du svippe skærmen opad for at få det vist.

4. Tryk på **TCP/IP**.

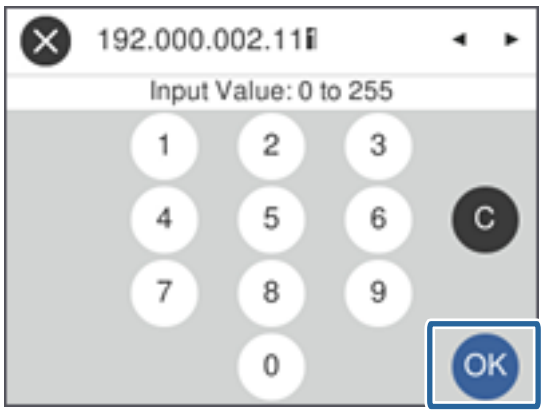


5. Vælg **Manuel** ved punktet **Hent IP-adresse**.



Bemærk:
*Når du indstiller IP-adressen automatisk ved hjælp af routerens DHCP-funktion, skal du vælge **Auto**. I dette tilfælde bliver **IP-adresse**, **Subnetmaske** og **Standard-gateway** i trin 6 til 7 også indstillet automatisk, så gå til trin 8.*

6. Tryk på feltet **IP-adresse**, indtast IP-adressen ved hjælp af tastaturet på skærmen, og tryk derefter på **OK**.



Bekræft værdien, som vises på den forrige skærm.

7. Indstil **Subnetmaske** og **Standard-gateway**.

Bekræft værdien, som vises på den forrige skærm.

Bemærk:
Hvis kombinationen af IP-adresse, Subnetmaske og Standard-gateway ikke er korrekt, er ***Start opsætning*** *inaktiv og kan ikke fortsætte med indstillingerne. Bekræft, at der ikke er nogen fejl i indtastningen.*

8. Tryk på feltet **Primære DNS** for **DNS-server**, indtast IP-adressen for den primære DNS-server ved hjælp af tastaturet på skærmen, og tryk derefter på **OK**.

   Bekræft værdien, som vises på den forrige skærm.

   Bemærk:
   Når du vælger ***Auto*** *for indstillingerne til tildeling af IP-adresse, kan du vælge DNS serverindstillingerne fra* ***Manuel*** *eller* ***Auto****. Hvis du ikke kan få DNS-serveradressen automatisk, skal du vælge* ***Manuel*** *og indtaste DNS-serveradressen. Indtast derefter den sekundære DNS-serveradresse direkte. Hvis du vælger* ***Auto****, skal du gå til trin 10.*

9. Tryk på feltet **Sekundær DNS**, indtast IP-adressen for den sekundære DNS-server ved hjælp af tastaturet på skærmen, og tryk derefter på **OK**.

   Bekræft værdien, som vises på den forrige skærm.

10. Tryk på **Start opsætning**.

11. Tryk på **Luk** på bekræftelsesskærmbilledet.

    Skærmen slukker automatisk efter en angiven tid, hvis du ikke trykker på **Luk**.

Tilslutning til Ethernet

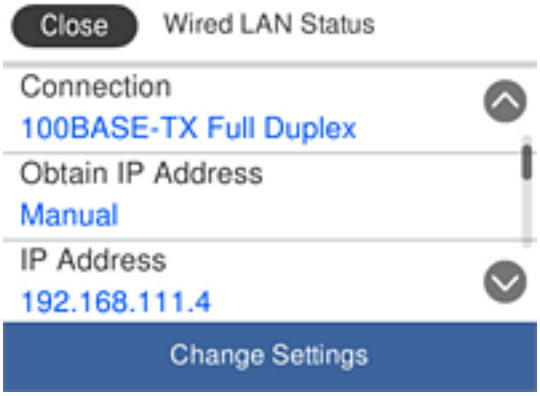
Slut scanneren til netværket ved hjælp af Ethernet-kablet, og kontroller forbindelsen.

1. Tilslut scanneren og hub (L2 switch) via Ethernet-kabel.

   Ikonet på startskærmen ændres til  .

2. Tryk på  på startskærmen.

3. Svirp skærmen opad, og kontroller, at status på forbindelsen og IP-adressen er korrekt.



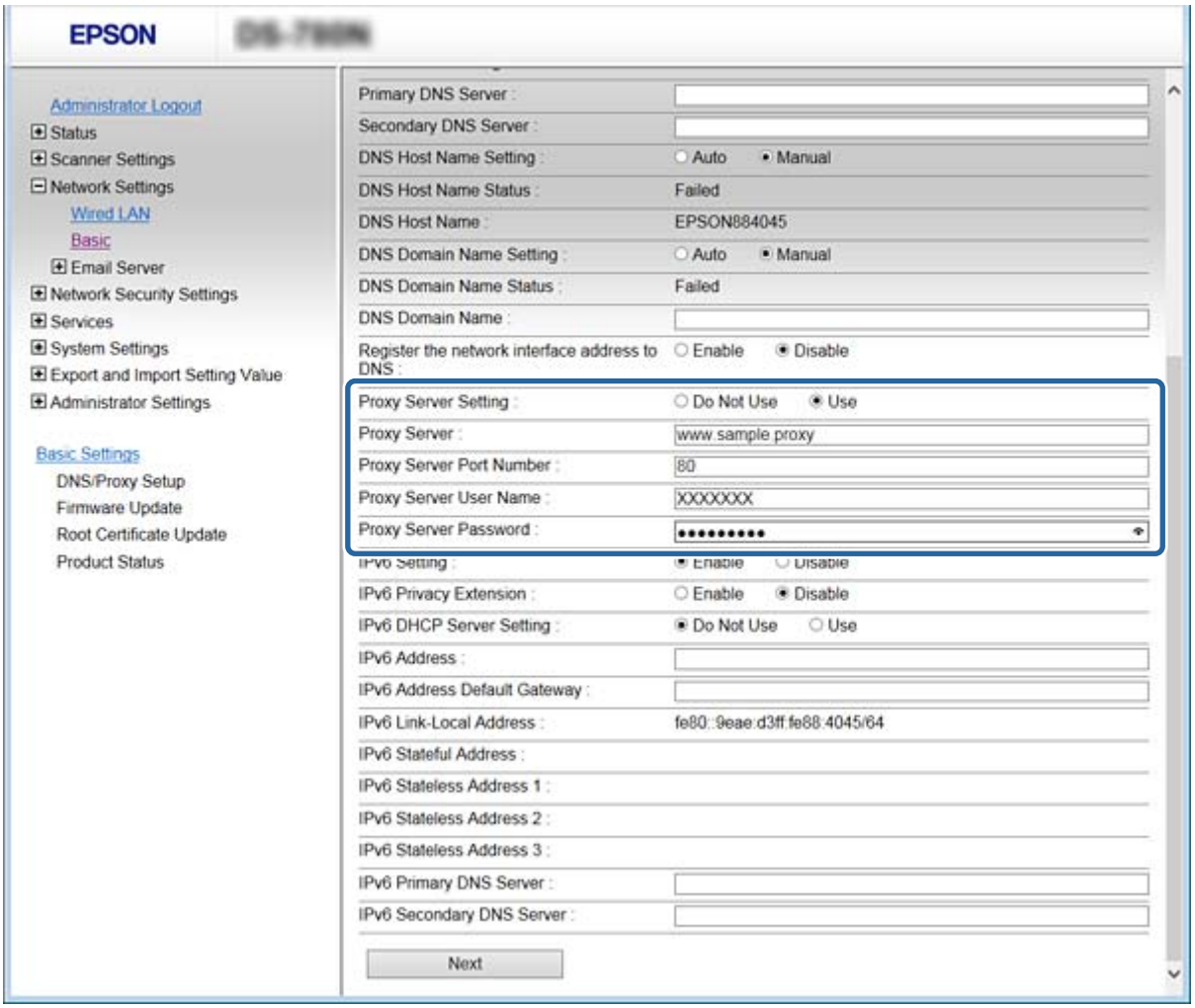
Indstilling af proxyserver

Proxyserveren kan ikke indstilles på panelet. Konfigurere ved brug af Web Config.

1. Gå til Web Config og vælg **Network Settings** > **Basic**.
2. Vælg **Use** i **Proxy Server Setting**.
3. Angiv proxyserver i IPv4-adresse eller FQDN-format i **Proxy-server**, og indtast herefter portnummeret i **Proxy Server Port Number**.

   For proxyservere, der kræver godkendelse, skal du indtaste brugernavn og adgangskode for godkendelse af proxyserveren.

4. Klik på knappen **Next**.



5. Bekræft indstillingerne, og klik derefter på **Indstillinger**.

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23

Tilslutning til netværket ved hjælp af installationsprogrammet

Vi anbefaler at køre installationsprogrammet til at tilslutte scanneren til en computer. Du kan køre installationsprogrammet vha. en af følgende metoder.

❏ Konfiguration fra webstedet

Gå ind på følgende websted, og indtast derefter produktnavnet. Gå til **Opsætning**, og påbegynd konfiguration.

http://epson.sn

❏ Konfiguration ved hjælp af softwaredisk (kun for modeller, der leveres med en softwaredisk, og brugere med computere med diskdrev.)

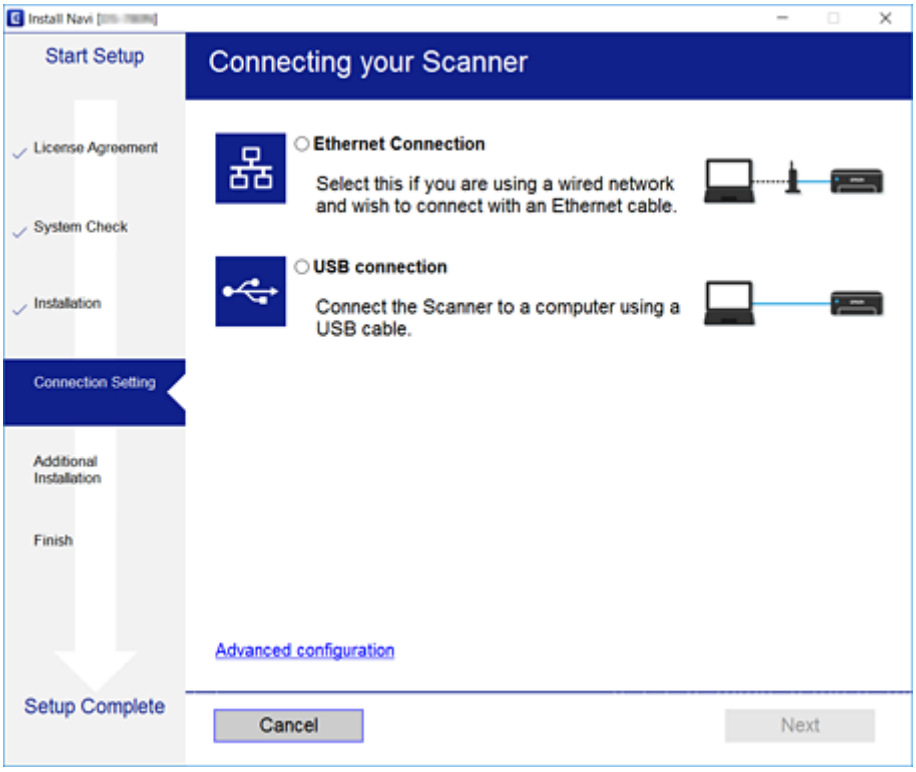
Sæt softwaredisken i computeren, og følg vejledningen på skærmen.

Valg af forbindelsesmuligheder

Følg vejledningen på skærmen, indtil følgende skærm vises, og vælg derefter metoden for tilslutning af scanneren til computeren.

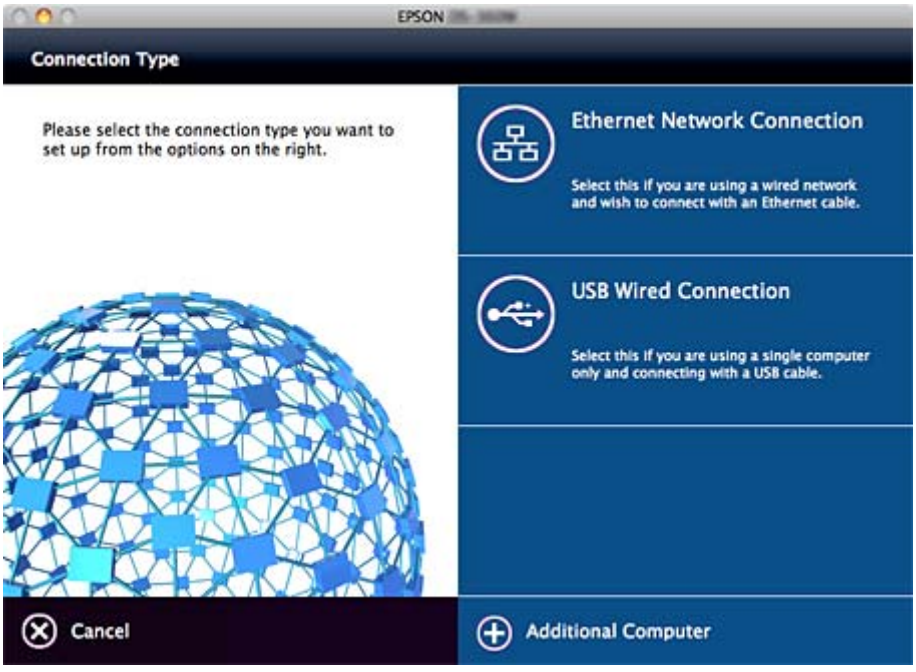
❏ Windows

Vælg forbindelsestypen, og klik på **Næste**.



❏ Mac OS

Vælg forbindelsestypen.



Tilslutning

Følg vejledningen på skærmen. Den nødvendige software er installeret.

Funktionsindstillinger

Dette kapitel forklarer de indledende indstillinger til at kunne bruge hver funktion på enheden.

Software til opsætning

I dette emne forklares proceduren for indstillinger fra administratorens computer ved hjælp af Web Config.

Web Config (enhedens hjemmeside)

Om Web Config

Web Config er et browserbaseret program til konfiguration af scannerens indstillinger.

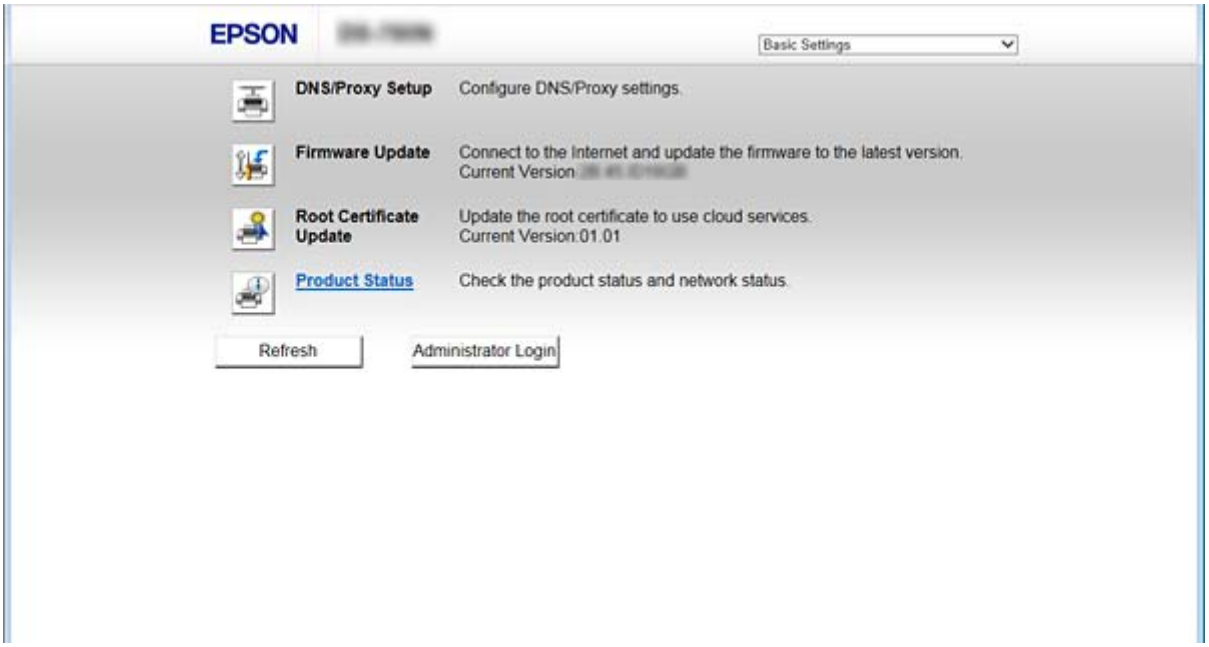
For at få adgang til Web Config, skal du først tildele en IP-adresse til scanneren.

Bemærk:
Du kan låse indstillingerne ved at konfigurere administratoradgangskoden til scanneren.

Der er to indstillingssider som vist herunder.

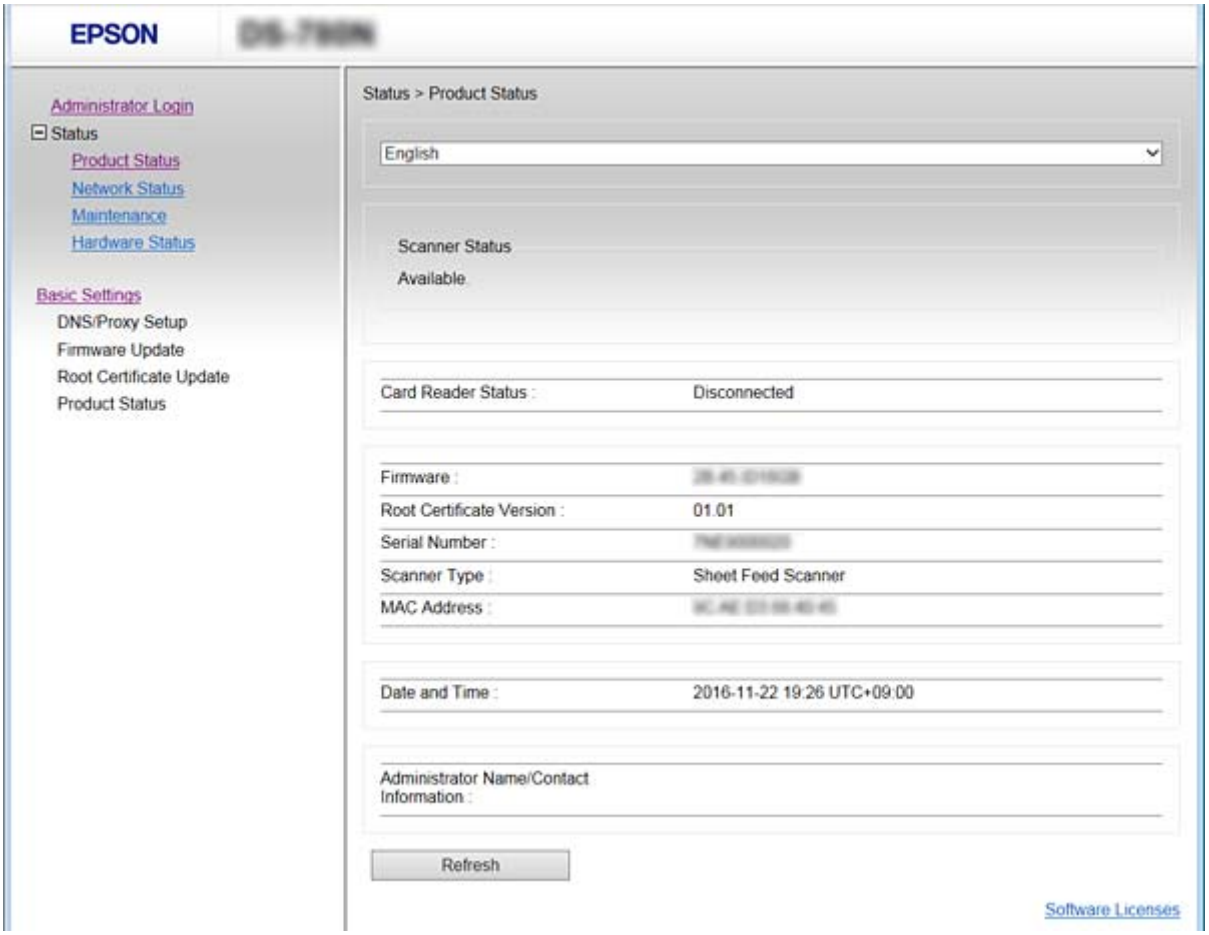
❏ **Basic Settings**

Du kan konfigurere de grundlæggende indstillinger for scanneren.



❏ **Advanced Settings**

Du kan konfigurere de avancerede indstillinger for scanneren. Denne side er primært til en administrator.



Tilgå Web Config

Indtast scannerens IP-adresse i en webbrowser. JavaScript skal være aktiveret. Når du tilgår Web Config via HTTPS, vises der en advarselsmeddelelse i browseren, da der anvendes et selvsigneret certifikat, gemt i scanneren.

❏ Tilgå via HTTPS

IPv4: https://<scannerens IP-adresse> (uden < >)

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

❏ Adgang via HTTP

IPv4: http://<scannerens IP-adresse> (uden < >)

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

Bemærk:

❏ *Eksempler*

IPv4:

https://192.0.2.111/

http://192.0.2.111/

IPv6:

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

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

❏ *Hvis scannernavnet er registreret med DNS-serveren, kan du bruge scannernavnet i stedet for scannerens IP-adresse.*

Relaterede oplysninger

➡ "SSL/TLS-kommunikation med scanneren" på side 63

➡ "Om digitalt certifikat" på side 63

Brug af scanningsfunktioner

Afhængigt af hvordan du bruger scanneren, skal du installere følgende software og foretage indstillinger, når du bruger den.

❏ **Scan fra computer**

- ❏ Bekræft gyldigheden af netværksscanningstjenesten med Web Config (gyldig ved fabriksforsendelse).
- ❏ Installer Epson Scan 2 på din computer, og indstill IP-adressen
- ❏ Ved scanning ved hjælp af job skal du installere Document Capture Pro (Document Capture) og foretage indstillinger for job.

❏ **Scan fra kontrolpanel**

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

  Installer Document Capture Pro eller Document Capture Pro Server

  DCP-indstilling (servertilstand, klienttilstand).
- ❏ Ved brug af WSD-protokollen:

  Bekræft gyldigheden af WSD på Web Config eller kontrolpanelet (gyldig ved fabriksforsendelse)

  Yderligere enhedsindstillinger (Windows-computer).

Scanning fra en computer

Installer softwaren, og kontroller, at netværksscanningstjeneste er aktiveret for at scanne via et netværk fra computeren.

Relaterede oplysninger

➡ "Software, som skal installeres" på side 25

➡ "Aktiver netværksscanning" på side 25

Software, som skal installeres

❏ Epson Scan 2

Dette er en scannerdriver. Hvis du bruger enheden fra en computer, skal du installere driveren på hver klientcomputer. Hvis Document Capture Pro/Document Capture er installeret, du kan udføre de handlinger, som er tildelt knapperne på enheden.

Med EpsonNet SetupManager kan printerdrivere også distribueres sammen i pakker.

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

Installer på klientcomputeren. Du kan ringe og udføre job, der er registreret på en computer med Document Capture Pro/Document Capture, som er installeret på netværket fra computeren og scannerens kontrolpanel.

Du kan også scanne fra computeren via netværket. Epson Scan 2 er på krævet for at scanne.

Relaterede oplysninger

➡ "EpsonNet SetupManager" på side 56

Indstil scannerens IP-adresse til Epson Scan 2

Angiv scannerens IP-adresse, så scanneren kan bruges på netværket.

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

   Hvis en anden scanner allerede er registreret, skal du gå til trin 2.

   Hvis ingen anden scanner er registreret, skal du gå til trin 4.

2. Klik på ▼ på **Scanner**.
3. Klik på **Indstillinger**.
4. Klik på **Aktivér redigering**, og klik derefter på **Tilføj**.
5. Vælg scannerens modelnavn fra **Model**.
6. Vælg scannerens IP-adresse, som skal bruges, fra **Adresse** i **Søg efter netværk**.

   Klik på  , og klik på  for at opdatere listen. Hvis du ikke kan finde IP-adressen på scanneren, skal du vælge **Angiv adresse** og indtaste IP-adressen.

7. Klik på **Tilføj**.
8. Klik på **OK**.

Aktiver netværksscanning

Du kan indstille netværksscanningstjenesten, når du scanner fra en klientcomputer via netværket. Standardindstillingen er aktiveret.

1. Gå til Web Config og vælg **Services** > **Network Scan**.

2. Sørg for, at **Enable scanning** i **EPSON Scan** er valgt.

   Hvis den er valgt, er denne opgave afsluttet. Luk Web Config.

   Hvis det er ryddet, skal du markere det og gå til næste trin.

3. Klik på **Next**.

4. Klik på **OK**.

   Netværket er forbundet igen, og indstillingerne er derefter aktiveret.

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23

Scanning vha. kontrolpanelet

Scan til mappe-funktionen og scan til mail-funktionen ved hjælp af scannerens kontrolpanel samt overførsel af scanningsresultater til mail, mapper mv. foretages ved at udføre et job fra computeren.

Når du overfører scanningsresultater, skal du opsætte job med Document Capture Pro Server eller Document Capture Pro.

For yderligere oplysninger om indstillinger og opsætning af job bedes du se dokumentation eller hjælp til Document Capture Pro Server eller Document Capture Pro.

Relaterede oplysninger

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

➡ "Indstillinger for servere og mapper" på side 27

Software til at installere på computeren

❏ **Document Capture Pro Server**

Dette er serverversionen af Document Capture Pro. Den skal installeres på en Windows-server. Flere enheder og arbejdspladser kan styres centralt af serveren. Flere job kan udføres samtidig fra flere scannere.

Ved at bruge den certificerede version af Document Capture Pro Server kan du administrere job- og scanningshistorik, som er knyttet til brugere og grupper.

For yderligere oplysninger om Document Capture Pro Server bedes du kontakte din lokale Epson-forhandler.

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

Ligesom scanning fra en computer kan du ringe til job, som er registreret på computeren fra kontrolpanelet, og udføre dem. Det er ikke muligt at køre computerjob samtidig fra flere scannere.

Document Capture Pro Server/Document Capture Pro indstillinger

Foretag indstillinger for brug af scanningsfunktionen fra scannerens kontrolpanel.

1. Gå til Web Config og vælg **Services** > **Document Capture Pro**.

2. Vælg **Betjeningsindst.**.

   ❏ Server Mode:

   Vælg dette, når du bruger Document Capture Pro Server, eller når du bruger Document Capture Pro udelukkende for job, der er indstillet til en specifik computer.

   ❏ Client Mode:

   Indstil dette, hvis du vælger jobindstillingen for Document Capture Pro (Document Capture), som er installeret på hver klientcomputer i netværket uden angivelse af computer.

3. Indstil følgende i henhold til den valgte tilstand.

   ❏ Server Mode:

   I **Server Address** skal du angive den server, hvor Document Capture Pro Server er installeret. Det kan være mellem 2 og 252 tegn i IPv4, IPv6, værtsnavn, FQDN-format. ASCII-bogstaver, tal, alfabeter og bindestreger (undtagen forreste og bageste) kan bruges i det amerikanske FQDN-format.

   ❏ Client Mode:

   Angiv **Group Settings**, som skal bruges i en scannergruppe angivet fra Document Capture Pro (Document Capture).

4. Klik på **Indstillinger**.

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23

Indstillinger for servere og mapper

Document Capture Pro og Document Capture Pro Server gemmer de scannede data til serveren eller klientcomputeren én gang og bruger overførselsfunktionen til at udføre funktionen Scan til mappe og Scan til mail.

Du skal have rettighederne og oplysningerne til at overføre fra den computer, hvor Document Capture Pro, Document Capture Pro Server er installeret på computeren eller cloud-tjenesten.

Forbered oplysninger om den funktion, du vil bruge, med henvisning til følgende.

Du kan foretage indstillinger for disse funktioner ved hjælp af Document Capture Pro eller Document Capture Pro Server. For yderligere oplysninger om indstillingerne, se dokumentationen eller hjælp til Document Capture Pro Server eller Document Capture Pro.

Navn	Indstillinger	Krav
Scan til netværksmappe (SMB)	Oprettelse og opsætning af deling af lagringsmappe	Den administrative brugerkonto til computeren, der opretter lagringsmapper.
	Destination for Scan til netværksmappe (SMB)	Brugernavn og adgangskode for at logge på den computer, der har lagringsmappe og rettigheder at opdatere lagringsmappen.
Scan til netværksmappe (FTP)	Opsætning til at logge på FTP-server	Logonoplysninger til FTP-server og rettigheder til at opdatere lagringsmappe.
Scan til e-mail	Opsætning til e-mailserver	Konfigurationsoplysninger for e-mailserver

Navn	Indstillinger	Krav
Scan til Document Castere Pro (når der bruges Document Capture Pro Server)	Opsætning til at logge på cloud-tjenester	Internetforbindelsesmiljø Registrering af konto til cloud-tjenester

Brug WSD-scanning (kun Windows)

Hvis computeren bruger Windows Vista eller nyere versioner, kan du bruge WSD-scanning.

Når WSD-protokollen kan bruges, vises menuen **Computer (WSD)** på scannerens kontrolpanel.

1. Gå til Web Config og vælg **Services** > **Protocol**.
2. Bekræft, at **Enable WSD** er markeret i **WSD Settings**.
   Hvis det er markeret, er din opgave færdig, og du kan lukke Web Config.
   Hvis det ikke er markeret, skal du kontrollere det og gå videre til næste trin.
3. Klik på knappen **Next**.
4. Bekræft indstillingerne, og klik på **Indstillinger**.

Overføre systemindstillinger

Systemindstillinger på kontrolpanelet

Indstil skærmens lysstyrke

Indstil LCD-skærmens lysstyrke.

1. Tryk på **Indstillinger** på startskærmen.
2. Tryk på **Almindelige indstil.** > **LCD-lysstyrke**.
3. Tryk på  eller  for at indstille lysstyrken.
   Du kan indstille fra 1 til 9.
4. Tryk på **OK**.

Indstil lyd

Indstil panelets betjeningslyd og fejllyde.

1. Tryk på **Indstillinger** på startskærmen.

2. Tryk på **Almindelige indstil.** > **Lyd**.
3. Indstil følgende elementer efter behov.
   - ❏ Betjeningslyd
     Indstil lydstyrken af betjeningslyden på kontrolpanelet.
   - ❏ Fejllyd
     Indstil lydstyrken af fejllyd.
4. Tryk på **OK**.

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23

Registrer dobbelt indføring af original

Angiver funktionen til at registrere dobbelt indføring af det dokument, der skal scannes, og stopper scanningen, når der sker indføring af flere dokumenter.

Hvis du vil scanne originaler, der vurderes at være dobbelt indført, f.eks. konvolutter eller papir med klistermærker, skal du deaktivere funktionen.

Bemærk:
Den kan også indstilles fra Web Config eller Epson Scan 2.

1. Tryk på **Indstillinger** på startskærmen.
2. Tryk på **Eksterne Scanningsindstillinger** > **Ultralyd-registrering af dobbeltfødning**.
3. Tryk på **Ultralyd-registrering af dobbeltfødning** for at slå det til eller fra.
4. Tryk på **Luk**.

Indstil lav hastighedstilstand

Indstil til at scanne ved lav hastighed, så der ikke opstår papirstop ved scanning af tynde dokumenter, f.eks. pamfletter.

1. Tryk på **Indstillinger** på startskærmen.
2. Tryk på **Eksterne Scanningsindstillinger** > **Langsom**.
3. Tryk på **Langsom** for at slå det til eller fra.
4. Tryk på **Luk**.

Systemindstillinger ved hjælp af Web Config

Indstillinger for strømbesparelse under inaktivitet

Foretag indstillingen for strømbesparelse for, når scanneren er uden aktivitet. Indstil tiden afhængigt af dit brugsmiljø.

Bemærk:
Du kan også foretage strømbesparende indstillingerne på scannerens kontrolpanel.

1. Gå til Web Config og vælg **System Settings** > **Power Saving**.
2. Indtast den tid, hvor **Sleep Timer** skal skifte til strømbesparelsestilstand ved inaktivitet.

   Du kan indstille op til 240 minutter ved minutinterval.
3. Vælg slukketid for **Power Off Timer**.
4. Klik på **OK**.

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23

Indstilling af kontrolpanelet

Konfiguration af scannerens kontrolpanel. Du kan konfigurere som følger.

1. Gå til Web Config og vælg **System Settings** > **Control Panel**.
2. Indstil følgende elementer efter behov.

   ❏ Language

   Vælg det viste sprog på kontrolpanelet.

   ❏ Panel Lock

   Hvis du vælger **ON**, er administratoradgangskoden påkrævet, når du udfører en handling, der kræver administratorens godkendelse. Hvis administratoradgangskoden ikke er indstillet, er panellås deaktiveret.

   ❏ Operation Timeout

   Hvis du vælger **ON**, når du logger på som administrator, bliver du automatisk logget ud og sendt til startskærmbilledet, hvis der ikke er aktivitet i en bestemt periode.

   Du kan angive mellem 10 sekunder og 240 minutter ved sekundinterval.
3. Klik på **OK**.

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23

Indstilling af begrænsning for den eksterne grænseflade

Du kan begrænse USB-forbindelsen fra computeren. Indstilles for at begrænse scanning, som sker fra andre steder end via netværket.

1. Gå til Web Config og vælg **System Settings** > **External Interface**.
2. Vælg **Enable** eller **Disable**.

   For at begrænse skal du vælge **Disable**.
3. Tryk på **OK**.

Synkronisering af dato og klokkeslæt med tidsserver

Hvis du bruger et CA-certifikat, kan du forhindre problemer med tiden.

1. Gå til Web Config, og vælg **System Settings** > **Date and Time** > **Time Server**.
2. Vælg **Use** ved punktet **Use Time Server**.
3. Indtast serveradressens tid til **Time Server Address**.

   Du kan bruge IPv4, IPv6 eller FQDN-format. Indtast op til 252 tegn. Hvis du ikke angiver dette, skal du lade det stå tomt.
4. Indtast **Update Interval (min)**.

   Du kan indstille op til 10.800 minutter ved minutinterval.
5. Klik på **OK**.

   Bemærk:
   *Du kan bekræfte forbindelsesstatussen med tidsserveren på **Time Server Status**.*

Relaterede oplysninger

➡ “Tilgå Web Config” på side 23

Grundlæggende sikkerhedsindstillinger

Dette kapitel forklarer de grundlæggende sikkerhedsindstillinger, der ikke kræver et særligt miljø.

Introduktion til grundlæggende sikkerhedsfunktioner

Vi introducerer de grundlæggende sikkerhedsfunktioner for Epson-enheder.

Funktionsnavn	Funktionstype	Hvad skal indstilles	Hvad skal forebygges
Opsætning for administratoradgangskoden	Lås indstillinger for systemet, såsom netværks- og USB-forbindelsesindstillinger, så de ikke kan ændres, undtagen af administratoren.	En administrator indstiller en adgangskode til enheden. Konfiguration eller opdatering er tilgængelig overalt fra Web Config, kontrolpanelet, Epson Device Admin og EpsonNet Config.	Undgå ulovlig læsning og ændring af oplysninger, som er gemt på enheden, såsom id, adgangskode, netværksindstillinger og kontakter. Reducer også en bred vifte af sikkerhedsrisici såsom lækage af information om netværksmiljøet eller sikkerhedspolitikken.
SSL/TLS-kommunikation	Når du får adgang til en Epson-server på internettet fra en enhed, som f.eks. kommunikation med en computer via en browser eller firmwareopdatering, er indholdet i kommunikationen krypteret med SSL/TLS-kommunikation.	Indhent et CA-signeret certifikat, og importer det derefter til scanneren.	Når du fjerner identifikation af enheden ved hjælp af CA-underskrevne certifikater, forhindres personefterligning og uautoriseret adgang. Herudover beskyttes kommunikations SSL/TLS-indhold, og lækage af indhold for udskrivnings- og installationsdata forhindres.
Kontrolprotokoller	Kontrolprotokoller bruges til kommunikation mellem enheder og computere og aktiverer/deaktiverer funktioner.	En protokol eller tjeneste, der anvendes til funktioner, som er tilladt eller forbudt separat.	Reducerer sikkerhedsrisici, der kan opstå gennem utilsigtet brug, ved at forhindre brugere i at anvende unødvendige funktioner.

Relaterede oplysninger

➡ “Om Web Config” på side 22
➡ “EpsonNet Config” på side 55
➡ “Epson Device Admin” på side 55
➡ “Konfiguration af administratoradgangskode” på side 32
➡ “Styring af protokoller” på side 35

Konfiguration af administratoradgangskode

Når du indstiller administratoradgangskoden, vil ingen andre end administratorerne kunne ændre indstillingerne for systemadministration. Du kan indstille og ændre administratoradgangskoden ved hjælp af enten Web Config,

scannerens kontrolpanel eller software (Epson Device Admin eller EpsonNet Config). Når du bruger softwaren, skal du læse dokumentationen for hver software.

Relaterede oplysninger

➡ "Konfiguration af administratoradgangskoden fra kontrolpanelet" på side 33
➡ "Konfiguration af administratoradgangskode ved hjælp af Web Config" på side 33
➡ "EpsonNet Config" på side 55
➡ "Epson Device Admin" på side 55

Konfiguration af administratoradgangskoden fra kontrolpanelet

Du kan indstille administratoradgangskoden fra scannerens kontrolpanel.

1. Tryk på **Indstillinger** på startskærmen.
2. Tryk på **Systemadministration** > **Administratorindstillinger**.

   Hvis elementet ikke vises, skal du svippe skærmen opad for at få vist elementet.
3. Tryk på **Administratoradgangskode** > **Register**.
4. Indtast den nye adgangskode, og tryk derefter på **OK**.
5. Indtast adgangskoden igen, og tryk derefter på **OK**.
6. Tryk på **OK** på bekræftelsesskærmbilledet.

   Skærmbilledet med administratorindstillinger vises.
7. Tryk på **Låseindstilling**, og tryk derefter på **OK** på bekræftelsesskærmbilledet.

   Låseindstilling er indstillet il **Til**, og administratoradgangskoden er påkrævet, når du betjener det låste menupunkt.

Bemærk:

❏ *Hvis du har indstillet **Indstillinger** > **Almindelige indstil.** > **Tiden gået for handling** > **Til**, vil scanneren logge dig ud efter en periode med inaktivitet på kontrolpanelet.*

❏ *Du kan ændre eller slette administratoradgangskoden ved at vælge **Skift** eller **Nulstil** på skærmbilledet **Administratoradgangskode** og indtaste administratoradgangskoden.*

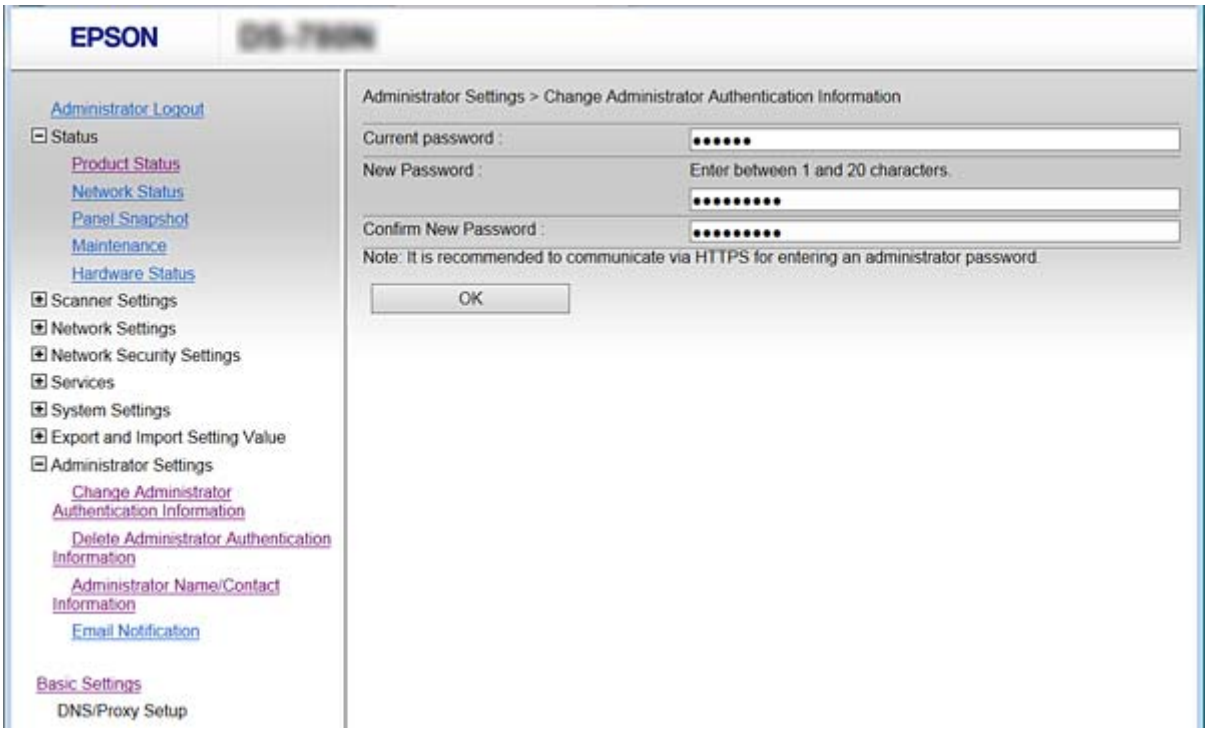
Konfiguration af administratoradgangskode ved hjælp af Web Config

Du kan indstille administratoradgangskoden ved hjælp af Web Config.

1. Gå til Web Config og vælg **Administrator Settings** > **Change Administrator Authentication Information**.

2. Indtast en adgangskode i **New Password** og **Confirm New Password**. Indtast brugernavnet, hvis det er nødvendigt.

   Hvis du vil ændre adgangskoden til en ny, skal du indtaste den nuværende adgangskode.



3. Vælg **OK**.

   Bemærk:

   ❏ *For at indstille eller ændre låste menupunkter skal du klikke på **Administrator Login** og indtaste administratoradgangskoden.*

   ❏ *For at slette administratoradgangskoden skal du klikke på **Administrator Settings** > **Delete Administrator Authentication Information** og derefter indtaste administratoradgangskoden.*

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23

Elementer, der skal låses med administratoradgangskode

Administratorer har rettigheder til at indstille og ændre alle enhedsfunktioner.

Desuden, hvis du indstiller administratoradgangskoden på enheden, kan du låse den, så du ikke kan ændre emner relateret til enhedshåndtering.

Følgende elementer kan kontrolleres af en administrator.

Element	Beskrivelse
Scannerindstillinger	Indstilling af dobbeltregistrering af indføring og lav hastighedstilstand.

Element	Beskrivelse
Indstillinger for Ethernet-forbindelse	Skift navn på enheder og IP-adresse, opsætning af DNS-server eller proxyserver, og indstil ændringer i forbindelse med netværksforbindelser.
Indstillinger for brugertjenester	Opsætning til styring af kommunikationsprotokoller, netværksscanning og Document Capture Pro-tjenester.
Indstillinger for e-mailserver	Opsætning af en e-mailserver, som enheder kommunikerer med direkte.
Sikkerhedsindstillinger	Indstillinger for netværkssikkerhed, såsom SSL/TLS-kommunikation, IPsec/IP-filtrering og IEEE802.1X.
Opdatering til rodcertifikat	En opdatering af rodcertifikat er påkrævet for Document Capture Pro Server-godkendelse og firmwareopdatering fra Web Config.
Firmwareopdatering	Kontrol og opdatering af firmwareenheder.
Tid, indstilling af timer	Overgangstid til dvale, automatisk sluk, dato/tid, timer til inaktivitet, andre indstillinger for timer.
Gendannelse til fabriksindstillinger	Indstilling til gendannelse af scanneren til fabriksindstillingerne.
Administratorindstilling	Indstilling til administratorlås eller administratoradgangskode.
Indstilling for certificeret enhed	Id-indstilling for godkendelsesenheden. Indstilling til når scanneren bruges på et godkendelsessystem, der understøtter godkendelsesenheder.

Styring af protokoller

Du kan scanne ved hjælp af forskellige stier og protokoller. Du kan også bruge netværksscanning fra et uspecificeret antal netværkscomputere. For eksempel er scanning, som kun bruger bestemte veje og protokoller, tilladt. Du kan reducere utilsigtede sikkerhedsrisici ved at begrænse scanningen til specifikke stier eller ved at styre de tilgængelige funktioner.

Konfiguration af protokolindstillingerne.

1. Gå til Web Config og vælg **Services** > **Protocol**.
2. Konfigurer hvert element.
3. Klik på **Next**.
4. Klik på **OK**.

   Indstillingerne anvendes på scanneren.

Relaterede oplysninger

➡ “Tilgå Web Config” på side 23

➡ “Protokoller, du kan aktivere eller deaktivere” på side 36

➡ “Protokolindstillingselementer” på side 37

Protokoller, du kan aktivere eller deaktivere

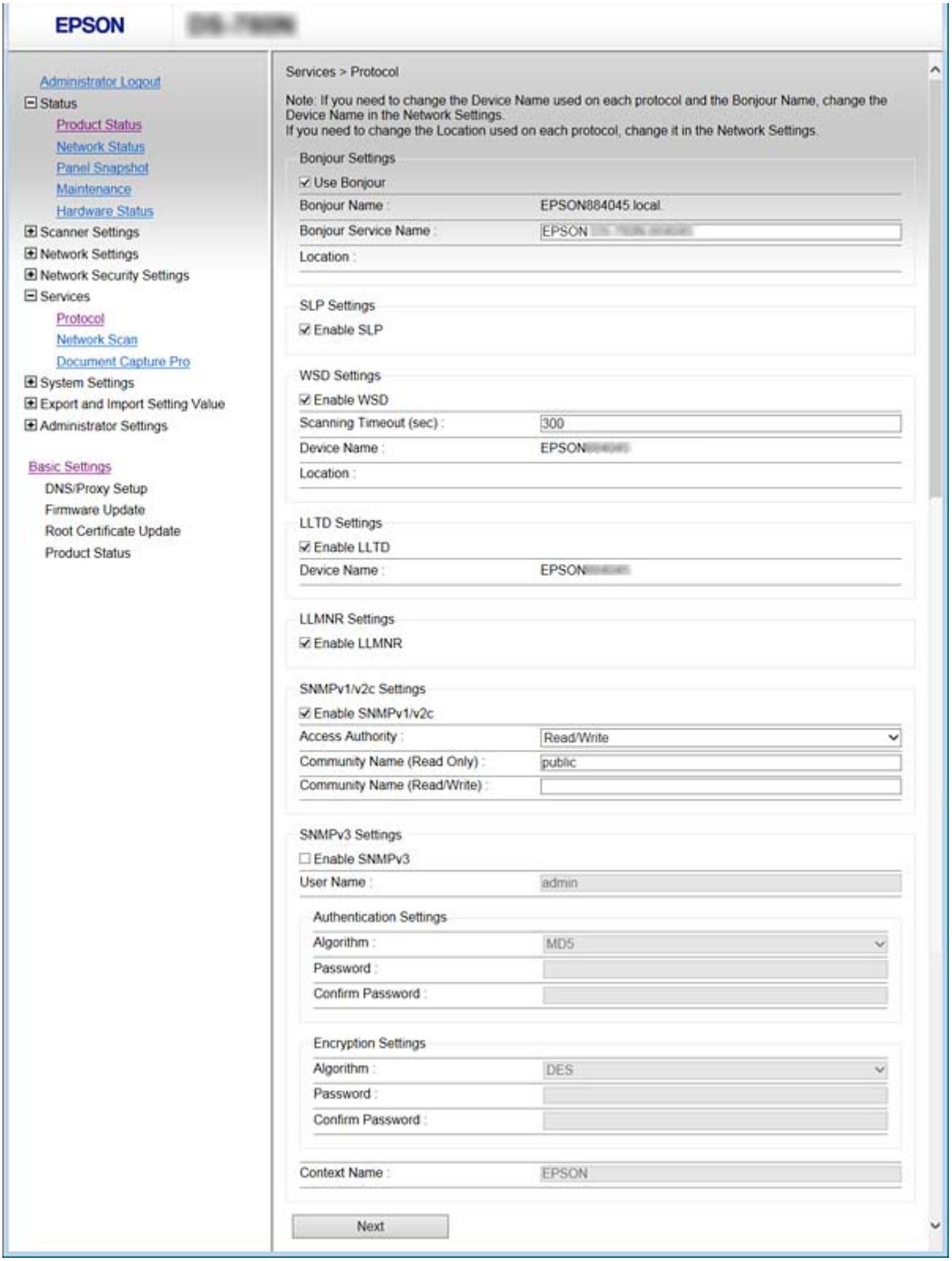
Protokol	Beskrivelse
Bonjour Settings	Du kan specificere, om du vil bruge Bonjour. Bonjour bruges til at søge efter enheder, scanne osv.
SLP Settings	Du kan aktivere eller deaktivere funktionen SLP. SLP bruges til Epson Scan 2 og netværkssøgning i EpsonNet Config.
WSD Settings	Du kan aktivere eller deaktivere WSD-funktionen. Når den er aktiveret, kan du tilføje WSD-enheder eller scanne fra WSD-porten.
LLTD Settings	Du kan aktivere eller deaktivere funktionen LLTD. Når den er aktiveret, vises den på Windows netværkskort.
LLMNR Settings	Du kan aktivere eller deaktivere funktionen LLMNR. Når den er aktiveret, kan du bruge navneoversættelse uden NetBIOS, også selv om du ikke kan bruge DNS.
SNMPv1/v2c Settings	Du kan specificere, om du vil aktivere SNMPv1/v2c. Dette bruges til at opsætte enheder monitorere osv.
SNMPv3 Settings	Du kan specificere, om du vil aktivere SNMPv3. Dette bruges til at oprette krypterede enheder, overvågning osv.

Relaterede oplysninger

➡ “Styring af protokoller” på side 35

➡ “Protokolindstillingselementer” på side 37

Protokolindstillingselementer



Punkter	Indstillingsværdi og beskrivelse
Bonjour Settings	

Grundlæggende sikkerhedsindstillinger

Punkter	Indstillingsværdi og beskrivelse
Use Bonjour	Vælg denne funktion til at søge efter eller bruge enheder via Bonjour.
Bonjour Name	Viser navnet Bonjour.
Bonjour Service Name	Du kan få vist og indstille navnet for Bonjour-tjenesten.
Location	Viser Bonjour-placeringsnavnet.
SLP Settings	
Enable SLP	Vælg denne for at aktivere funktionen SLP. Det bruges til at finde netværk i Epson Scan 2 og EpsonNet Config.
WSD Settings	
Enable WSD	Vælg denne for at aktivere tilføjelse af enheder med WSD og for at kunne udskrive og scanne fra WSD-porten.
Scanning Timeout (sec)	Indtast timeout-værdien for kommunikation for WSD scanning. Skal være mellem 3 til 3.600 sekunder.
Device Name	Viser WSD enhedsnavnet.
Location	Viser WSD-placeringsnavnet.
LLTD Settings	
Enable LLTD	Vælg denne for at aktivere LLTD. Scanneren vises i Windows netværkskort.
Device Name	Viser LLTD enhedsnavnet.
LLMNR Settings	
Enable LLMNR	Vælg denne for at aktivere LLMNR. Du kan bruge navneoversættelse uden NetBIOS, også selv om du ikke kan bruge DNS.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	Vælg for at aktivere SNMPv1/v2c. Der vises kun scannere, der understøtter SNMPv3.
Access Authority	Indstil godkendelse af afgang, når SNMPv1/v2c er aktiveret. Vælg **Read Only** eller **Read/Write**.
Community Name (Read Only)	Indtast 0 til 32 ASCII (0x20 til 0x7E) tegn.
Community Name (Read/Write)	Indtast 0 til 32 ASCII (0x20 til 0x7E) tegn.
SNMPv3 Settings	
Enable SNMPv3	SNMPv3 er aktiveret, når feltet er markeret.
User Name	Indtast mellem 1 og 32 tegn ved hjælp af 1 byte-tegn.
Authentication Settings	
Algorithm	Vælg en godkendelsesalgoritme til SNMPv3.

Grundlæggende sikkerhedsindstillinger

Punkter	Indstillingsværdi og beskrivelse
Password	Indtast adgangskoden til godkendelse for SNMPv3. Indtast mellem 8 og 32 tegn i ASCII (0x20–0x7E). Hvis du ikke angiver dette, skal du lade det stå tomt.
Confirm Password	Indtast den konfigurerede adgangskode for at bekræfte.
Encryption Settings	
Algorithm	Vælg en algoritme for kryptering for SNMPv3.
Password	Indtast adgangskoden til kryptering for SNMPv3. Indtast mellem 8 og 32 tegn i ASCII (0x20–0x7E). Hvis du ikke angiver dette, skal du lade det stå tomt.
Confirm Password	Indtast den konfigurerede adgangskode for at bekræfte.
Context Name	Indtast op til 32 tegn i Unicode (UTF-8). Hvis du ikke angiver dette, skal du lade det stå tomt. Antallet af tegn, der kan indtastes, varierer afhængigt af sproget.

Relaterede oplysninger

➡ “Styring af protokoller” på side 35
➡ “Protokoller, du kan aktivere eller deaktivere” på side 36

Indstillinger for betjening og administration

Dette kapitel forklarer de elementer, som er relateret til den daglige betjening og administration af enheden.

Bekræft oplysninger for en enhed

Du kan kontrollere følgende oplysninger på den aktive enhed fra **Status** ved hjælp af Web Config.

❏ Product Status

Kontroller sprog, status, produktnummer, MAC-adresse osv.

❏ Network Status

Kontroller oplysninger om status for netværksforbindelsen, IP-adresse, DNS-server osv.

❏ Panel Snapshot

Få vist et øjebliksbillede af det skærmbillede, der vises på enhedens kontrolpanel.

❏ Maintenance

Kontroller startdato, scanningsoplysninger osv.

❏ Hardware Status

Kontroller status for scanneren.

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23

Administration af enheder (Epson Device Admin)

Du kan administrere og betjene mange enheder ved hjælp af Epson Device Admin. Epson Device Admin giver dig mulighed for at styre enheder, som er placeret på et andet netværk. Følgende beskriver de vigtigste funktioner til administration.

For mere information om funktioner og brug af softwaren skal du se dokumentationen og hjælp til Epson Device Admin.

❏ Opdagelse af enheder

Du kan opdage enheder på netværket og derefter registrere dem til en liste. Hvis Epson-enheder såsom printere og scannere er tilsluttet det samme netværkssegment som administratorens computer, kan du finde dem, selv om de ikke er blevet tildelt en IP-adresse.

Du kan også opdage enheder, der er tilsluttet computere på netværket med USB-kabler. Du skal installere Epson Device USB Agent på computeren.

❏ Indstilling af enheder

Du kan lave en skabelon, der indeholder indstillingselementer såsom netværkskort og papirkilde, og anvende den til andre enheder som delte indstillinger. Når den er tilsluttet netværket, kan du tildele en IP-adresse til en enhed, der ikke er tildelt en IP-adresse.

❏ Overvågning af enheder

Du kan løbende hente status for og detaljerede oplysninger om enheder på netværket. Du kan også overvåge enheder, der er tilsluttet computere på netværket med USB-kabler, og enheder fra andre virksomheder, der er registreret til enhedslisten. For at overvåge enheder, som er forbundet med USB-kabler, skal du installere Epson Device USB Agent.

❏ Administration af alarmer

Du kan overvåge alarmer om status for enheder og forbrugsmaterialer. Systemet sender automatisk e-mails til administratoren baseret på fastsatte betingelser.

❏ Administration af rapporter

Du kan oprette regelmæssige rapporter, efterhånden som systemet akkumulerer data om forbrug og forbrugsmaterialer. Du kan derefter gemme disse oprettede rapporter og sende dem via e-mail.

Relaterede oplysninger

➡ "Epson Device Admin" på side 55

Modtagelse af meddelelser med e-mail, når hændelser opstår

Om e-mail-meddelelser

Du kan bruge denne funktion til at modtage advarsler via e-mail, når der opstår hændelser. Du kan registrere op til 5 e-mailadresser og vælge, hvilke begivenheder du ønsker at modtage meddelelser for.

Mailserveren skal være konfigureret til at bruge denne funktion.

Relaterede oplysninger

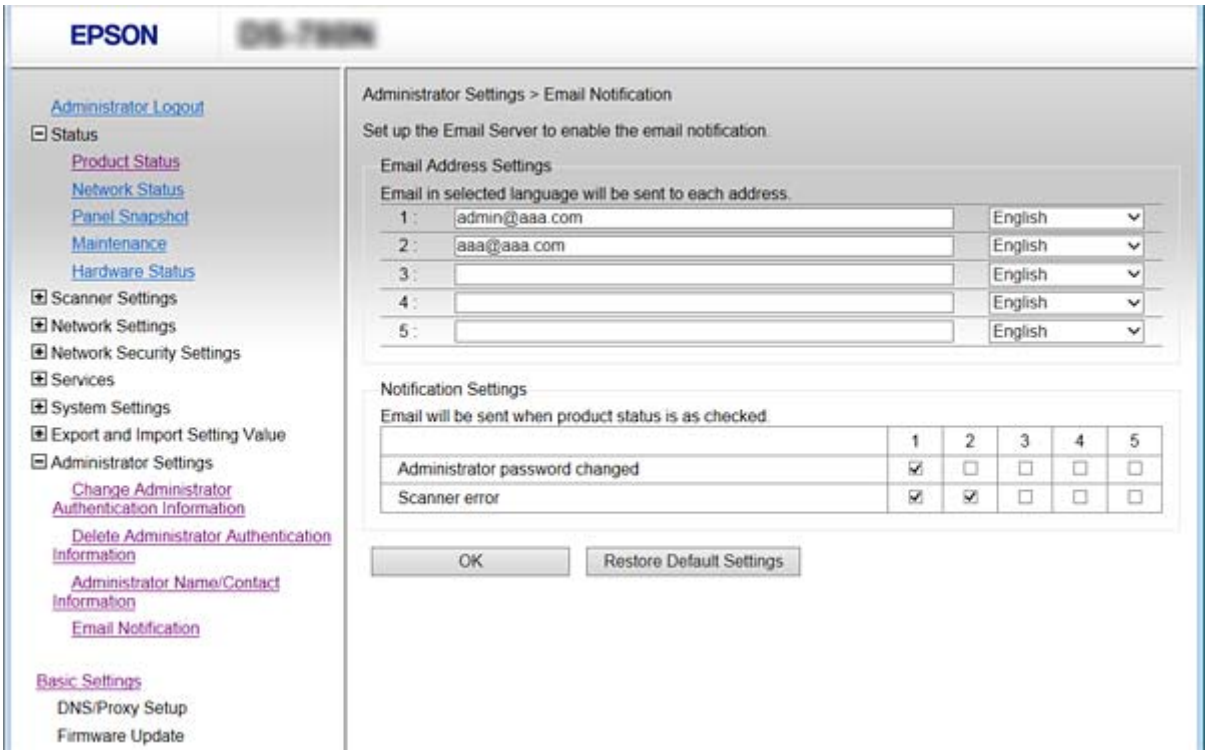
➡ "Konfiguration af en mailserver" på side 42

Konfigurere email-meddelelser

For at bruge funktionen, skal du konfigurere en mailserver.

1. Gå til Web Config og vælg **Administrator Settings** > **Email Notification**.
2. Indtast en emailadresse, som du ønsker skal modtage email-meddelelser.
3. Vælg sproget til e-mail-meddelelserne.

4. Marker felterne for de meddelelser, du ønsker at modtage.



5. Klik på **OK**.

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23
➡ "Konfiguration af en mailserver" på side 42

Konfiguration af en mailserver

Kontroller følgende inden konfiguration.

❏ Scanneren har forbindelse til et netværk.

❏ Oplysningerne om computerens e-mailserver.

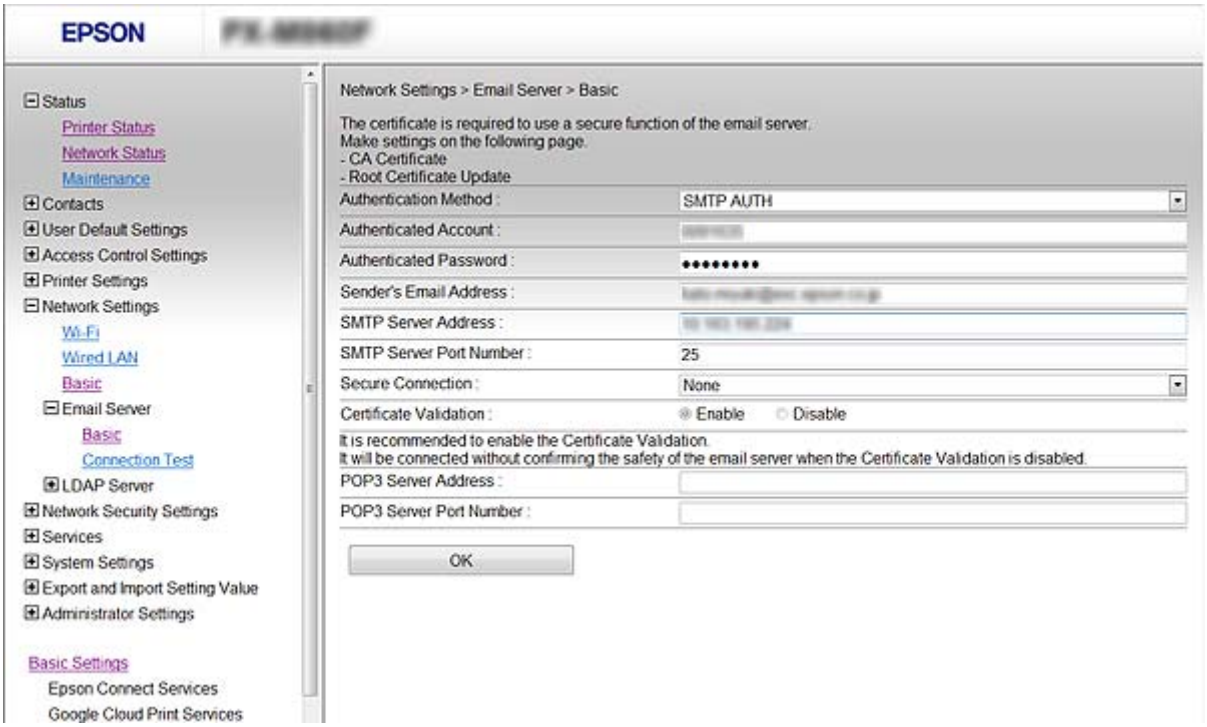
1. Gå til Web Config og vælg **Network Settings** > **Email Server** > **Basic**.
2. Indtast en værdi for hvert element.
3. Vælg **OK**.

   De indstillinger, du har valgt, vises.

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23
➡ "Indstillingselementer for mailserver" på side 43

Indstillingselementer for mailserver



Elementer	Indstillinger og forklaring	
Authentication Method	Angiv godkendelsesmetoden, for at scanneren kan få adgang til mailserveren.	
	Off	Godkendelse er deaktiveret, når der kommunikeres med en mailserver.
	SMTP AUTH	Kræver, at en mailserver understøtter SMTP-godkendelse.
	POP before SMTP	Konfigurer POP3-serveren, når du vælger denne metode.
Authenticated Account	Hvis du vælger **SMTP AUTH** eller **POP before SMTP** som **Authentication Method**, skal du indtaste det godkendte kontonavn på mellem 0 og 255 tegn i ASCII (0x20–0x7E).	
Authenticated Password	Hvis du vælger **SMTP AUTH** eller **POP before SMTP** som **Authentication Method**, skal du indtaste det godkendte kontonavn på mellem 0 og 20 tegn bestående af A–Z a–z 0–9! # $ % & ' * + - . / = ? ^ _ { | } ~ @.	
Sender's Email Address	Indtast afsenderens emailadresse. Indtast mellem 0 og 255 tegn i ASCII (0x20–0x7E) med undtagelse af : ( ) < > [ ] ; ¥. Et punktum "." ikke kan være det første tegn.	
SMTP Server Address	Indtast mellem 0 og 255 tegn bestående af A–Z a–z 0–9. - . Du kan bruge IPv4- eller FQDN-format.	
SMTP Server Port Number	Indtast et tal mellem 1 og 65535.	

Elementer	Indstillinger og forklaring	
Secure Connection	Specificer den sikre forbindelsesmetode for e-mailserveren.	
	None	Hvis du vælger **POP before SMTP** i **Authentication Method**, indstilles forbindelsesmetoden til **None**.
	SSL/TLS	Den er tilgængelig når **Authentication Method** er indstillet til **Off** eller **SMTP AUTH**.
	STARTTLS	Den er tilgængelig når **Authentication Method** er indstillet til **Off** eller **SMTP AUTH**.
Certificate Validation	Certifikatet valideres når det aktiveres. Vi anbefaler, at det indstilles til **Enable**.	
POP3 Server Address	Hvis du vælger **POP before SMTP** som **Authentication Method**, skal du indtaste POP3-serveradressen mellem 0 og 255 tegn bestående af A–Z a–z 0–9. - . Du kan bruge IPv4- eller FQDN-format.	
POP3 Server Port Number	Hvis du vælger **POP before SMTP** som **Authentication Method**, skal du indtaste et tal mellem 1 og 65535.	

Relaterede oplysninger

➡ "Konfiguration af en mailserver" på side 42

Kontrol af en mailserverforbindelse

1. Gå til Web Config og vælg **Network Settings** > **Email Server** > **Connection Test**.
2. Vælg **Start**.

   Forbindelsestesten til e-mailserveren startes. Kontrolrapporten vises efter testen.

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23
➡ "Testreferencer for mailserverforbindelse" på side 44

Testreferencer for mailserverforbindelse

Meddelelser	Forklaring
Connection test was successful.	Denne meddelelse vises, når forbindelsen til serveren er oprettet.
SMTP server communication error. Check the following. - Network Settings	Denne meddelelse vises, når ❏ Scanneren har ikke forbindelse til et netværk ❏ SMTP serveren er nede ❏ Netværksforbindelsen afbrydes under kommunikation ❏ Der modtages ufuldstændige data

Indstillinger for betjening og administration

Meddelelser	Forklaring
POP3 server communication error. Check the following. - Network Settings	Denne meddelelse vises, når ❏ Scanneren har ikke forbindelse til et netværk ❏ POP3 serveren er nede ❏ Netværksforbindelsen afbrydes under kommunikation ❏ Der modtages ufuldstændige data
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Denne meddelelse vises, når ❏ Oprettelse af forbindelse til en DNS server mislykkedes ❏ Navneoversættelse for en SMTP server mislykkedes
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Denne meddelelse vises, når ❏ Oprettelse af forbindelse til en DNS server mislykkedes ❏ Navneoversættelse for en POP3 server mislykkedes
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Denne meddelelse vises, når godkendelse af SMTP serveren mislykkedes.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Denne meddelelse vises, når godkendelse af POP3 serveren mislykkedes.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Denne meddelelse vises, når du forsøger at kommunikere med ikke-understøttede protokoller.
Connection to SMTP server failed. Change Secure Connection to None.	Denne meddelelse vises, når der opstår en SMTP uoverensstemmelse mellem en server og en klient, eller når serveren ikke understøtter SMTP sikker forbindelse (SSL-forbindelse).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Denne meddelelse vises, når der opstår en SMTP uoverensstemmelse mellem en server og en klient, eller når serveren anmoder om at bruge en SSL/TLS forbindelse til en SMTP sikker forbindelse.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Denne meddelelse vises, når der opstår en SMTP uoverensstemmelse mellem en server og en klient, eller når serveren anmoder om at bruge en STARTTLS forbindelse til en SMTP sikker forbindelse.
The connection is untrusted. Check the following. - Date and Time	Denne meddelelse vises, når scannerens indstilling for dato og tid er forkert eller hvis certifikatet er udløbet.
The connection is untrusted. Check the following. - CA Certificate	Denne meddelelse vises, når scanneren ikke har et rodcertifikat, der svarer til serveren, eller der ikke er importeret et CA Certificate.
The connection is not secured.	Denne meddelelse vises, når det hentede certifikat er beskadiget.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Denne meddelelse vises, når der opstår en uoverensstemmelse i en godkendelsesmetode mellem en server og en klient. Serveren understøtter SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Denne meddelelse vises, når der opstår en uoverensstemmelse i en godkendelsesmetode mellem en server og en klient. Serveren understøtter ikke SMTP AUTH.

Meddelelser	Forklaring
Sender's Email Address is incorrect. Change to the email address for your email service.	Denne meddelelse vises, når den specificerede senders e-mailadresse er forkert.
Cannot access the product until processing is complete.	Denne meddelelse vises, når scanneren er optaget.

Relaterede oplysninger

➡ "Kontrol af en mailserverforbindelse" på side 44

Opdatering af firmware

Opdatering af firmware ved hjælp af Web Config

Opdater firmware ved hjælp af Web Config. Enheden skal være tilsluttet internettet.

1. Gå til Web Config og vælg **Basic Settings** > **Firmware Update**.
2. Klik på **Start**.

   Bekræftelsen af firmwaren starter, og firmwarens oplysninger vises, hvis den opdaterede firmware eksisterer.
3. Klik på **Start**, og følg vejledningen på skærmen.

Bemærk:
Du kan også opdatere firmwaren ved hjælp af Epson Device Admin. Du kan bekræfte firmwareoplysningerne visuelt på enhedslisten. Det er nyttigt, når du vil opdatere flere enheders firmware. Se i vejledningen eller hjælpen til Epson Device Admin for at få flere oplysninger.

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23
➡ "Epson Device Admin" på side 55

Opdatering af firmware ved hjælp af Epson Firmware Updater

Du kan downloade enhedens firmware fra Epsons hjemmeside til computeren og derefter tilslutte enheden og computeren med et USB-kabel for at opdatere firmwaren. Hvis du ikke kan opdatere via netværket, kan du prøve denne metode.

1. Gå til Epsons hjemmeside, og download firmwaren.
2. Tilslut den computer, der indeholder den downloadede firmware, til enheden via USB-kabel.
3. Dobbeltklik på den downloadede .exe-fil.

   Epson Firmware Updater starter.
4. Følg vejledningen på skærmen.

Sikkerhedskopiering af indstillingerne

Ved at eksportere indstillingsemnerne på Web Config kan du kopiere elementerne til de andre scannere.

Eksport af indstillingerne

Eksportér hver indstilling for scanneren.

1. Tilgå Web Config, og vælg derefter **Export and Import Setting Value** > **Export**.
2. Vælg indstillingerne, som du vil eksportere.

   Vælg indstillingerne, du vil eksportere. Hvis du vælger den overordnede kategori vælges underkategorierne også. Underkategorier, der kan medføre fejl ved at blive duplikeret inden i det samme netværk (som f.eks. IP-adresser osv.), kan ikke vælges.
3. Indtast en adgangskode for at kryptere eksportfilen.

   Du skal bruge adgangskoden til at importere filen. Lad feltet være tomt hvis du ikke vil kryptere filen.
4. Klik på **Export**.

> ***Vigtigt:***
>
> *Hvis du vil eksportere scannerens netværksindstillinger som f.eks. scannernavn og IP-adresse skal du vælge* ***Enable to select the individual settings of device*** *og vælge yderligere elementer. Brug kun de valgte værdier til erstatningsscanneren.*

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23

Import af indstillingerne

Import den eksporterede Web Config fil til scanneren.

> ***Vigtigt:***
>
> *Når du importerer værdier, der inkluderer individuelle oplysninger som f.eks. scannernavn eller IP-adresse skal du sørge for, at den samme IP-adresse ikke findes allerede på det samme netværk. Hvis IP-adressen overlapper, reflekterer scanneren ikke værdien.*

1. Tilgå Web Config, og vælg derefter **Export and Import Setting Value** > **Import**.
2. Væld den eksporterede fil og indtast adgangskoden for krypteringen.
3. Klik på **Next**.
4. Vælg den indstilling, du vil importere, og klik derefter på **Next**.
5. Klik på **OK**.

Indstillingerne anvendes på scanneren.

Indstillinger for betjening og administration

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23

Problemløsning

Tip til problemløsning

Du kan finde flere oplysninger i følgende manual.

❏ Brugervejledning

Indeholder vejledning til brug af scanneren, vedligeholdelse samt problemløsning.

Kontrol af log for server og netværksenhed

I tilfælde af problemer med netværksforbindelsen kan årsagen muligvis identificeres ved at bekræfte aflogning af mailserver, LDAP-server, osv. og kontrollere status ved hjælp af netværkslog for systemets udstyrslogge og kommandoer, såsom routere.

Initialisering af netværksindstillingerne

Gendannelse af netværksindstillingerne fra kontrolpanelet

Du kan gendanne alle netværksindstillinger til deres standardindstillinger.

1. Tryk på **Indstillinger** på startskærmen.
2. Tryk på **Systemadministration** > **Gendan standardindstillinger** > **Netværksindstillinger**.
3. Læs meddelelsen, og tryk derefter på **Ja**.
4. Når der vises en fuldført-meddelelse, skal du trykke på **Luk**.

   Skærmen slukker automatisk efter en angiven tid, hvis du ikke trykker på **Luk**.

Kontrol af kommunikation mellem enheder og computere

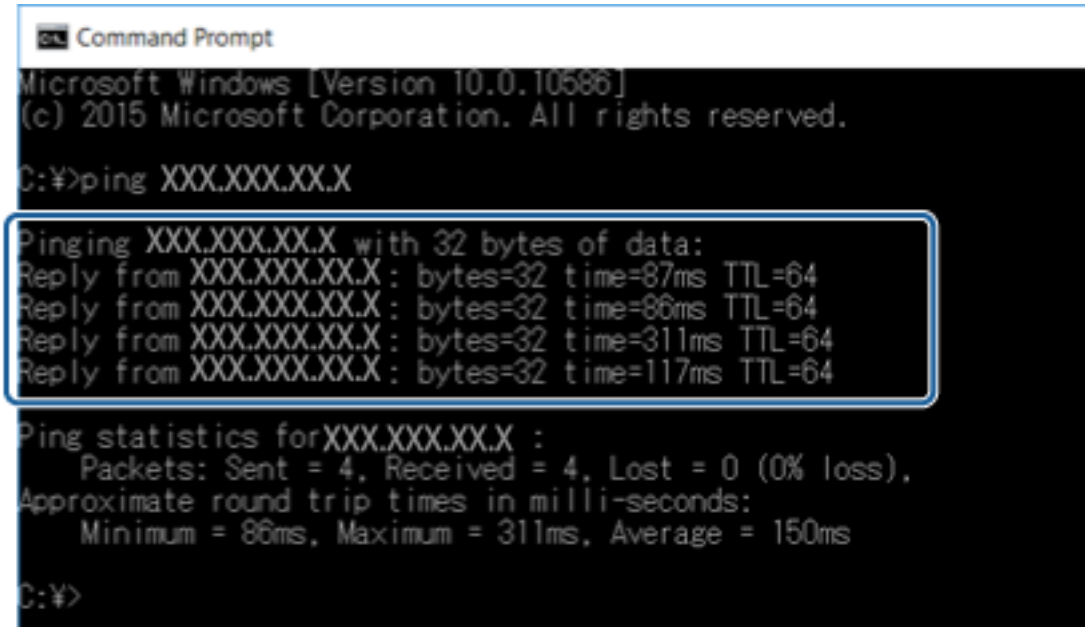
Kontrol af forbindelse vha. en ping-kommando — Windows

Du kan bruge en Ping-kommando for at sikre, at computeren er sluttet til scanneren. Følg nedenstående trin for at kontrollere forbindelsen ved hjælp af en Ping-kommando.

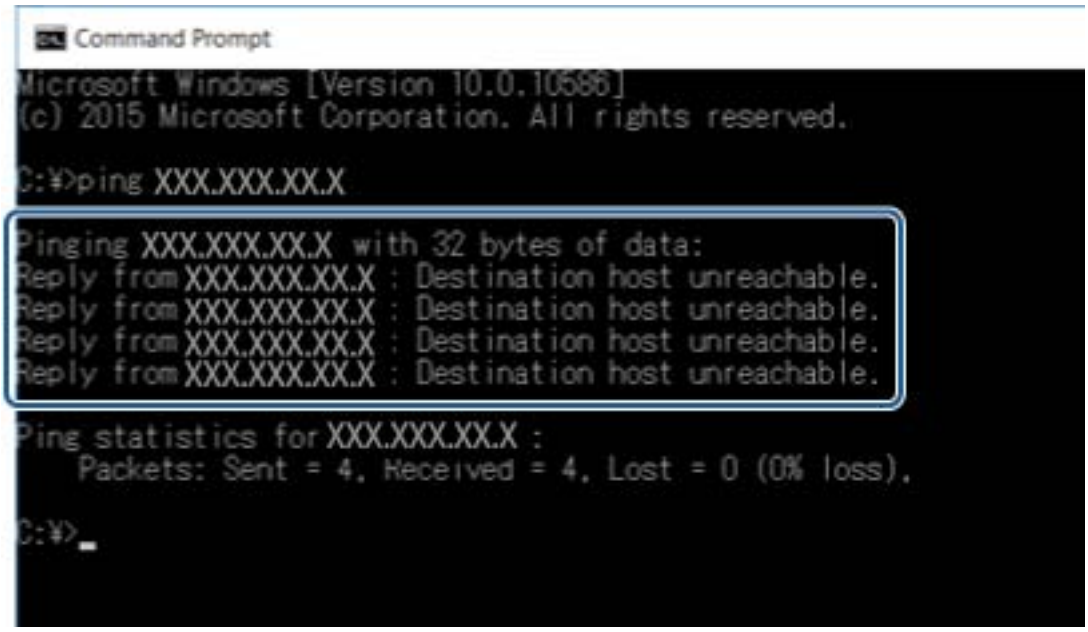
1. Kontrollér scannerens IP-adresse for den forbindelse, du vil kontrollere.

   Du kan kontrollere dette ved hjælp af Epson Scan 2.

2. Åbn computerens kommandopromptskærm.
   - ❏ Windows 10
     Højreklik på start-knappen, eller tryk på og hold den nede, og vælg derefter **Kommandoprompt**.
   - ❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
     Åbn programskærmen, og vælg derefter **Kommandoprompt**.
   - ❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 eller tidligere
     Klik på startknappen, vælg **Alle programmer** eller **Programmer** > **Tilbehør** > **Kommandoprompt**.
3. Indtast "ping xxx.xxx.xxx.xxx", og tryk derefter på tasten Enter.
   Indtast scannerens IP-adresse i stedet for xxx.xxx.xxx.xxx.
4. Kontrollér kommunikationsstatus.
   Folgende meddelelse vises, hvis scanneren og computeren kommunikerer.



Folgende meddelelse vises, hvis scanneren og computeren ikke kommunikerer.



Kontrol af forbindelse vha. en ping-kommando — Mac OS

Du kan bruge en Ping-kommando for at sikre, at computeren er sluttet til scanneren. Følg nedenstående trin for at kontrollere forbindelsen ved hjælp af en Ping-kommando.

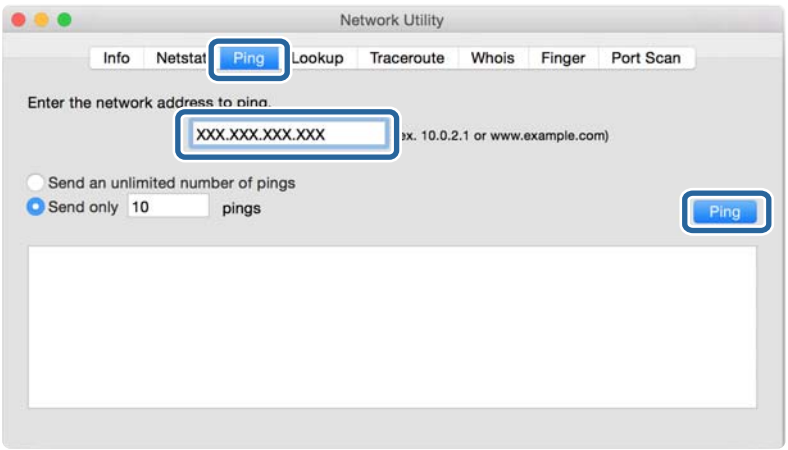
1. Kontrollér scannerens IP-adresse for den forbindelse, du vil kontrollere.

   Du kan kontrollere dette ved hjælp af Epson Scan 2.

2. Kør Network Utility.

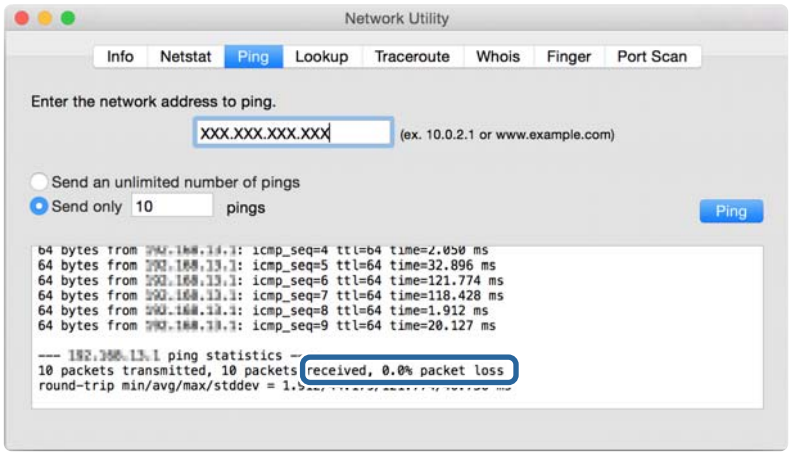
   Skift til "Network Utility" i **Spotlight**.

3. Klik på fanen **Ping**, indtast den IP-adresse, du kontrollerede i trin 1, og klik derefter på **Ping**.

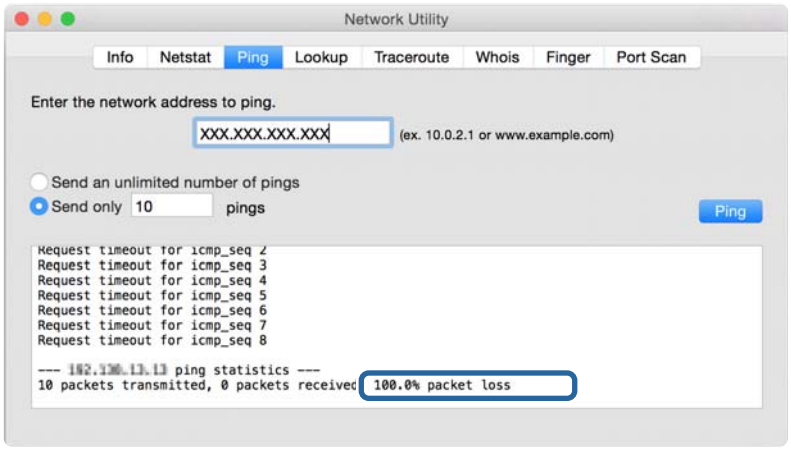


4. Kontroller kommunikationsstatus.

   Følgende meddelelse vises, hvis scanneren og computeren kommunikerer.



   Følgende meddelelse vises, hvis scanneren og computeren ikke kommunikerer.



Problemer med brug af netværkssoftwaren

Kan ikke få adgang til Web Config

Er scannerens IP-adresse konfigureret korrekt?

Konfiguration af IP-adressen ved hjælp af Epson Device Admin eller EpsonNet Config.

Understøtter din browser bulk-krypteringer for Encryption Strength til SSL/TLS?

Bulk-krypteringerne for Encryption Strength til SSL/TLS er som følger. Web Config kan kun tilgås i en browser, der understøtter følgende bulk-krypteringer. Kontroller den kryptering, din browser understøtter.

❏ 80 bit: AES256/AES128/3DES

❏ 112 bit: AES256/AES128/3DES

❏ 128 bit: AES256/AES128

❏ 192 bit: AES256

❏ 256 bit: AES256

Meddelelsen "Forældet" vises, når Web Config tilgås vha. SSL-kommunikation (https).

Hent certifikatet igen, hvis det er forældet. Hvis meddelelsen vises før udløbsdatoen, skal du kontrollere, at scannerens dato er konfigureret korrekt.

Meddelelsen "Navnet på sikkerhedscertifikatet stemmer ikke overens med…" vises, når Web Config tilgås vha. SSL-kommunikation (https).

Scannerens IP-adresse, der er indtastet for **Common Name** til oprettelse af et selvsigneret certifikat eller en CSR, stemmer ikke overens med den adresse, der er indtastet i browseren. Hent og importer et certifikat igen, eller skift scannernavnet.

Scanneren tilgås via en proxyserver.

Hvis du bruger en proxyserver til din scanner, skal du konfigurere din browsers proxyindstillinger.

❏ Windows:

Vælg **Kontrolpanel** > **Netværk og internet** > **Internetindstillinger** > **Forbindelse** > **LAN-indstillinger** > **Proxyserver**, og konfigurer derefter ikke at bruge proxyserveren til lokale adresser.

❏ Mac OS:

Vælg **Systemindstillinger** > **Netværk** > **Avanceret** > **Proxyservere**, og registrer derefter den lokale adresse for **Ohita näiden palvelimien ja domainien välipalvelinasetukset**.

Eksempel:

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

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

Relaterede oplysninger

➡ “Tilgå Web Config” på side 23

➡ “Tildeling af IP-adressen” på side 15

➡ “Tildeling af en IP-adressen ved hjælp af EpsonNet Config” på side 56

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

Valgte du Bloker, Annuller eller Luk da en Windows-sikkerhedsskærm eller en firewall-skærm blev vist?

Hvis du vælger **Bloker**, **Annuller**, eller **Luk**, vises IP-adressen og modelnavnet ikke på EpsonNet Config eller EpsonNet Setup.

For at korrigere dette skal du registrere EpsonNet Config som en undtagelse vha. Windows firewall og kommerciel sikkerhedssoftware. Hvis du bruger et antivirus- eller sikkerhedsprogram, skal du lukke det, når du forsøger at bruge EpsonNet Config.

Er timeout-indstillingen for kommunikationsfejl indstillet for kort?

Kør EpsonNet Config, og vælg **Tools** > **Options** > **Timeout**; forøg derefter tiden for indstillingen **Communication Error**. Bemærk, at dette kan få EpsonNet Config til at arbejde langsommere.

Relaterede oplysninger

➡ "Kørsel af EpsonNet Config — Windows" på side 56

➡ "Kørsel af EpsonNet Config — Mac OS" på side 56

Appendiks

Introduktion til netværkssoftware

I det følgende beskrives den software, der konfigurerer og administrerer enheder.

Epson Device Admin

Epson Device Admin er et program, der tillader dig at installere enheder på netværket, og derefter konfigurere og administrere enhederne. Du kan indhente detaljerede oplysninger om enheder, såsom status og forbrugsmaterialer, sende meddelelser om advarsler og oprette rapporter for enhedsbrug. Du kan også lave en skabelon, der indeholder indstillingsemner og anvende den til andre enheder som delte indstillinger. Du kan downloade Epson Device Admin fra Epson support-webstedet. Se dokumentationen eller hjælpen i Epson Device Admin for at få flere oplysninger.

Kørsel af Epson Device Admin (kun Windows)

Vælg **Alle programmer** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**.

Bemærk:
Tillad adgang for Epson Device Admin, hvis firewall-alarmen vises.

EpsonNet Config

Med EpsonNet Config kan administratoren konfigurere scannerens netværksindstillinger, f.eks. tildele en IP-adresse og ændre tilslutningstilstand. Batchindstillingsfunktionen understøttes af Windows. Se dokumentationen eller hjælpen i EpsonNet Config for at få flere oplysninger.

Kørsel af EpsonNet Config — Windows

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

Bemærk:
Tillad adgang for EpsonNet Config, hvis firewall-alarmen vises.

Kørsel af EpsonNet Config — Mac OS

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

EpsonNet SetupManager

EpsonNet SetupManager er en software til oprettelse af en pakke til en enkel scannerinstallation, som f.eks. at installere og konfigurere scannerdriveren, og installation af Document Capture Pro. Med denne software kan administratoren oprette unikke softwarepakker og distribuere dem blandt grupper.

For mere information, besøg dit regionale Epson websted.

Tildeling af en IP-adressen ved hjælp af EpsonNet Config

Du kan tildele en IP-adresse til scanneren ved hjælp af EpsonNet Config. EpsonNet Config giver mulighed for at tildele en IP-adresse til en scanner, der ikke er blevet tildelt en efter tilslutning med et Ethernet-kabel.

Tildeling af IP-adresse ved hjælp af batchindstillinger

Oprettelse af fil til batchindstillinger

Ved at bruge MAC-adresse og modelnavn som nøgler, kan du oprette en ny SYLK-fil til at indstille IP-adressen.

1. Åbn et regneark (f.eks. Microsoft Excel) eller en teksteditor.

2. Indtast "Info_MACAddress", "Info_ModelName" og "TCPIP_IPAddress" i første række som navne for indstillingselementer.

   Indtast indstillingsemner for de følgende tekststrenge. For at skelne mellem store/små bogstaver og dobbelt-byte/enkelt-byte tegn vil elementet ikke blive genkendt, hvis bare et tegn er forskelligt.

   Indtast navnet på indstillingselementet som beskrevet nedenfor; ellers kan EpsonNet Config ikke genkende indstillingselementet.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. Indtast MAC-adresse, modelnavn og IP-adresse for hvert netværksgrænseflade.

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. Indtast et navn, og gem som en SYLK-fil (*.slk).

Foretage batchindstillinger ved hjælp af en konfigurationsfil

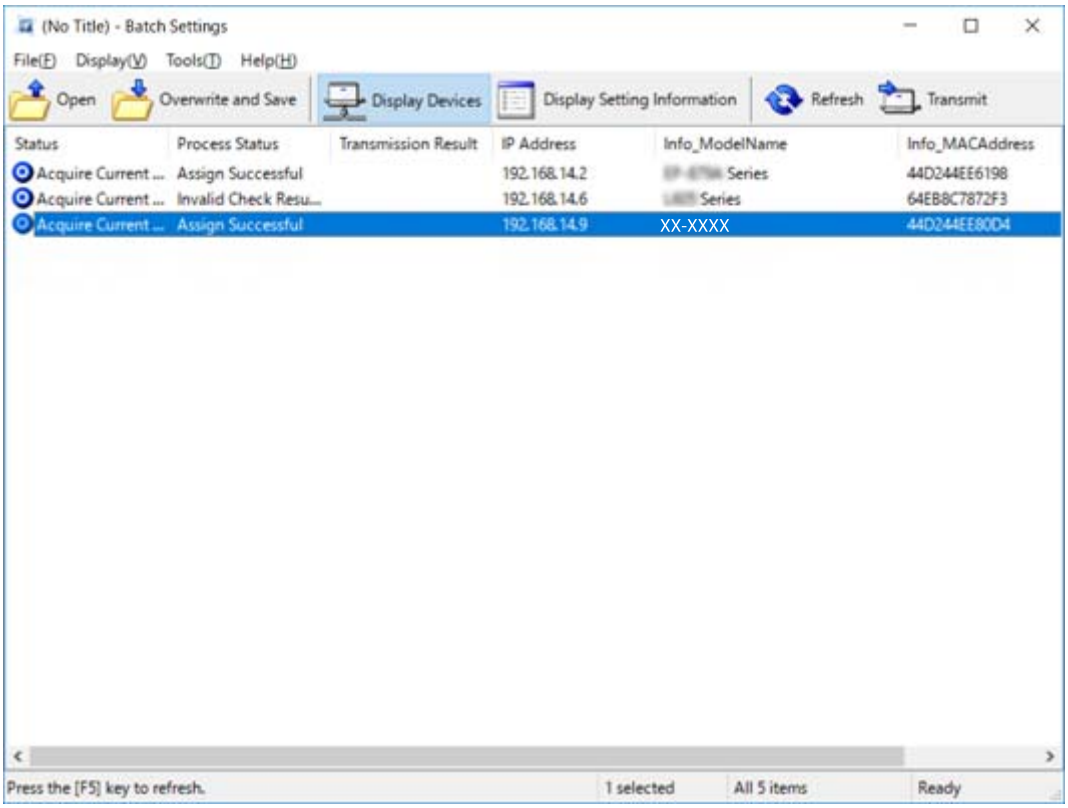
Tildel IP-adresser i konfigurationsfilen (SYLK fil) på én gang. Du skal oprette konfigurationsfilen før tildeling.

1. Tilslut alle enheder til netværket ved hjælp af Ethernet-kabler.
2. Tænd for scanneren.
3. Start EpsonNet Config.

   Der vises en liste over scannere på netværket. Det kan tage et stykke tid, før de vises.
4. Klik på **Tools** > **Batch Settings**.
5. Klik på **Open**.
6. På skærmbilledet til filvalg skal du vælge den SYLK-fil (*.sylk), der indeholder indstillingerne, og derefter klikke på **Open**.

7. Vælg de enheder, som du ønsker at foretage batchindstillinger for, med kolonnen **Status** indstillet til **Unassigned** og **Process Status** indstillet til **Assign Successful**.

   Når du foretager flere valg, skal du trykke på Ctrl eller Shift og klikke eller trække med musen.



8. Klik på **Transmit**.

9. Når skærmbilledet til indtastning af adgangskode vises, skal du indtaste adgangskoden og derefter klikke på **OK**.

   Overfør indstillingerne.

   Bemærk:
   Informationerne sendes til netværkskortet, indtil statusindikatoren er færdig. Du må ikke slukke for enheden eller den trådløse adapter, og du må ikke sende data til enheden.

10. På skærmbilledet **Transmitting Settings** skal du klikke på **OK**.

11. Kontroller status for den enhed, du har indstillet.

    For enheder, der viser  eller  , skal du kontrollere indholdet af indstillingsfilen eller kontrollere, at enheden er genstartet normalt.

Ikon	Status	Process Status	Forklaring
	Setup Complete	Setup Successful	Opsætning fuldført normalt.
	Setup Complete	Rebooting	Når oplysningerne er sendt, skal hver enhed genstarte for at aktivere indstillingerne. Der udføres en kontrol for at bestemme, om enheden kan tilsluttes efter genstart.
	Setup Complete	Reboot Failed	Kan ikke bekræfte enheden efter transmissionsindstillingerne. Kontroller, at enheden er tændt, eller om den er genstartet normalt.
	Setup Complete	Searching	Søgning efter den enhed, som er angivet i indstillingsfilen.*
	Setup Complete	Search Failed	Kan ikke kontrollere enheder, der allerede er konfigurereret. Kontroller, at enheden er tændt, eller om den er genstartet normalt.*

    * Kun når der vises konfigurationsoplysninger.

Relaterede oplysninger

➡ "Kørsel af EpsonNet Config — Windows" på side 56

➡ "Kørsel af EpsonNet Config — Mac OS" på side 56

Tildeling af en IP-adresse til hver enhed

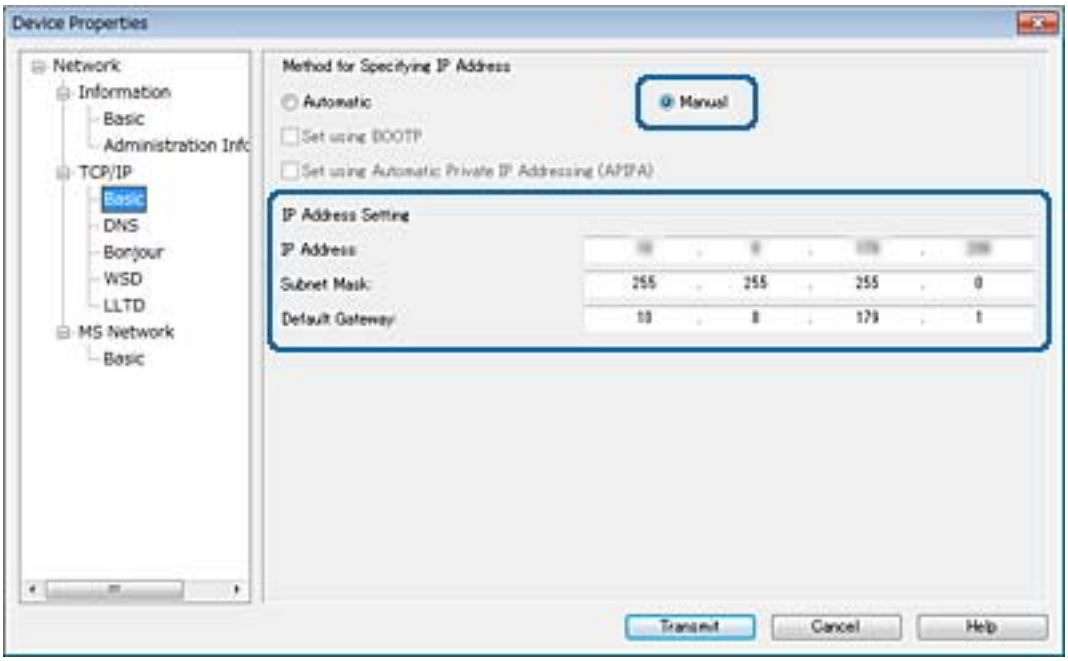
Tildel en IP-adresse til scanneren ved hjælp af EpsonNet Config.

1. Tænd for scanneren.
2. Slut scanneren til netværket vha. et Ethernet-kabel.
3. Start EpsonNet Config.

   Der vises en liste over scannere på netværket. Det kan tage et stykke tid, før de vises.
4. Dobbeltklik på den scanner, du vil tildele til.

   Bemærk:
   Hvis du har tilsluttet flere scannere af samme model, kan du identificere scanneren ved hjælp af MAC-adressen.
5. Vælg **Network** > **TCP/IP** > **Basic**.

6. Indtast adresserne for **IP Address**, **Subnet Mask** og **Default Gateway**.



Bemærk:
Indtast en statisk adresse, når du slutter scanneren til et sikkert netværk.

7. Klik på **Transmit**.

   Der vises et skærmbillede, som bekræfter fremsendelse af oplysningerne.

8. Klik på **OK**.

   Skærmbilledet med gennemført overførsel vises.

   Bemærk:
   Oplysningerne overføres til enheden, og derefter vises meddelelsen "Konfiguration gennemført". Du må ikke slukke for enheden, og du må ikke sende data til tjenesten.

9. Klik på **OK**.

Relaterede oplysninger

➡ "Kørsel af EpsonNet Config — Windows" på side 56
➡ "Kørsel af EpsonNet Config — Mac OS" på side 56

Brug af port til scanneren

Scanneren bruger følgende port. Disse porte skal stilles til rådighed af netværksadministratoren, som nødvendigt.

Appendiks

Afsender (klient)	Brug	Destination (server)	Protokol	Portnummer
Scanner	Afsendelse af e-mail (e-mailnotifikation)	SMTP-server	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	POP før SMTP-forbindelse (e-mailnotifikation)	POP-server	POP3 (TCP)	110
	WSD-kontrol	Klientcomputer	WSD (TCP)	5357
	Søg computeren med Push-scanning fra Document Capture Pro	Klientcomputer	Push-scanningsmappe på netværket	2968
	Indsamling af joboplysninger ved Push-scanning fra Document Capture Pro	Klientcomputer	Push-scanning på netværket	2968
Klientcomputer	Find scanneren fra et program som f.eks. EpsonNet Config og scannerdriver.	Scanner	ENPC (UDP)	3289
	Indsaml og opret MIB-information fra et program som f.eks. EpsonNet Config og scannerdriver.	Scanner	SNMP (UDP)	161
	Søg i WSD-scanneren	Scanner	WS-Discovery (UDP)	3702
	Videresendelse scanningsdata fra Document Capture Pro	Scanner	Netværksscanning (TCP)	1865

Avancerede sikkerhedsindstillinger for virksomheder

I dette kapitel beskriver vi de avancerede sikkerhedsfunktioner.

Sikkerhedsindstillinger og forebyggelse af fare

Når en enhed er tilsluttet et netværk, kan du få adgang til den fra en ekstern placering. Desuden kan mange mennesker dele enheden, hvilket er nyttigt i forhold til at forbedre driftseffektivitet og brugervenlighed. Dog er risici, såsom ulovlig adgang, ulovlig brug og manipulation med data, steget. Hvis du bruger enheden i et miljø, hvor du kan få adgang til internettet, er risiciene endnu højere.

For at undgå denne risiko har Epson-enheder en række forskellige sikkerhedsteknologier.

Indstil enheden efter behov i henhold til de miljøforhold, der er blevet skabt ud fra kundens miljøoplysninger.

Navn	Funktionstype	Hvad skal indstilles	Hvad skal forebygges
SSL/TLS-kommunikation	Kommunikationsstien for en computer og en enhed er krypteret med SSL/TLS-kommunikation. Indholdet af kommunikation via en browser er beskyttet.	Konfigurer et CA-certifikat for den server, der er certifikatunderskrevet af en CA (Certificate Authority) til enheden.	Undgå, at indstillingsoplysninger og indholdet af overførselsdata til scanneren fra computeren. Adgang til Epson-serveren på internettet fra enheden kan også beskyttes ved hjælp af en firmwareopdatering osv.
IPsec/IP-filtrering	Du kan indstille til at tillade adskillelse og afskæring af data, der kommer fra en bestemt klient eller er en bestemt type. Da IPsec beskytter data ved hjælp af en IP-pakkeenhed (kryptering og godkendelse), kan du trygt kommunikere usikrede scanningsprotokoller.	Opret en basispolitik og en individuel politik for at indstille, hvilke kunder eller hvilke datatyper, der kan få adgang til enheden.	Beskyt uautoriseret adgang og manipulation og aflytning af kommunikationsdata på enheden.
SNMPv3	Der er tilføjet funktioner, såsom overvågning af tilsluttede enheder i netværket, kontrol af dataintegritet på SNMP-protokollen, kryptering, brugergodkendelse osv.	Aktiver SNMPv3, og indstil derefter godkendelses og krypteringsmetoder.	Sørg for at ændre indstillingerne via netværket med fortrolig tilstandsovervågning.
IEEE802.1X	Giver kun en bruger, der er godkendt til Ethernet, lov for at oprette forbindelse. Giver kun en tilladt bruger lov til at bruge enheden.	Godkendelsesindstilling til RADIUS-serveren (godkendelsesserver).	Beskyt uautoriseret adgang til og brug af enheden.

Navn	Funktionstype	Hvad skal indstilles	Hvad skal forebygges
Læs id-kort	Du kan bruge enheden ved at holde et id-kort over den godkendte enhed, der er tilsluttet. Du kan begrænse erhvervelse af logfiler for hver bruger og enhed og begrænse den tilgængelige brug af enheder og de tilgængelige funktioner i hver bruger og gruppe.	Tilslut en godkendelsesenhed til enheden, og indstil derefter oplysninger om en bruger i godkendelsessystemet.	Forhindr uautoriseret brug og spoofing af enheden.

Relaterede oplysninger

➡ "SSL/TLS-kommunikation med scanneren" på side 63
➡ "Krypteret kommunikation ved hjælp af IPsec/IP-filtrering" på side 71
➡ "Brug af SNMPv3-protokol" på side 82
➡ "Tilslutning af scanneren til et IEEE802.1X-netværk" på side 84

Indstillinger for sikkerhedsfunktioner

Ved indstilling af IPsec/IP-filtrering eller IEEE802.1X anbefales det, at du tilgår Web Config ved hjælp af SSL/TLS for at kommunikere indstillingsoplysninger for at reducere sikkerhedsrisici såsom manipulation eller aflytning.

SSL/TLS-kommunikation med scanneren

Når servercertifikatet indstilles ved hjælp af SSL/TLS-kommunikation (Secure Sockets Layer/Transport Layer Security) til scanneren, kan du kryptere kommunikationsstien mellem computere. Gør dette, hvis du vil undgå fjernadgang og uautoriseret adgang.

Om digitalt certifikat

❏ Certifikat signeret af et CA

Du skal hente et certifikat, der er signeret af et CA (Certificate Authority, nøglecenter). Du kan sikre sikker kommunikation ved at bruge et CA-signeret certifikat. Du kan bruge et CA-signeret certifikat for hver sikkerhedsfunktion.

❏ CA-certifikat

Et CA-certifikat angiver, at en tredjepart har verificeret en servers identitet. Dette er en vigtig komponent i en sikkerhed af web of trust-typen. Du skal hente et CA-certifikat til servergodkendelse fra et CA, der udsteder det.

❏ Selvsigneret certifikat

Et selvsigneret certifikat er et certifikat, som scanneren selv udsteder og signerer. Dette certifikat er upålideligt og kan ikke undgå spoofing. Hvis du bruger dette certifikat til et SSL/TLS-certifikat, kan der blive vist en sikkerhedsalarm i en browser. Du kan kun bruge dette certifikat til en SSL/TLS-kommunikation.

Relaterede oplysninger

➡ "Hentning og import af et CA-signeret certifikat" på side 64

➡ "Sletning af et CA-signeret certifikat" på side 67
➡ "Opdatering af et selvsigneret certifikat" på side 68

Hentning og import af et CA-signeret certifikat

Hentning af et CA-signeret certifikat

For at hente et CA-signeret certifikat skal du oprette en CSR (Certificate Signing Request, anmodning om certifikatsignering) og ansøge om det hos et nøglecenter. Du kan oprette en CSR vha. Web Config og en computer.

Følg trinnene for at oprette en CSR og hente et CA-signeret certifikat vha. Web Config. Når du opretter en CSR vha. Web Config, er certifikatet i formatet PEM/DER.

1. Tilgå Web Config og vælg derefter **Network Security Settings**. Vælg derefter **SSL/TLS** > **Certificate** eller **IPsec/IP Filtering** > **Client Certificate** eller **IEEE802.1X** > **Client Certificate**.

2. Klik på **Generate** i **CSR**.

   En side til oprettelse af en CSR åbnes.

3. Indtast en værdi for hvert element.

   Bemærk:
   Den tilgængelige nøglelængde og forkortelser varierer afhængig af nøglecenteret. Opret en anmodning i henhold til det enkelte nøglecenters regler.

4. Klik på **OK**.

   Der vises en meddelelse om gennemførelse.

5. Vælg **Network Security Settings**. Vælg derefter **SSL/TLS** > **Certificate** eller **IPsec/IP Filtering** > **Client Certificate** eller **IEEE802.1X** > **Client Certificate**.

6. Klik på en af downloadknapperne i **CSR** i henhold til et format, der er angivet af hvert nøglecenter, for at downloade en CSR til en computer.

   > ***Vigtigt:***
   > *Opret ikke en CSR igen. Hvis du gør det, kan du muligvis ikke importere et udstedt CA-signed Certificate.*

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

   Følg de enkelte nøglecentres regler vedrørende sendemetode og form.

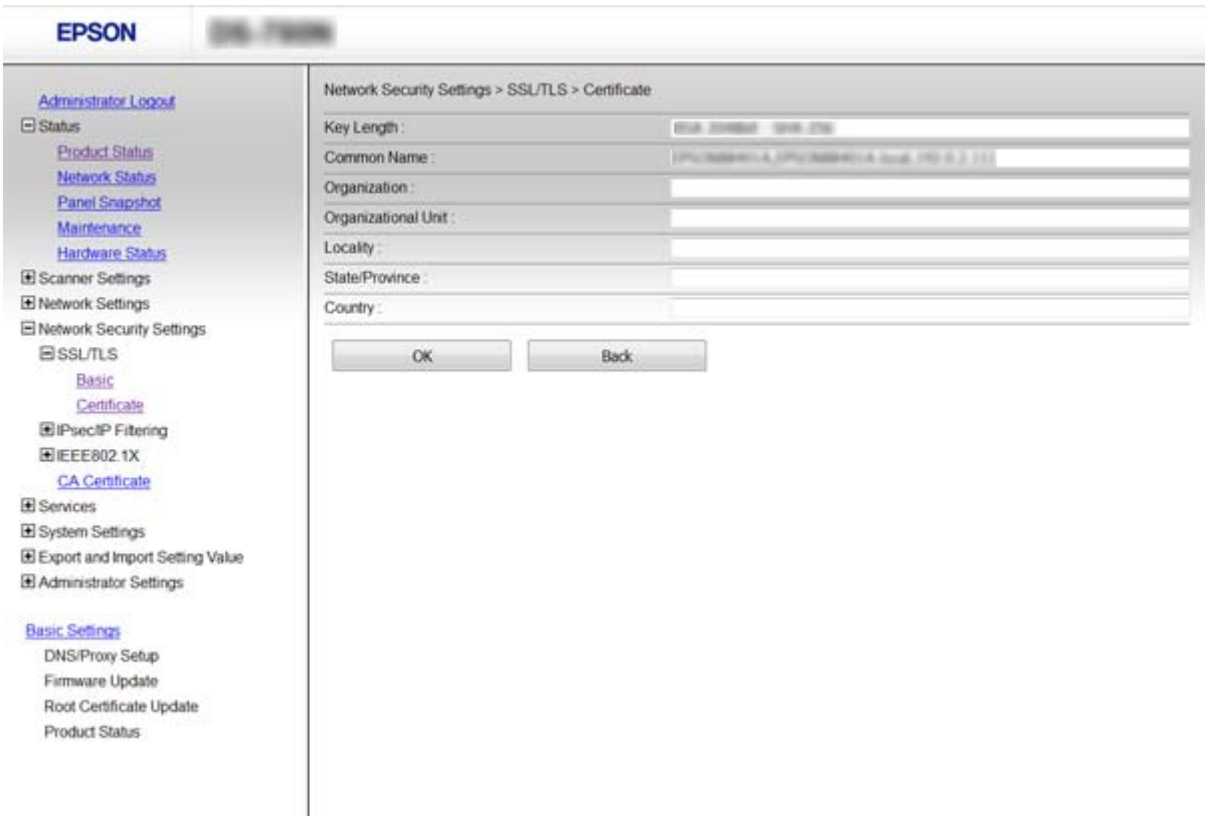
8. Gem det udstedte CA-signed Certificate på en computer, der er forbundet til scanneren.

   Hentningen af et CA-signed Certificate er gennemført, når du gemmer certifikatet på en destination.

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23
➡ "CSR-indstillingselementer" på side 65
➡ "Import af et CA-signeret certifikat" på side 65

CSR-indstillingselementer



Punkter	Indstillinger og forklaring
Key Length	Vælg en nøglelængde for en CSR.
Common Name	Du kan indtaste mellem 1 og 128 tegn. Hvis dette er en IP-adresse, bør det være en statisk IP-adresse. Eksempel: URL til åbning af Web Config: https://10.152.12.225 Almindeligt navn: 10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	Du kan indtaste mellem 0 og 64 tegn i ASCII (0x20–0x7E). Du kan dele adskilte navne med kommaer.
Country	Indtast en landekode på to cifre som angivet af ISO-3166.

Relaterede oplysninger

➡ "Hentning af et CA-signeret certifikat" på side 64

Import af et CA-signeret certifikat

Vigtigt:

❏ *Kontroller, at scannerens dato og klokkeslæt er indstillet korrekt.*

❏ *Hvis du henter et certifikat vha. en CSR, der er oprettet i Web Config, kan du importere et certifikat én gang.*

1. Tilgå Web Config og vælg derefter **Network Security Settings**. Vælg derefter **SSL/TLS** > **Certificate** eller **IPsec/IP Filtering** > **Client Certificate** eller **IEEE802.1X** > **Client Certificate**.

2. Klik på **Import**.

   En side til import af et certifikat åbnes.

3. Indtast en værdi for hvert element.

   Afhængig af hvor du opretter en CSR og filformatet for et certifikat, kan de nødvendige indstillinger variere. Indtast værdierne for de nødvendige elementer i henhold til nedenstående.

   - ❏ Der hentes et certifikat i PEM/DER-formatet fra Web Config
     - ❏ **Private Key**: Konfigurer ikke, da scanneren indeholder en privat nøgle.
     - ❏ **Password**: Konfigurer ikke.
     - ❏ **CA Certificate 1**/**CA Certificate 2**: Valgfrit
   - ❏ Et certifikat i PEM/DER-format hentet fra en computer
     - ❏ **Private Key**: Du skal indstille.
     - ❏ **Password**: Konfigurer ikke.
     - ❏ **CA Certificate 1**/**CA Certificate 2**: Valgfrit
   - ❏ Et certifikat i PKCS#12-format hentet fra en computer
     - ❏ **Private Key**: Konfigurer ikke.
     - ❏ **Password**: Valgfrit
     - ❏ **CA Certificate 1**/**CA Certificate 2**: Konfigurer ikke.

4. Klik på **OK**.

   Der vises en meddelelse om gennemførelse.

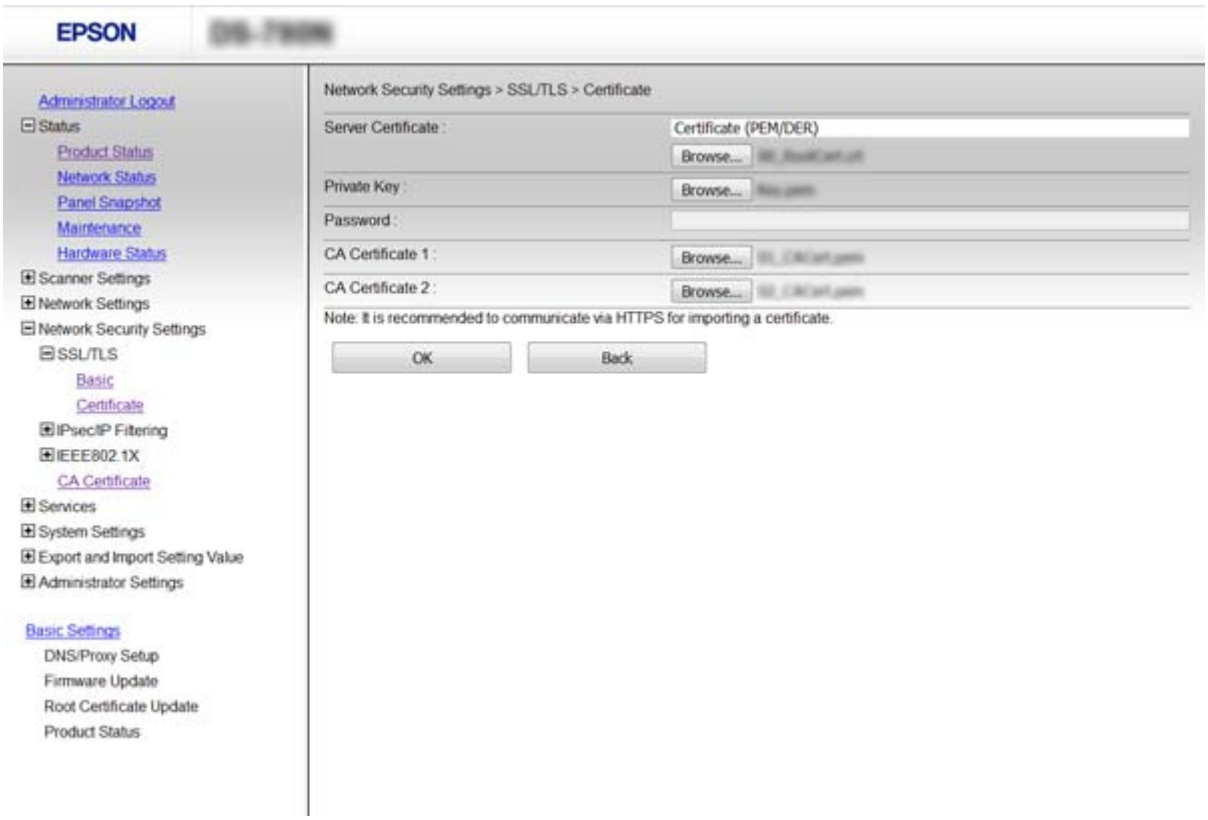
Bemærk:
Klik på ***Confirm*** *for at verificere certifikatoplysningerne.*

Relaterede oplysninger

➡ “Tilgå Web Config” på side 23

➡ “CA-signeret certifikat, importindstillingselementer” på side 67

CA-signeret certifikat, importindstillingselementer



Elementer	Indstillinger og forklaring
Server Certificate eller Client Certificate	Vælg et certifikatformat.
Private Key	Hvis du henter et certifikat i PEM/DER-format by vha. en CSR, der er oprettet fra en computer, skal du angive en privat nøglefil, der matcher et certifikat.
Password	Indtast en adgangskode til kryptering af en privat nøgle.
CA Certificate 1	Hvis certifikatets format er **Certificate (PEM/DER)**, skal du importere et certifikat fra et nøglecenter, som udsteder et servercertifikat. Angiv om nødvendigt en fil.
CA Certificate 2	Hvis certifikatets format er **Certificate (PEM/DER)**, skal du importere et certifikat fra et nøglecenter, der udsteder **CA Certificate 1**. Angiv om nødvendigt en fil.

Relaterede oplysninger

➡ "Import af et CA-signeret certifikat" på side 65

Sletning af et CA-signeret certifikat

Du kan slette en importeret, når certifikatet er udløbet, eller når en krypteret forbindelse er ikke længere er nødvendig.

> ***Vigtigt:***
> *Hvis du henter et certifikat vha. en CSR, der er oprettet i Web Config, kan du ikke importere et slettet certifikat igen. I så fald skal du oprette en CSR og hente et certifikat igen.*

1. Gå til Web Config, og vælg herefter **Network Security Settings**. Vælg derefter **SSL/TLS** > **Certificate** eller **IPsec/IP Filtering** > **Client Certificate** eller **IEEE802.1X** > **Client Certificate**.
2. Klik på **Delete**.
3. Bekræft, at du vil slette certifikatet, i den viste meddelelse.

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23

Opdatering af et selvsigneret certifikat

Hvis scanneren understøtter HTTPS-serverfunktionen, kan du opdatere et selvsigneret certifikat. Når du tilgår Web Config vha. et selvsigneret certifikat, vises en advarselsmeddelelse.

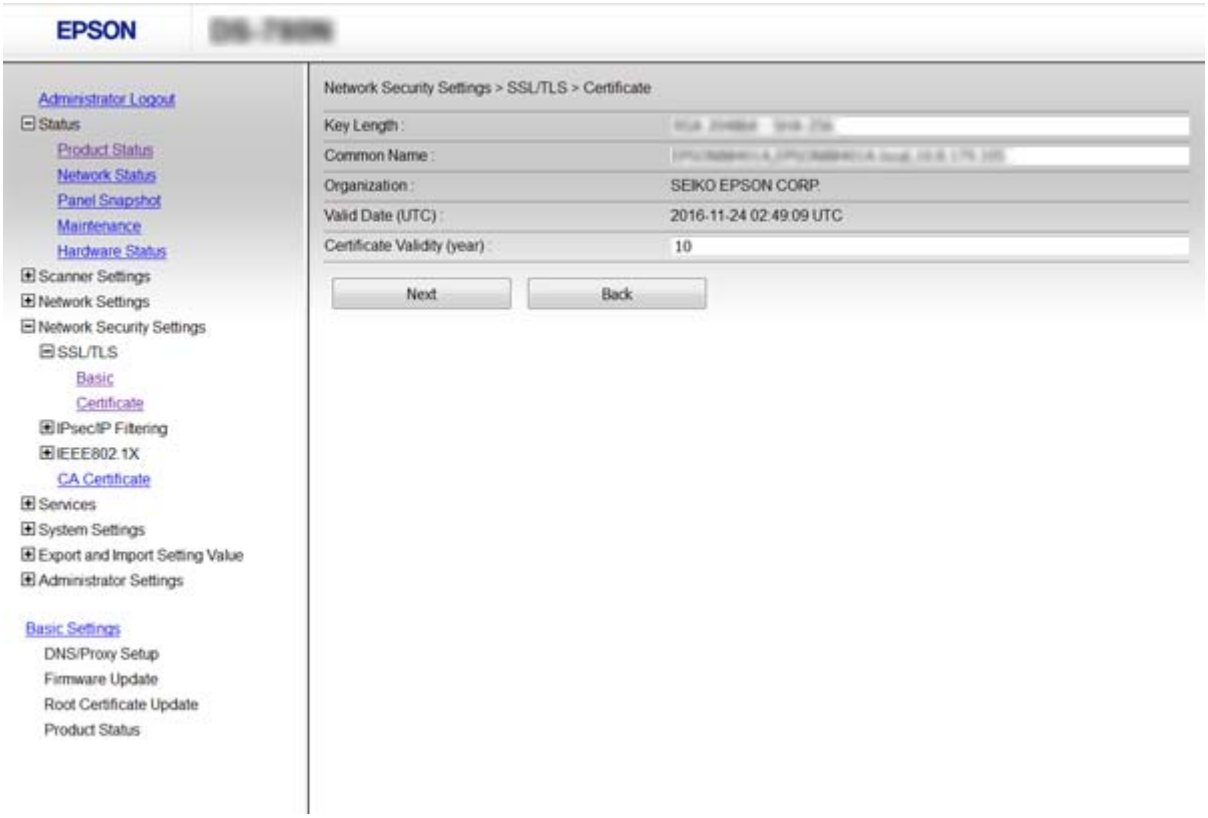
Brug et selvsigneret certifikat midlertidigt, til du henter og importerer et CA-signeret certifikat.

1. Gå til Web Config og vælg **Network Security Settings** > **SSL/TLS** > **Certificate**.
2. Klik på **Update**.
3. Indtast **Common Name**.

   Indtast en IP-adresse eller en id som f.eks. et FQDN-navn på scanneren. Du kan indtaste mellem 1 og 128 tegn.

   Bemærk:
   Du kan dele adskilte navne (CN) med kommaer.

4. Angiv en gyldighedsperiode for certifikatet.



5. Klik på **Next**.

   Der vises en bekræftelsesmeddelelse.

6. Klik på **OK**.

   Scanneren opdateres.

Bemærk:
*Klik på **Confirm** for at verificere certifikatoplysningerne.*

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23

Konfiguration af CA Certificate

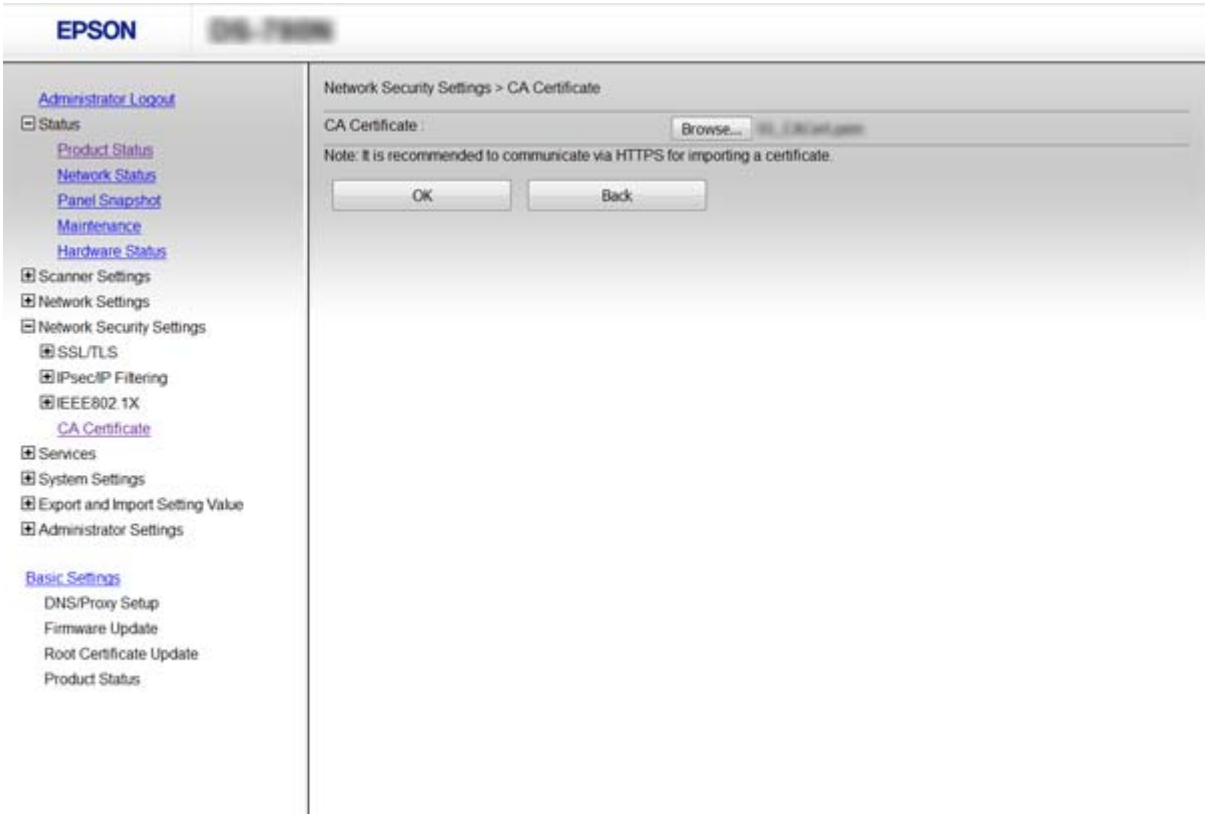
Du kan importere, vise, slette et CA Certificate.

Import af et CA Certificate

1. Tilgå Web Config og vælg derefter **Network Security Settings** > **CA Certificate**.

2. Klik på **Import**.

3. Specificer det CA Certificate, du vil importere.



4. Klik på **OK**.

Når importen er fuldført, vender du tilbage til skærmbilledet **CA Certificate**, hvor det importerede CA Certificate vises.

Relaterede oplysninger

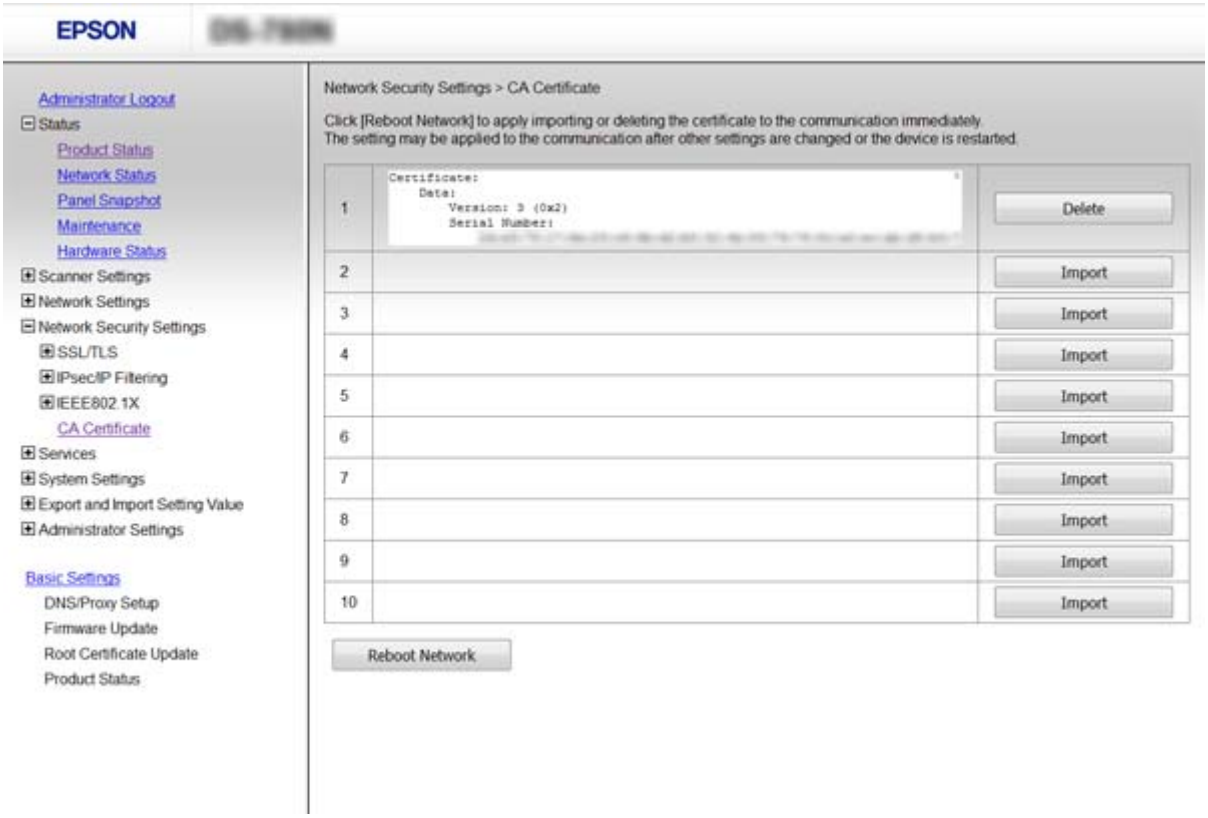
➡ "Tilgå Web Config" på side 23

Sletning af et CA Certificate

Du kan slette det importerede CA Certificate.

1. Tilgå Web Config og vælg derefter **Network Security Settings** > **CA Certificate**.

2. Klik på **Delete** ved siden af det CA Certificate, du vil slette.



3. Bekræft, at du vil slette certifikatet, i den viste meddelelse.

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23

Krypteret kommunikation ved hjælp af IPsec/IP-filtrering

Om IPsec/IP Filtering

Hvis scanneren understøtter en IPsec/IP-filtrering, kan du konfigurere at filtrere trafik baseret på IP-adresser, tjenester og port. Ved at kombinere filtreringen kan du konfigurere scanneren til at acceptere eller blokere angivne klienter og angivne data. Desuden kan du forbedre sikkerhedsniveauet ved hjælp af en IPsec.

Konfigurer standardpolitikken for at filtrere trafik. Standardpolitikken anvendes på hver bruger eller gruppe, der opretter forbindelse til scanneren. Konfigurer gruppepolitikker for at få en mere finmasket kontrol over brugere eller grupper af brugere. En gruppepolitik er en eller flere regler, der anvendes på en bruger eller brugergruppe. Scanneren styrer IP-pakker, der matcher konfigurerede politikker. IP-pakker godkendes i rækkefølgen af en gruppepolitik 1 til 10 og derefter en standardpolitik.

Bemærk:
Computere, der kører Windows Vista eller senere, eller Windows Server 2008 eller senere understøtter IPsec.

Konfiguration af Default Policy

1. Gå til Web Config og vælg **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Indtast en værdi for hvert element.
3. Klik på **Next**.

   Der vises en bekræftelsesmeddelelse.
4. Klik på **OK**.

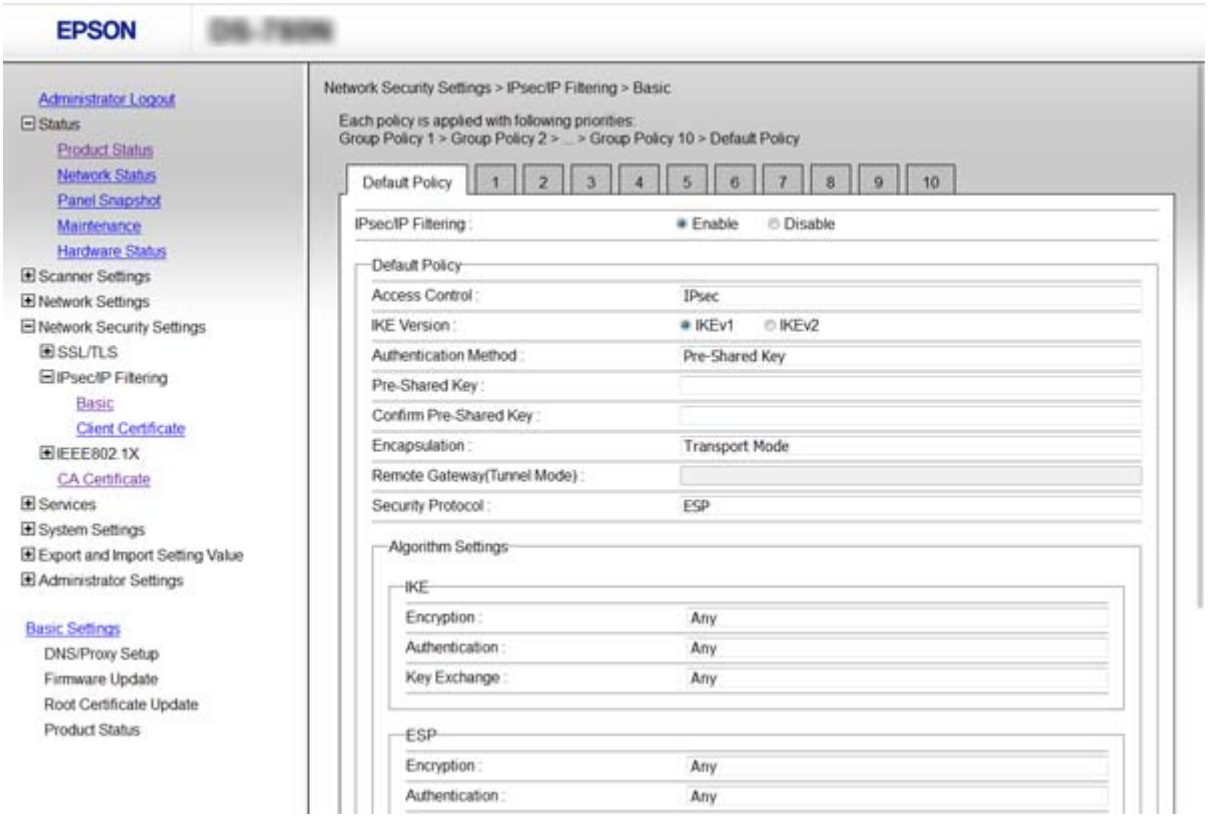
   Scanneren opdateres.

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23

➡ "Indstillingselementer for Default Policy" på side 72

Indstillingselementer for Default Policy



Punkter	Indstillinger og forklaring
IPsec/IP Filtering	Du kan aktivere eller deaktivere en IPsec/IP filtreringsfunktion.

Avancerede sikkerhedsindstillinger for virksomheder

Punkter	Indstillinger og forklaring	
Access Control	Konfigurer en kontrolmetode for IP-pakketrafik.	
	Permit Access	Vælg dette for at tillade konfigurerede IP-pakker at passere.
	Refuse Access	Vælg dette for at nægte konfigurerede IP-pakker at passere.
	IPsec	Vælg dette for at tillade konfigurerede IPsec-pakker at passere.
IKE Version	Vælg IKEv1 eller IKEv2 for IKE-version. Vælg en af dem i henhold til den enhed, som scanneren er tilsluttet.	
IKEv1	Følgende elementer vises, når du vælger **IKEv1** for **IKE Version**.	
	Authentication Method	For at vælge **Certificate**, skal du på forhånd hente og importere et CA-signeret certifikat.
	Pre-Shared Key	Hvis du vælger **Pre-Shared Key** som **Authentication Method**, skal du indtaste en forhåndsdelt nøgle på mellem 1 og 127 tegn.
	Confirm Pre-Shared Key	Indtast den konfigurerede nøgle for at bekræfte.
IKEv2	Følgende elementer vises, når du vælger **IKEv2** for **IKE Version**.	
Local	Authentication Method	For at vælge **Certificate**, skal du på forhånd hente og importere et CA-signeret certifikat.
	ID Type	Vælg scannerens id-type.
	ID	Indtast den id-type for scanneren, som stemmer overens med id-typen. Du kan ikke bruge "@", "#" og "=" som første tegn. **Distinguished Name**: Indtast 1 til 128 1-byte ASCII-tegn (0x20 til 0x7E). Du kan medtage "=". **IP Address**: Indtast IPv4 eller IPv6-format. **FQDN**: Indtast en kombination af mellem 1 og 255 tegn ved hjælp af A–Z, a–z, 0–9, "-" og punktum (.). **Email Address**: Indtast 1 til 128 1-byte ASCII-tegn (0x20 til 0x7E). Du skal medtage "@". **Key ID**: Indtast 1 til 128 1-byte ASCII-tegn (0x20 til 0x7E).
	Pre-Shared Key	Hvis du vælger **Pre-Shared Key** som **Authentication Method**, skal du indtaste en forhåndsdelt nøgle på mellem 1 og 127 tegn.
	Confirm Pre-Shared Key	Indtast den konfigurerede nøgle for at bekræfte.

Avancerede sikkerhedsindstillinger for virksomheder

Punkter	Indstillinger og forklaring	
Remote	Authentication Method	For at vælge **Certificate**, skal du på forhånd hente og importere et CA-signeret certifikat.
	ID Type	Vælg id-type for den enhed, du vil godkende.
	ID	Indtast den id-type for scanneren, som stemmer overens med id-typen. Du kan ikke bruge "@", "#" og "=" som første tegn. **Distinguished Name**: Indtast 1 til 128 1-byte ASCII-tegn (0x20 til 0x7E). Du kan medtage "=". **IP Address**: Indtast IPv4 eller IPv6-format. **FQDN**: Indtast en kombination af mellem 1 og 255 tegn ved hjælp af A–Z, a–z, 0–9, "-" og punktum (.). **Email Address**: Indtast 1 til 128 1-byte ASCII-tegn (0x20 til 0x7E). Du skal medtage "@". **Key ID**: Indtast 1 til 128 1-byte ASCII-tegn (0x20 til 0x7E).
	Pre-Shared Key	Hvis du vælger **Pre-Shared Key** som **Authentication Method**, skal du indtaste en forhåndsdelt nøgle på mellem 1 og 127 tegn.
	Confirm Pre-Shared Key	Indtast den konfigurerede nøgle for at bekræfte.
Encapsulation	Hvis du vælger **IPsec** som **Access Control**, skal du konfigurere en indkapslingstilstand.	
	Transport Mode	Vælg denne, hvis du kun bruger scanneren på samme LAN. IP-pakker af lag 4 eller senere krypteres.
	Tunnel Mode	Hvis du bruger scanneren på internettet-kompatible netværk såsom IPsec-VPN, skal du vælge denne mulighed. IP-pakkernes overskrift og data krypteres.
Remote Gateway(Tunnel Mode)	Hvis du vælger **Tunnel Mode** som **Encapsulation**, skal du indtaste en gateway-adresse på mellem 1 og 39 tegn.	
Security Protocol	**IPsec** for **Access Control**, vælg en indstilling.	
	ESP	Vælg dette for at sikre integriteten af en godkendelse og data og kryptere data.
	AH	Vælg dette for at sikre integriteten af en godkendelse og data. Du kan brug IPsec, selvom kryptering af data ikke er tilladt.
Algorithm Settings		
IKE	Encryption	Vælg krypteringsalgoritmen for IKE. Elementerne varierer afhængigt af IKE-versionen.
	Authentication	Vælg godkendelsesalgoritmen for IKE.
	Key Exchange	Vælg nøgleudvekslingsalgoritmen for IKE. Elementerne varierer afhængigt af IKE-versionen.

Punkter	Indstillinger og forklaring	
ESP	Encryption	Vælg krypteringsalgoritmen for ESP. Den er tilgængelig, når **ESP** er valgt for **Security Protocol**.
	Authentication	Vælg godkendelsesalgoritmen for ESP. Den er tilgængelig, når **ESP** er valgt for **Security Protocol**.
AH	Authentication	Vælg krypteringsalgoritmen for AH. Den er tilgængelig, når **AH** er valgt for **Security Protocol**.

Relaterede oplysninger

➡ "Konfiguration af Default Policy" på side 72

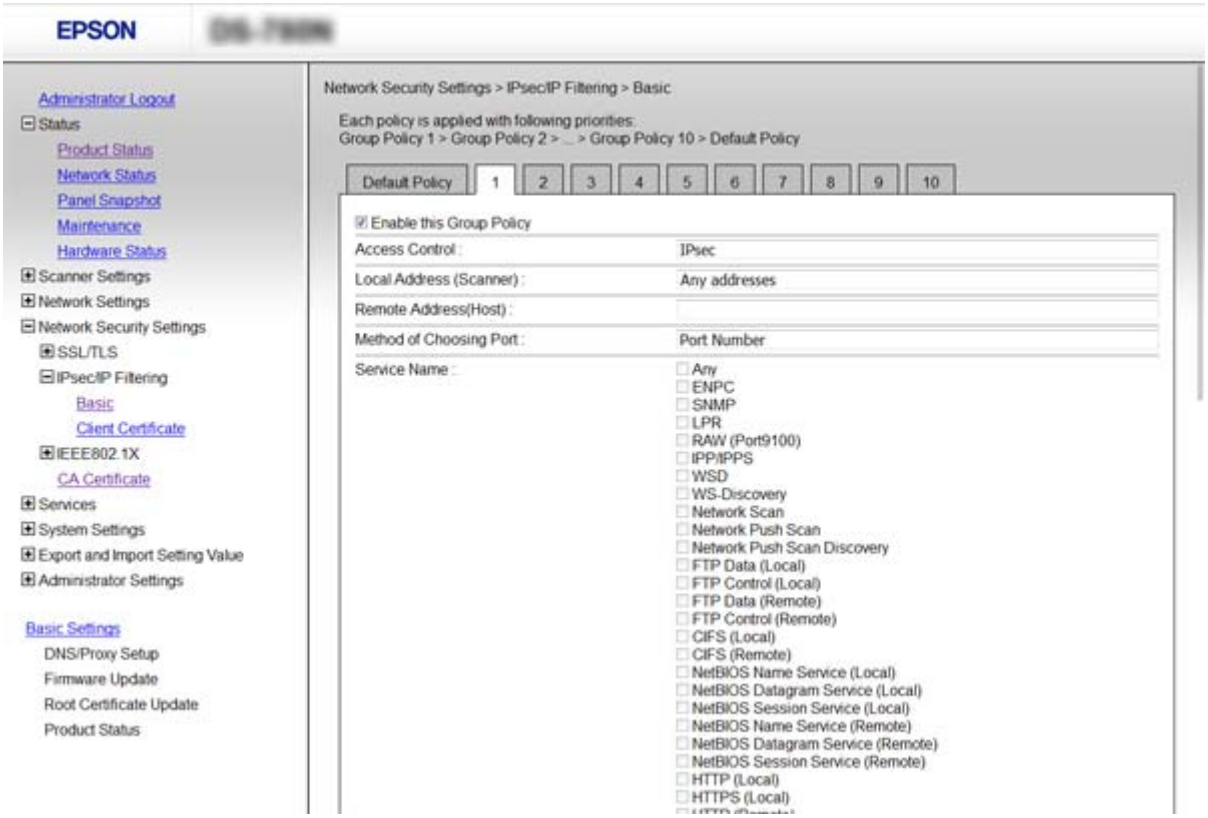
Konfiguration af Group Policy

1. Gå til Web Config og vælg **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Klik på en nummereret fane, du vil konfigurere.
3. Indtast en værdi for hvert element.
4. Klik på **Next**.
   Der vises en bekræftelsesmeddelelse.
5. Klik på **OK**.
   Scanneren opdateres.

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23
➡ "Indstillingselementer for Group Policy" på side 76

Indstillingselementer for Group Policy



Punkter	Indstillinger og forklaring	
Enable this Group Policy	Du kan aktivere eller deaktivere en gruppepolitik.	
Access Control	Konfigurer en kontrolmetode for IP-pakketrafik.	
	Permit Access	Vælg dette for at tillade konfigurerede IP-pakker at passere.
	Refuse Access	Vælg dette for at nægte konfigurerede IP-pakker at passere.
	IPsec	Vælg dette for at tillade konfigurerede IPsec-pakker at passere.
Local Address (Scanner)	Vælg en IPv4-adresse eller IPv6-adresse, der matcher dit netværksmiljø. Hvis en IP-adresse tildeles automatisk, kan du vælge **Use auto-obtained IPv4 address**.	
Remote Address(Host)	Indtast en enheds IP-adresse for at styre adgangen. IP-adressen skal være op til 43 tegn. Hvis du ikke indtaster en IP-adresse, styres alle adresser. ***Bemærk:*** *Hvis en IP-adresse tildeles automatisk (f. eks. tildeles af DHCP), kan forbindelsen være utilgængelig. Konfigurerer en statisk IP-adresse.*	
Method of Choosing Port	Vælg en metode til at specificere porte.	
Service Name	Hvis du vælger **Service Name** som **Method of Choosing Port**, skal du vælge en indstilling.	

Avancerede sikkerhedsindstillinger for virksomheder

Punkter	Indstillinger og forklaring	
Transport Protocol	Hvis du vælger **Port Number** som **Method of Choosing Port**, skal du konfigurere en indkapslingstilstand.	
	Any Protocol	Vælg dette for at styre alle protokoltyper.
	TCP	Vælg dette for at styre data til unicast.
	UDP	Vælg dette for at styre data til udsendelse og multicast.
	ICMPv4	Vælg dette for at styre ping-kommandoen.
Local Port	Hvis du vælger **Port Number** som **Method of Choosing Port**, og hvis du vælger **TCP** eller **UDP** som **Transport Protocol**, skal du indtaste portnumre for at styre modtagelse af pakker, ved at adskille dem med kommaer. Du kan højst indtaste 10 portnumre. Eksempel: 20,80,119,5220 Hvis du ikke indtaster et portnummer, styres alle porte.	
Remote Port	Hvis du vælger **Port Number** som **Method of Choosing Port**, og hvis du vælger **TCP** eller **UDP** som **Transport Protocol**, skal du indtaste portnumre for at styre afsendelse af pakker, ved at adskille dem med kommaer. Du kan højst indtaste 10 portnumre. Eksempel: 25,80,143,5220 Hvis du ikke indtaster et portnummer, styres alle porte.	
IKE Version	Vælg IKEv1 eller IKEv2 for IKE-version. Vælg en af dem i henhold til den enhed, som scanneren er tilsluttet.	
IKEv1	Følgende elementer vises, når du vælger **IKEv1** for **IKE Version**.	
	Authentication Method	Hvis du vælger **IPsec** som **Access Control**, skal du vælge en indstilling. Det anvendte certifikat er det samme som en standardpolitik.
	Pre-Shared Key	Hvis du vælger **Pre-Shared Key** som **Authentication Method**, skal du indtaste en forhåndsdelt nøgle på mellem 1 og 127 tegn.
	Confirm Pre-Shared Key	Indtast den konfigurerede nøgle for at bekræfte.
IKEv2	Følgende elementer vises, når du vælger **IKEv2** for **IKE Version**.	

Avancerede sikkerhedsindstillinger for virksomheder

Punkter	Indstillinger og forklaring	
Local	Authentication Method	Hvis du vælger **IPsec** som **Access Control**, skal du vælge en indstilling. Det anvendte certifikat er det samme som en standardpolitik.
	ID Type	Vælg scannerens id-type.
	ID	Indtast den id-type for scanneren, som stemmer overens med id-typen. Du kan ikke bruge "@", "#" og "=" som første tegn. **Distinguished Name**: Indtast 1 til 128 1-byte ASCII-tegn (0x20 til 0x7E). Du kan medtage "=". **IP Address**: Indtast IPv4 eller IPv6-format. **FQDN**: Indtast en kombination af mellem 1 og 255 tegn ved hjælp af A–Z, a–z, 0–9, "-" og punktum (.). **Email Address**: Indtast 1 til 128 1-byte ASCII-tegn (0x20 til 0x7E). Du skal medtage "@". **Key ID**: Indtast 1 til 128 1-byte ASCII-tegn (0x20 til 0x7E).
	Pre-Shared Key	Hvis du vælger **Pre-Shared Key** som **Authentication Method**, skal du indtaste en forhåndsdelt nøgle på mellem 1 og 127 tegn.
	Confirm Pre-Shared Key	Indtast den konfigurerede nøgle for at bekræfte.
Remote	Authentication Method	Hvis du vælger **IPsec** som **Access Control**, skal du vælge en indstilling. Det anvendte certifikat er det samme som en standardpolitik.
	ID Type	Vælg id-type for den enhed, du vil godkende.
	ID	Indtast den id-type for scanneren, som stemmer overens med id-typen. Du kan ikke bruge "@", "#" og "=" som første tegn. **Distinguished Name**: Indtast 1 til 128 1-byte ASCII-tegn (0x20 til 0x7E). Du kan medtage "=". **IP Address**: Indtast IPv4 eller IPv6-format. **FQDN**: Indtast en kombination af mellem 1 og 255 tegn ved hjælp af A–Z, a–z, 0–9, "-" og punktum (.). **Email Address**: Indtast 1 til 128 1-byte ASCII-tegn (0x20 til 0x7E). Du skal medtage "@". **Key ID**: Indtast 1 til 128 1-byte ASCII-tegn (0x20 til 0x7E).
	Pre-Shared Key	Hvis du vælger **Pre-Shared Key** som **Authentication Method**, skal du indtaste en forhåndsdelt nøgle på mellem 1 og 127 tegn.
	Confirm Pre-Shared Key	Indtast den konfigurerede nøgle for at bekræfte.

Avancerede sikkerhedsindstillinger for virksomheder

Punkter	Indstillinger og forklaring	
Encapsulation	Hvis du vælger **IPsec** som **Access Control**, skal du konfigurere en indkapslingstilstand.	
	Transport Mode	Vælg denne, hvis du kun bruger scanneren på samme LAN. IP-pakker af lag 4 eller senere krypteres.
	Tunnel Mode	Hvis du bruger scanneren på internettet-kompatible netværk såsom IPsec-VPN, skal du vælge denne mulighed. IP-pakkernes overskrift og data krypteres.
Remote Gateway(Tunnel Mode)	Hvis du vælger **Tunnel Mode** som **Encapsulation**, skal du indtaste en gateway-adresse på mellem 1 og 39 tegn.	
Security Protocol	Hvis du vælger **IPsec** som **Access Control**, skal du vælge en indstilling.	
	ESP	Vælg dette for at sikre integriteten af en godkendelse og data og kryptere data.
	AH	Vælg dette for at sikre integriteten af en godkendelse og data. Du kan brug IPsec, selvom kryptering af data ikke er tilladt.
Algorithm Settings		
IKE	Encryption	Vælg krypteringsalgoritmen for IKE. Elementerne varierer afhængigt af IKE-versionen.
	Authentication	Vælg godkendelsesalgoritmen for IKE.
	Key Exchange	Vælg nøgleudvekslingsalgoritmen for IKE. Elementerne varierer afhængigt af IKE-versionen.
ESP	Encryption	Vælg krypteringsalgoritmen for ESP. Den er tilgængelig, når **ESP** er valgt for **Security Protocol**.
	Authentication	Vælg godkendelsesalgoritmen for ESP. Den er tilgængelig, når **ESP** er valgt for **Security Protocol**.
AH	Authentication	Vælg godkendelsesalgoritmen for AH. Den er tilgængelig, når **AH** er valgt for **Security Protocol**.

Relaterede oplysninger

➡ "Konfiguration af Group Policy" på side 75

➡ "Kombination af Local Address (Scanner) og Remote Address(Host) på Group Policy" på side 79

➡ "Referencer for tjenestenavn på gruppepolitik" på side 80

Kombination af Local Address (Scanner) og Remote Address(Host) på Group Policy

	Indstilling af Local Address (Scanner)		
	IPv4	IPv6*2	Any addresses*3

Indstilling af Remote Address(Host)	IPv4*1	✓	–	✓
	IPv6*1, *2	–	✓	✓
	Blank	✓	✓	✓

*1 Hvis **IPsec** er valgt for **Access Control**, kan du ikke angive i en præfiks-længde.

*2 Hvis **IPsec** er valgt for **Access Control**, kan du vælge en link-lokal adresse (fe80::) men gruppepolitik vil blive deaktiveret.

*3 Undtagen IPv6 link-lokale adresser.

Referencer for tjenestenavn på gruppepolitik

Bemærk:
Ikke tilgængelige tjenester vises, men kan ikke vælges.

Tjenestenavn	Protokoltype	Lokalt portnummer	Fjernportnummer	Kontrollerede funktioner
Any	–	–	–	Alle tjenester
ENPC	UDP	3289	Enhver port	Søgning efter en scanner fra programmer såsom EpsonNet Config og en scannerdriver
SNMP	UDP	161	Enhver port	Anskaffelse og konfiguration af MIB fra programmer såsom EpsonNet Config og Epson scannerdriveren
WSD	TCP	Enhver port	5357	Styring af WSD
WS-Discovery	UDP	3702	Enhver port	Søgning efter en scanner fra WSD
Network Scan	TCP	1865	Enhver port	Videresendelse af scannerdata fra Document Capture Pro
Network Push Scan Discovery	UDP	2968	Enhver port	Søger efter en computer fra scanneren.
Network Push Scan	TCP	Enhver port	2968	Anskaffelse af jobinformation fra push-scanning fra Document Capture Pro eller Document Capture
HTTP (Local)	TCP	80	Enhver port	HTTP(S)-server (videresendelse af Web Config- og WSD-data)
HTTPS (Local)	TCP	443	Enhver port	
HTTP (Remote)	TCP	Enhver port	80	HTTP(S)-klient (kommunikere mellem firmwareopdatering og opdatering af rodcertifikat)
HTTPS (Remote)	TCP	Enhver port	443	

Eksempler på konfiguration af IPsec/IP Filtering

Kun modtagelse af IPsec-pakker

Dette eksempel gælder kun konfiguration af en standardpolitik.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **IPsec**

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

❏ **Pre-Shared Key**: Indtast op til 127 tegn.

Group Policy:

Konfigurer ikke.

Accept af scanning ved hjælp af Epson Scan 2 og scannerindstillinger

Dette eksempel tillader kommunikation af scannerdata og scannerkonfiguration fra specificerede tjenester.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy:

❏ **Enable this Group Policy**: Marker afkrydsningsfeltet.

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

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

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

❏ **Service Name**: Afkryds felterne **ENPC**, **SNMP**, **Network Scan**, **HTTP (Local)** og **HTTPS (Local)**.

Kun modtagelse af adgang fra en angivet IP-adresse

Dette eksempel tillader en angivet IP-adresse at få adgang til scanneren.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

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

Group Policy:

❏ **Enable this Group Policy**: Marker afkrydsningsfeltet.

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

❏ **Remote Address(Host)**: En administrators klients IP-adresse

Bemærk:
Uanset konfiguration af politik kan klienten få adgang til og konfigurere scanneren.

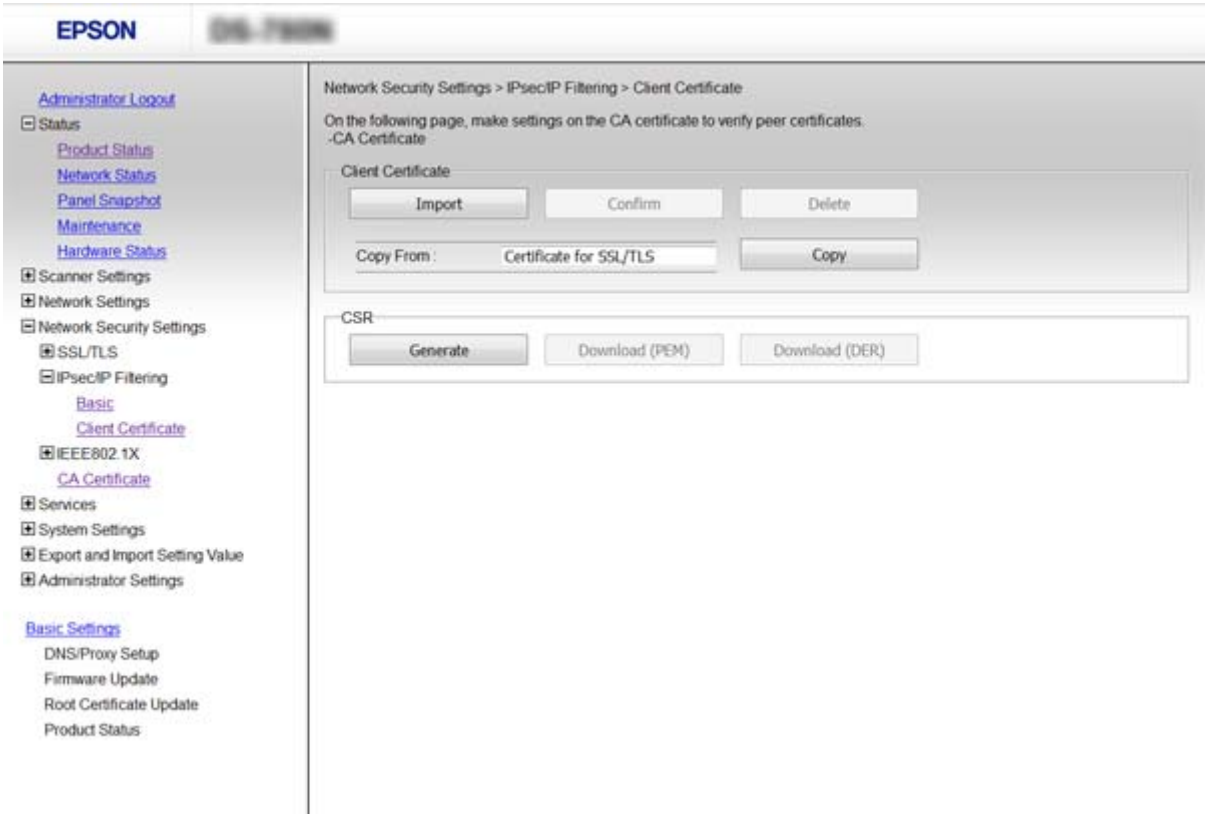
Konfiguration af et certifikat til IPsec/IP Filtering

Konfigurer klientcertifikatet for IPsec/IP-filtrering. Hvis du vil konfigurere nøglecenteret skal du gå til **CA Certificate**.

1. Gå til Web Config og vælg **Network Security Settings** > **IPsec/IP Filtering** > **Client Certificate**.

2. Importer certifikatet i **Client Certificate**.

   Hvis du allerede har importeret et certifikat, der er udgivet af et nøglecenter i IEEE802.1X eller SSL/TLS, kan du kopiere certifikatet og bruge det i IPsec/IP-filtrering. Du kopierer ved at vælge certifikatet fra **Copy From** og klikke på **Copy**.



Relaterede oplysninger

➡ "Tilgå Web Config" på side 23

➡ "Hentning og import af et CA-signeret certifikat" på side 64

Brug af SNMPv3-protokol

Om SNMPv3

SNMP er en protokol, der udfører overvågning og kontrol for at indsamle oplysninger om de enheder, der er tilsluttet netværket. SNMPv3 er den version af styringssikkerhedsfunktionen, der er blevet forbedret.

Når du bruger SNMPv3, kan tilstandsovervågning og indstillingsændringer på SNMP-kommunikationen (pakke) godkendes og krypteres for at beskytte SNMP-kommunikationen (pakke) fra netværksrisici, såsom telefonaflytning, personefterligning og manipulation.

Konfiguration af SNMPv3

Hvis scanneren understøtter SNMPv3-protokollen, kan du overvåge og kontrollere adgang til scanneren.

1. Gå til Web Config og vælg **Services** > **Protocol**.
2. Indtast en værdi for hvert element i **SNMPv3 Settings**.
3. Klik på **Next**.

   Der vises en bekræftelsesmeddelelse.
4. Klik på **OK**.

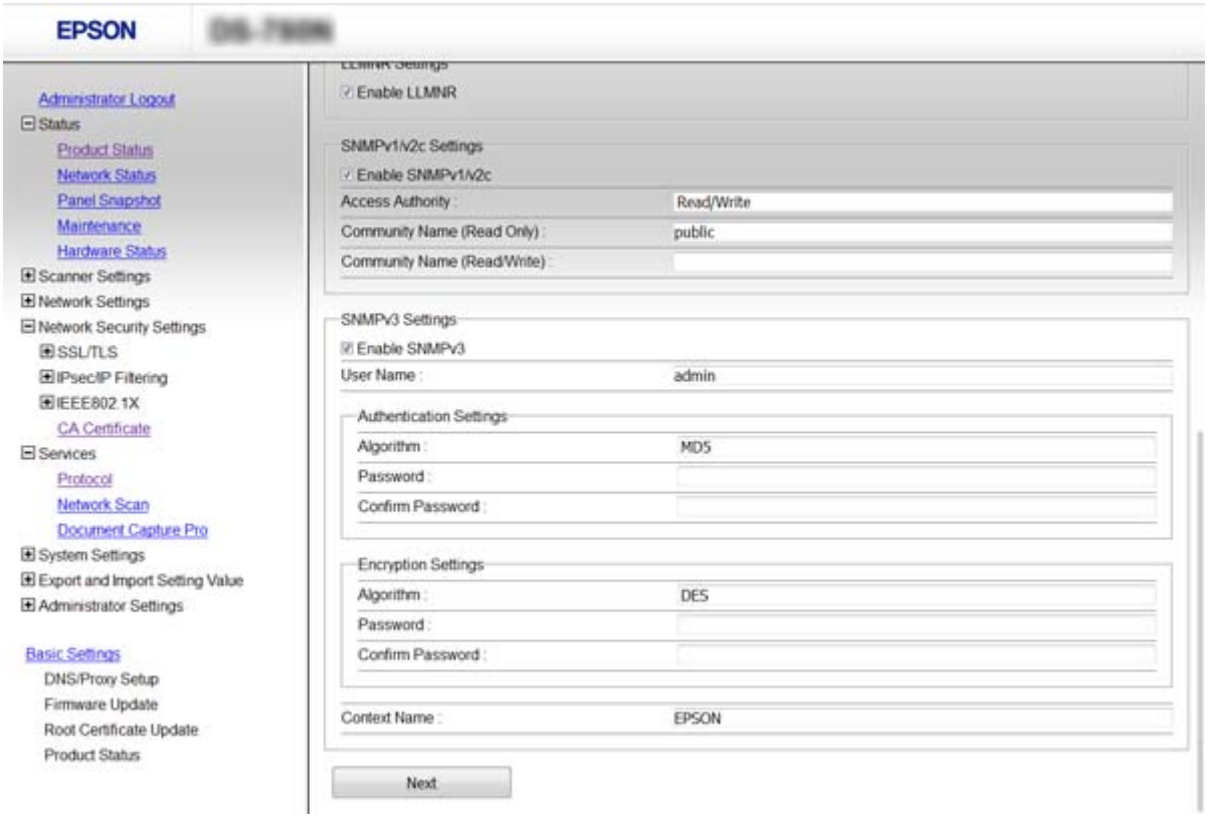
   Scanneren opdateres.

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23

➡ "SNMPv3-indstillingselementer" på side 83

SNMPv3-indstillingselementer



Elementer	Indstillinger og forklaring
Enable SNMPv3	SNMPv3 aktiveres, når feltet markeres.
User Name	Indtast mellem 1 og 32 tegn bestående af 1-bytetegn.
Authentication Settings	
Algorithm	Vælg en algoritme for en godkendelse.

Elementer	Indstillinger og forklaring
Password	Indtast mellem 8 og 32 tegn i ASCII (0x20-0x7E).
Confirm Password	Indtast den adgangskode, du har konfigureret, som bekræftelse.
Encryption Settings	
Algorithm	Vælg en algoritme for en kryptering.
Password	Indtast mellem 8 og 32 tegn i ASCII (0x20-0x7E).
Confirm Password	Indtast den adgangskode, du har konfigureret, som bekræftelse.
Context Name	Indtast mellem 1 og 32 tegn bestående af 1-bytetegn.

Relaterede oplysninger

➡ "Konfiguration af SNMPv3" på side 82

Tilslutning af scanneren til et IEEE802.1X-netværk

Konfiguration af et IEEE802.1X-netværk

Hvis scanneren understøtter IEEE802.1X, kan du bruge scanneren på et netværk med godkendelse, der er forbundet til en RADIUS-server og en hub som en godkender.

1. Gå til Web Config og vælg **Network Security Settings** > **IEEE802.1X** > **Basic**.
2. Indtast en værdi for hvert element.
3. Klik på **Next**.

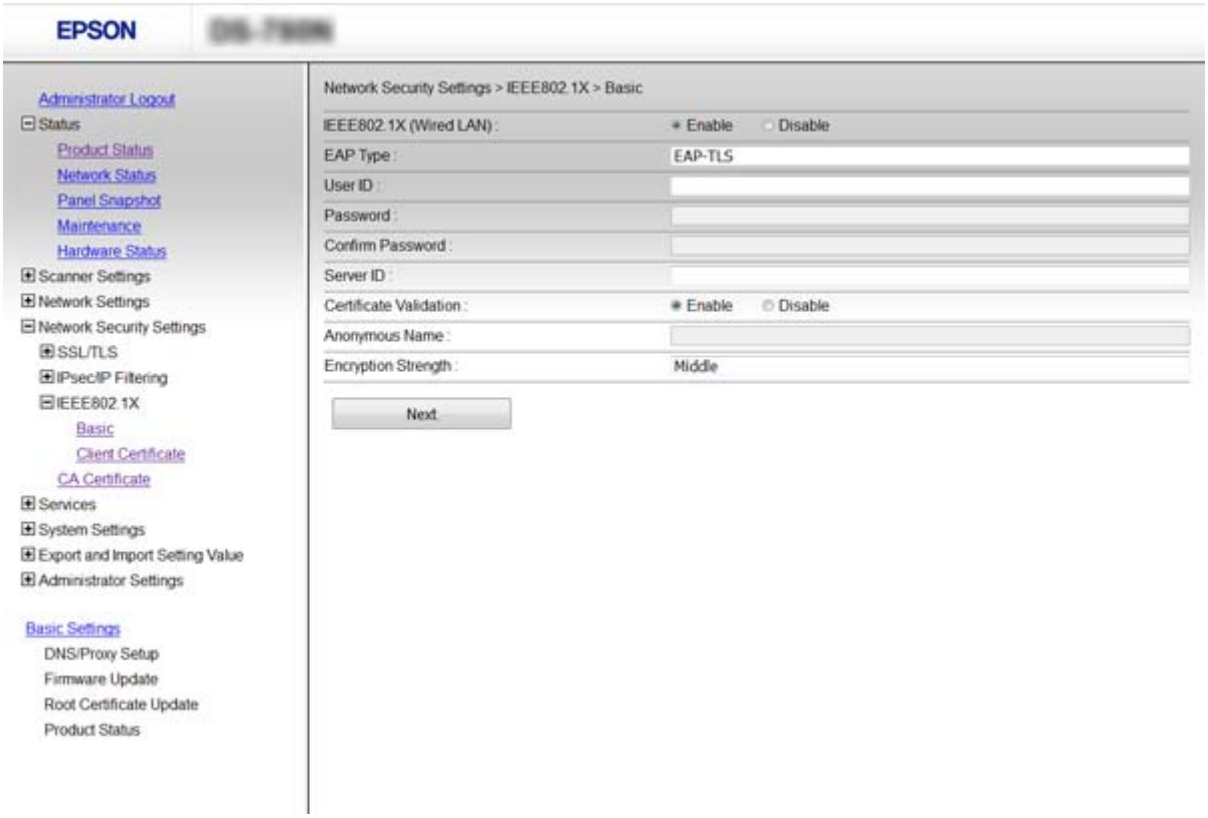
   Der vises en bekræftelsesmeddelelse.
4. Klik på **OK**.

   Scanneren opdateres.

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23
➡ "Indstillingselementer for IEEE802.1X-netværk" på side 85
➡ "Kan ikke få adgang til printeren eller scanneren efter konfiguration af IEEE802.1X" på side 89

Indstillingselementer for IEEE802.1X-netværk



Punkter	Indstillinger og forklaring	
IEEE802.1X (Wired LAN)	Du kan aktivere eller deaktivere indstillingerne for siden (**IEEE802.1X** > **Basic**) for IEEE802.1X (kabeltilsluttet LAN).	
EAP Type	Vælg en indstilling for en godkendelsesmetode mellem scanneren og en RADIUS-server.	
	EAP-TLS	Du skal hente og importere et nøglecentersigneret certifikat.
	PEAP-TLS	
	PEAP/MSCHAPv2	Du skal konfigurere en adgangskode.
User ID	Konfigurer en id, der skal bruges til en godkendelse af en RADIUS-server. Indtast 1 til 128 1-byte ASCII-tegn (0x20 til 0x7E).	
Password	Konfigurer en adgangskode til godkendelse af scanneren. Indtast 1 til 128 1-byte ASCII-tegn (0x20 til 0x7E). Hvis du bruger en Windows server som en RADIUS server, kan du indtaste op til 127 tegn.	
Confirm Password	Indtast den konfigurerede adgangskode for at bekræfte.	
Server ID	Du kan konfigurere en server-id til godkendelse med en angivet RADIUS-server. Godkenderen verificerer, om en server-id er indeholdt i feltet subject/subjectAltName i et servercertifikat, der er sendt fra en RADIUS -server. Indtast 0 til 128 1-byte ASCII-tegn (0x20 til 0x7E).	
Certificate Validation	Du kan indstille validering af servercertifikat uanset godkendelsesmetode. Importer certifikatet i **CA Certificate**.	

Punkter	Indstillinger og forklaring	
Anonymous Name	Hvis du vælger **PEAP-TLS** eller **PEAP/MSCHAPv2** som **Authentication Method**, kan du konfigurere et anonymt navn i stedet for en bruger-id for en fase 1 af en PEAP-godkendelse. Indtast 0 til 128 1-byte ASCII-tegn (0x20 til 0x7E).	
Encryption Strength	Du kan vælge et af følgende.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Relaterede oplysninger

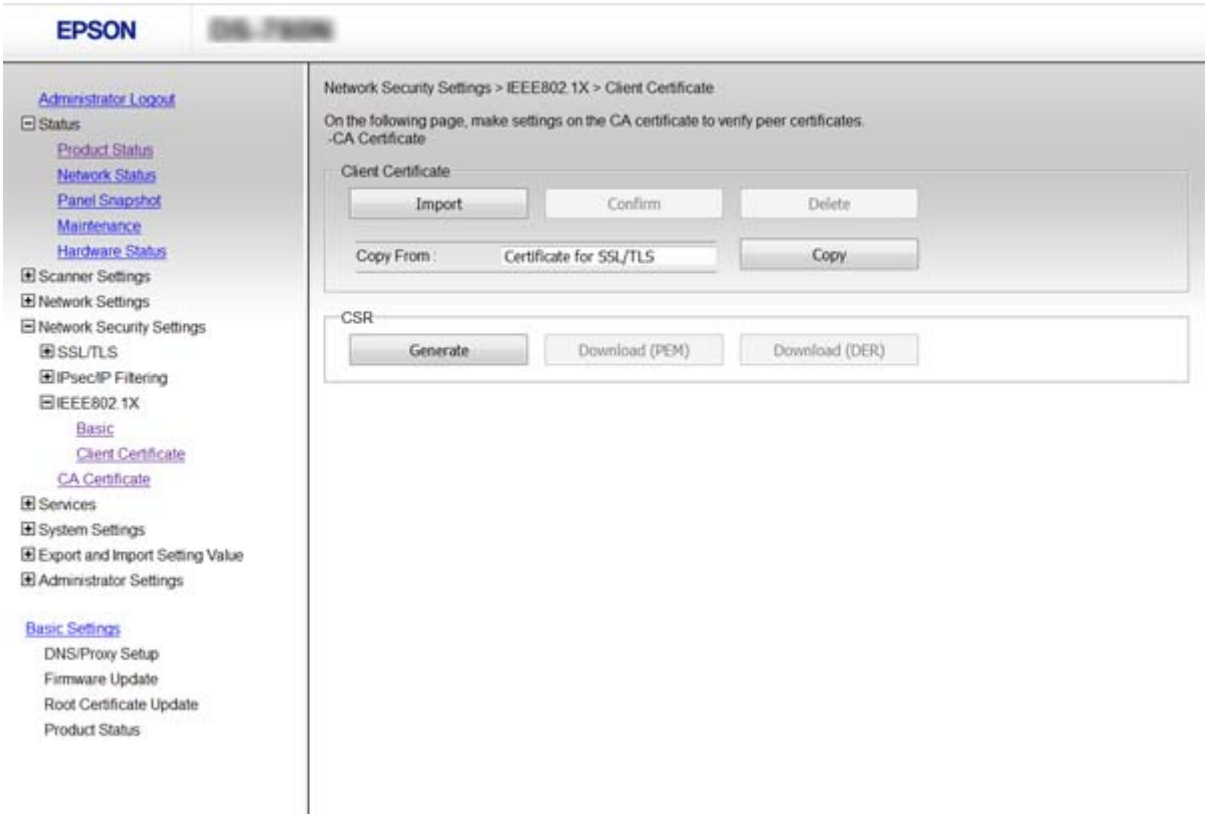
➡ "Konfiguration af et IEEE802.1X-netværk" på side 84

Konfiguration af et certifikat til IEEE802.1X

Konfiguration af klientcertifikatet til IEEE802.1X. Hvis du vil konfigurere nøglecentercertifikatet skal du gå til **CA Certificate**.

1. Gå til Web Config og vælg **Network Security Settings** > **IEEE802.1X** > **Client Certificate**.
2. Indtast et certifikat i **Client Certificate**.

   Du kan kopiere certifikatet, hvis der er udgivet af et nøglecenter. Du kopierer ved at vælge certifikatet fra **Copy From** og klikke på **Copy**.



Relaterede oplysninger

➡ "Tilgå Web Config" på side 23

➡ "Hentning og import af et CA-signeret certifikat" på side 64

Problemløsning for avanceret sikkerhed

Gendannelse af sikkerhedsindstillingerne

Når du opretter et meget sikkert miljø som f.eks. IPsec/IP-filtrering eller IEEE802.1X, kan du muligvis ikke kommunikere med enheder på grund af forkerte indstillinger eller problemer med enheden eller serveren. I dette tilfælde skal du gendanne sikkerhedsindstillingerne og foretage indstillinger for enheden igen eller tillade midlertidig brug.

Deaktivering af sikkerhedsfunktionen ved hjælp af kontrolpanelet

Du kan deaktivere IPsec/IP-filtrering eller IEEE802.1X ved hjælp af scannerens kontrolpanel.

1. Tryk på **Indstillinger** > **Netværksindstillinger**.
2. Tryk på **Skift indstillinger**.
3. Tryk på de elementer, du vil deaktivere.
   - ❏ **IPsec/IP Filtering**
   - ❏ **IEEE802.1X**
4. Når der vises en fuldført-meddelelse, skal du trykke på **Forts.**.

Gendannelse af sikkerhedsfunktionen ved hjælp af Web Config

For IEEE802.1X vil enheder muligvis ikke blive genkendt på netværket. I så fald skal du deaktivere funktionen ved hjælp af scannerens kontrolpanel.

For IPsec/IP-filtrering kan du deaktivere funktionen, hvis du kan få adgang til enheden fra computeren.

Deaktivering af IPsec/IP-filtrering ved hjælp af Web Config

1. Gå til Web Config, og vælg **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Vælg **Disable** for **IPsec/IP Filtering** i **Default Policy**.
3. Klik på **Next**, og ryd **Enable this Group Policy** for alle gruppepolitikker.
4. Klik på **OK**.

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23

Problemer med brug af netværkssikkerhedsfunktioner

Glemt en forhåndsdelt nøgle

Konfigurer nøglen igen vha. Web Config.

For at ændre nøglen, skal du gå til Web Config og vælge **Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Default Policy** eller **Group Policy**.

Når du ændrer den forhåndsdelte nøgle, skal du konfigurere den forhåndsdelte nøgle til computere.

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23

Kan ikke kommunikere med IPsec-kommunikation

Bruger du en ikke-understøttet algoritme til computerindstillingerne?

Scanneren understøtter følgende algoritmer.

Sikkerhedsmetoder	Algoritmer
IKE-krypteringsalgoritme	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE-godkendelsesalgoritme	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE-nøgleudvekslingsalgoritme	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-godkendelsesalgoritme	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH-godkendelsesalgoritme	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* Kun tilgængelig for IKEv2

Relaterede oplysninger

➡ "Krypteret kommunikation ved hjælp af IPsec/IP-filtrering" på side 71

Kan pludselig ikke kommunikere

Er scannerens IP-adresse ugyldig, eller er den ændret?

Deaktiver IPsec vha. scannerens kontrolpanel.

Hvis DHCP er forældet eller genstarter, eller hvis IPv6-adressen er forældet eller ikke er hentet, kan IP-adressen, som er registreret for scannerens Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**), muligvis ikke findes.

Brug af en statisk IP-adresse.

Er computerens IP-adresse ugyldig, eller er den ændret?

Deaktiver IPsec vha. scannerens kontrolpanel.

Hvis DHCP er forældet eller genstarter, eller hvis IPv6-adressen er forældet eller ikke er hentet, kan IP-adressen, som er registreret for scannerens Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**), muligvis ikke findes.

Brug af en statisk IP-adresse.

Relaterede oplysninger

➡ "Tilgå Web Config" på side 23

➡ "Krypteret kommunikation ved hjælp af IPsec/IP-filtrering" på side 71

Kan ikke oprette forbindelse efter konfiguration af IPsec/IP-filtrering

Indstillingsværdien er muligvis forkert.

Deaktiver IPsec/IP-filtrering på scannerens kontrolpanel. Forbind scanneren og computeren og juster indstillingerne for IPsec/IP-filtrering igen.

Relaterede oplysninger

➡ "Krypteret kommunikation ved hjælp af IPsec/IP-filtrering" på side 71

Kan ikke få adgang til printeren eller scanneren efter konfiguration af IEEE802.1X

Indstillingerne kan være forkert.

Deaktiver IEEE802.1X fra scannerens kontrolpanel. Tilslut scanneren og en computer, og konfigurer derefter IEEE802.1X igen.

Relaterede oplysninger

➡ "Konfiguration af et IEEE802.1X-netværk" på side 84

Problemer med brug af et digitalt certifikat

Kan ikke importere et CA-signeret certifikat

Stemmer det CA-signerede certifikat og oplysningerne i CSR'en overens?

Hvis det CA-signerede certifikat og CSR'en ikke indeholder samme oplysninger, kan CSR'en ikke importeres. Kontroller følgende:

❏ Forsøger du at importere certifikatet til en enhed, der ikke indeholder samme oplysninger?

Kontroller oplysninger i CSR'en, og importer derefter certifikatet til en enhed, der indeholder samme oplysninger.

❏ Har du overskrevet den CSR, der er gemt i scanneren, efter at have sendt CSR'en til et nøglecenter?

Hent det CA-signerede certifikat igen med CSR'en.

Er det CA-signerede certifikat større end 5 KB?

Du kan ikke importere et CA-signeret certifikat, der er større end 5 KB.

Er adgangskoden til import af certifikatet korrekt?

Hvis du glemmer adgangskoden, kan du ikke importere certifikatet.

Relaterede oplysninger

➡ "Import af et CA-signeret certifikat" på side 65

Kan ikke opdatere et selvsigneret certifikat

Er Common Name indtastet?

Common Name skal indtastes.

Er der ikke-understøttede tegn i Common Name? F.eks. understøttes japansk ikke.

Indtast mellem 1 og 128 tegn i enten IPv4-, IPv6-, værtsnavn- eller FQDN-format i ASCII (0x20-0x7E).

Er der et komma eller mellemrum i Common Name?

Hvis et komma indtastes, opdeles **Common Name** på dette sted. Hvis der kun er indtastet et mellemrum før eller efter et komma, opstår der en fejl.

Relaterede oplysninger

➡ "Opdatering af et selvsigneret certifikat" på side 68

Kan ikke oprette en CSR

Er Common Name indtastet?

Common Name skal indtastes.

Er der ikke-understøttede tegn i Common Name, Organization, Organizational Unit, Locality, State/ Province? F.eks. understøttes japansk ikke.

Indtast tegn i enten IPv4-, IPv6-, værtsnavn eller FQDN-format i ASCII (0x20-0x7E).

Er der et komma eller mellemrum i Common Name?

Hvis et komma indtastes, opdeles **Common Name** på dette sted. Hvis der kun er indtastet et mellemrum før eller efter et komma, opstår der en fejl.

Relaterede oplysninger

➡ "Hentning af et CA-signeret certifikat" på side 64

Advarsel vedrørende et digitalt certifikats udseende

Meddelelser	Årsag/Afhjælpning
Enter a Server Certificate.	**Årsag:** Du har ikke valgt en fil til import. **Afhjælpning:** Vælg en fil, og klik på **Import**.
CA Certificate 1 is not entered.	**Årsag:** CA-certifikat 1 er ikke indtastet, og kun CA-certifikat 2 er indtastet. **Afhjælpning:** Importer CA-certifikat 1 først.
Invalid value below.	**Årsag:** Der er ikke-understøttede tegn i filstien og/eller adgangskoden. **Afhjælpning:** Kontroller, at tegnede er indtastet korrekt for elementet.
Invalid date and time.	**Årsag:** Data og klokkeslæt er ikke indstillet i scanneren. **Afhjælpning:** Indstil dato og klokkeslæt vha. Web Config eller EpsonNet Config.
Invalid password.	**Årsag:** Den indstillede adgangskode for CA-certifikatet og den indtastede adgangskode stemmer ikke overens. **Afhjælpning:** Indtast den korrekte adgangskode.

Avancerede sikkerhedsindstillinger for virksomheder

Meddelelser	Årsag/Afhjælpning
Invalid file.	**Årsag:** Du importerer ikke en certifikatfil i X509-format. **Afhjælpning:** Kontroller, at du vælger det korrekte certifikat sendt af et nøglecenter, der er tillid til.
	Årsag: Den fil, du har importeret, er for stor. Den maksimale filstørrelse er 5 KB. **Afhjælpning:** Hvis du vælger den korrekte fil, kan certifikatet være beskadiget eller bearbejdet.
	Årsag: Kæden i certifikatet er ugyldig. **Afhjælpning:** Set nøglecenterets websted for at få flere oplysninger om certifikatet.
Cannot use the Server Certificates that include more than three CA certificates.	**Årsag:** Certifikatet i PKCS#12-format indeholder mere end 3 CA-certifikater. **Afhjælpning:** Importer hvert certifikat konverteret fra PKCS#12-format til PEM-format, eller importer certifikatfilen i PKCS#12-format, der indeholder op til 2 CA-certifikater.
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**Årsag:** Certifikatet er forældet. **Afhjælpning:** ❏ Hent og importer det nye certifikat, hvis certifikatet er udløbet. ❏ Hvis certifikatet ikke er forældet, skal du kontrollere, at scannerens dato og klokkeslæt er indstillet korrekt.
Private key is required.	**Årsag:** Der er ingen parret privat nøgle med certifikatet. **Afhjælpning:** ❏ Hvis certifikatet er i PEM/DER-format og hentes fra en CSR vha. en computer, skal du angive den private nøglefil. ❏ Hvis certifikatet er i PKCS#12-format og hentes fra en CSR vha. en computer, skal du oprette en fil, der indeholder den private nøgle.
	Årsag: Du har genimporteret det PEM/DER-certifikat, der blev hentet fra en CSR vha. Web Config. **Afhjælpning:** Hvis certifikatet er i PEM/DER-format og er hentet fra en CSR vha. Web Config, kan du kun importere det én gang.

Meddelelser	Årsag/Afhjælpning
Setup failed.	**Årsag:** Kan ikke afslutte konfigurationen, fordi kommunikationen mellem scanneren og computeren mislykkedes, eller filen kan ikke læses pga. fejl. **Afhjælpning:** Importer filen igen, når du har kontrolleret den angivne fil og kommunikationen.

Relaterede oplysninger

➡ "Om digitalt certifikat" på side 63

Sletning af et CA-signeret certifikat ved en fejl

Er der en backup-fil for certifikatet?

Importer certifikatet igen, hvis du har backup-filen.

Hvis du henter et certifikat vha. en CSR, der er oprettet i Web Config, kan du ikke importere et slettet certifikat igen. Opret en CSR, og hent et nyt certifikat.

Relaterede oplysninger

➡ "Sletning af et CA-signeret certifikat" på side 67

➡ "Import af et CA-signeret certifikat" på side 65