

Nätverkshandbok

Innehållsförteckning

Innehållsförteckning

Upphovsrätter

Varumärken

Om den här handboken

Varumärken och symboler.	6
Beskrivningar som används i den här användarhandboken.	6
Referenser för operativsystem.	6

Introduktion

Manuell komponent.	8
Definition av termer som används i den här handboken.	8

Förberedelse

Flöde för skrivarinställningar.	10
Introduktion till skrivaranslutning.	10
Server-/klientanslutningsinställningar.	11
Peer to Peer-anslutningsinställningar.	11
Förbereda anslutningen för ett nätverk.	11
Samla information i anslutningsinställningarna.	11
Skrivarspecifikationer.	12
Typ av IP-adresstilldelning.	12
Metod för inställning av nätverksanslutning.	12
Installera EpsonNet Config.	13
Kör EpsonNet Config.	13

Anslutning

Ansluta till nätverket.	14
Ansluta till LAN.	14
Tilldela en IP-adress med EpsonNet Config.	14
Ansluta till nätverket med installationsprogrammet.	18

Funktionsinställningar

Web Config (Webbsida för enhet).	20
Om Web Config.	20

Öppna Web Config.	20
Använda utskriftsfunktionerna.	21
Krav för utskrift över ett nätverk.	21
Inställning av skrivardrivrutinen med server-/klientanslutning.	21
Skrivardrivrutinsinställningar för Peer to Peer-anslutning.	26

Säkerhetsinställningar

Säkerhetsinställningar och förebyggande av fara	28
Säkerhetsfunktionsinställningar.	29
Konfigurera administratörslösenord.	29
Konfigurera administratörslösenord med Web Config.	29
Kontrollera protokoll och tjänster.	30
Kontrollera protokoll.	30
SSL-/TLS-kommunikation med skrivaren.	34
Om digital certifiering.	34
Hämta och importera ett CA-signerat certifikat.	35
Radera ett CA-signerat certifikat.	38
Uppdatera ett självsignerat certifikat.	39
Krypterad kommunikation med IPsec/IP Filtering.	40
Om IPsec/IP Filtering.	40
Konfigurera standardpolicy.	40
Konfigurera Gruppolicy.	42
Exempel på konfigurering av IPsec/IP Filtering.	47
Använda SNMPv3-protokoll.	48
Om SNMPv3.	48
Konfigurera SNMPv3.	48

Lösa problem

Kontrollera loggen för server- och nätverksenheten.	51
Skriva ut ett statusark för nätverket.	51
Initiera nätverksinställningar.	51
Återställa nätverksinställningar från skrivaren	51
Återställa nätverksinställningar med EpsonNet Config.	51
Kontrollera kommunikationen mellan enheter och datorer.	52

Innehållsförteckning

Kontrollera anslutningen med Ping-kommandot.	52
Problem att använda nätverksprogram.	53
Kan inte öppna Web Config.	53
Modellnamn och/eller IP-adress visas inte i EpsonNet Config.	54
Lösa problem med avancerad säkerhet.	54
Återställa säkerhetsinställningarna.	54
Inaktivering av säkerhetsfunktionen från skrivaren.	54
Återställa säkerhetsfunktionen med Web Config.	55
Problem att använda funktionerna för nätverkssäkerhet.	55
Problem att använda ett digitalt certifikat.	57

Bilaga

Introduktion till nätverksmjukvara.	61
Epson Device Admin.	61
EpsonNet Print.	61
EpsonNet SetupManager.	61

Upphovsrätter

Upphovsrätter

Ingen del av denna publikation får återges, lagras i ett återvinningssystem eller överföras i någon form eller på något sätt, vare sig elektroniskt, mekaniskt, genom fotokopiering, inspelning eller på något annat sätt, utan föregående skriftligt tillstånd från Seiko Epson Corporation. Inget patentansvar antages vad gäller användandet av informationen häri. Ansvar antages ej heller vad gäller skador orsakade av användandet av informationen häri. Informationen som anges här är endast utformad för användning med den här Epson-produkten. Epson ansvarar inte för att uppgifterna är tillämpliga på andra produkter.

Varken Seiko Epson Corporation eller dess dotterbolag påtar sig något ansvar gentemot köparen av produkten eller tredje part för skador, förluster, kostnader eller utgifter som köparen eller tredje part har ådragit sig till följd av olyckshändelse, felaktig användning eller missbruk av produkten eller ej godkända modifieringar, reparationer eller ändringar av produkten eller (gäller ej i USA) underlåtenhet att följa Seiko Epson Corporation användnings- och underhållsanvisningar.

Seiko Epson Corporation och dess dotterbolag skall inte hållas ansvariga för skador eller problem som uppstår vid användning av eventuella tillval eller förbrukningsartiklar än sådana som har märkts med Original Epson Products (originalprodukter från Epson) eller Epson Approved Products by (av Epson godkända produkter) Seiko Epson Corporation.

Seiko Epson Corporation skall inte hållas ansvarigt för skador som uppstår till följd av elektromagnetiska störningar som beror på att andra gränssnittskablar än de som är märkta Epson Approved Products by (Epson-godkända produkter) av Seiko Epson Corporation har använts.

© 2017 Seiko Epson Corporation

Innehållet i den här handboken och specifikationerna för den här produkten kan ändras utan förvarning.

Varumärken

Varumärken

- EPSON® är ett registrerat varumärke och EPSON EXCEED YOUR VISION eller EXCEED YOUR VISION är ett varumärke som tillhör Seiko Epson Corporation.
- Epson Scan 2-programvaran är delvis baserat på arbetet från Independent JPEG Group.
- Google Cloud Print™, Chrome™, Chrome OS™, och Android™ är varumärken som tillhör Google Inc.
- Microsoft®, Windows®, Windows Server® och Windows Vista® är registrerade varumärken som tillhör Microsoft Corporation.
- IBM är ett registrerat varumärke som tillhör International Business Machines Corporation.
- Allmänt meddelande: Övriga produktnamn som förekommer i detta dokument används endast i identifieringssyfte och kan vara varumärken som tillhör respektive ägare. Epson fransäger sig all rätt till dessa varumärken.

Om den här handboken

Om den här handboken

Varumärken och symboler

**Varning!**

Anvisningarna måste efterföljas noga för att undvika kroppsskador.

**Viktigt!**

Anvisningar som måste följas för att undvika skador på utrustningen.

Obs!

Anvisningar som innehåller användbara tips och restriktioner för utskriftsåtgärder.

Relaterad information

➔ Klicka på den här ikonen om du vill läsa relaterad information.

Beskrivningar som används i den här användarhandboken

Skrivarillustrationerna som används i den här användarhandboken är endast exempel. Det kan finnas små skillnader mellan modellerna, men driftsättet är det samma.

Referenser för operativsystem

Windows

I den här användarhandboken syftar termer som "Windows 10", "Windows 8.1", "Windows 8", "Windows 7", "Windows Vista", "Windows XP", "Windows Server 2012 R2", "Windows Server 2012", "Windows Server 2008 R2", "Windows Server 2008", "Windows Server 2003 R2" och "Windows Server 2003" på följande operativsystem. Dessutom används "Windows" som referens till alla 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

Om den här handboken

- 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

Introduktion

Manuell komponent

Denna handbok förklarar hur man ansluter skrivaren till nätverket och innehåller information om hur man utför inställningarna för att använda funktionerna.

Se *Användarhandbok* för funktionsanvändningsinformation.

Förberedelse

Förklarar hur man ställer in enheter och programvaran som används för hantering.

Anslutning

Förklarar hur man ansluter en skrivare till nätverket.

Funktionsinställningar

Förklarar utskriftsinställningarna.

Säkerhetsinställningar

Förklarar säkerhetsinställningar, som t.ex. lösenordsinställningar för administratör och protokollstyrning.

Lösa problem

Beskriver återställning av inställningar och felsökning av nätverket.

Definition av termer som används i den här handboken

Följande termer används i den här handboken.

Administratör

Personen som ansvarar för installation och konfiguration av enheten eller nätverket i ett kontor eller en organisation. För små organisationer kan den här personen ansvara för både enhets- och nätverksadministration. För stora organisationer har administratörer behörighet för nätverk eller enheter i gruppenheten för en avdelning eller division och nätverksadministratörerna ansvarar för kommunikationsinställningarna utöver organisationen, såsom Internet.

Nätverksadministratör

Personen som ansvarar för att styra nätverkskommunikationen. Personen som konfigurerar router, proxyserver, DNS-server och mejlserver för att styra kommunikationen genom Internet eller nätverket.

Användare

Personen som använder enheterna, såsom skrivare eller skannrar.

Server/klientanslutning (skrivardelning med the Windows-server)

Anslutningen som indikerar att skrivaren är ansluten till Windows-servern genom nätverket eller via USB-kabeln, och utskriftsköns inställning på servern kan delas. Kommunikationen mellan skrivaren och datorn går via servern och skrivaren kontrolleras på servern.

Peer to peer-anslutning (direkt utskrift)

Anslutningen som indikerar att skrivaren och datorn är anslutna till nätverket genom hubben eller åtkomstpunkten, och utskriftsjobbet, kan köras direkt från datorn.

Introduktion

Web Config (enhetens webbsida)

Webbservern som är integrerad i enheten. Kallas för Web Config. Du kan kontrollera och ändra enhetens status med webbläsaren.

Utskriftskö

För Windows visas ikonen för varje port i **Device and Printer (Enhet och skrivare)**, exempelvis skrivare. Två eller fler ikoner skapas även för en enkel enhet om enheten är ansluten till nätverket med två eller fler portar, såsom standard TCP/IP.

Verktyg

En generisk term för programvaran för att konfigurera eller hantera en enhet som t.ex. Epson Device Admin, EpsonNet Config, EpsonNet SetupManager osv.

ASCII (American Standard Code for Information Interchange)

En av standardteckenkoderna. 128 tecken definieras, inklusive bokstäver (a–z, A–Z), arabiska siffror (0–9), symboler, mellanslag och kontrolltecken. När "ASCII" beskrivs i den här handboken indikerar det 0x20–0x7E (hexadecimalnummer) som beskrivs nedan och involverar inte kontrolltecken.

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

* Mellanslag.

Unicode (UTF-8)

En internationell standardkod, som täcker de främsta globala språken. När "UTF-8" beskrivs i den här handboken indikerar det teckenkoder i UTF-8-format.

Förberedelse

Detta kapitel förklarar vad som behöver förberedas innan inställningarna utförs.

Flöde för skrivarinställningar

Du utför anslutningsinställningar för nätverket och kör en initial konfiguration så att skrivaren är tillgänglig för användare.

- 1** Förberedelse
 - Samla in information om anslutningsinställningar
 - Beslut för anslutningsmetod
- 2** Anslutning
 - Utför en nätverksanslutning med EpsonNet Config
- 3** Konfigurera utskrifter
 - Skrivardrivrutinsinställningar
- 4** Säkerhetsinställningar
 - Administratörsinställningar
 - SSL/TLS
 - Protokollstyrning
 - IPsec/IP-filtrering

Relaterad information

- ➔ ["Anslutning" på sidan 14](#)
- ➔ ["Funktionsinställningar" på sidan 20](#)
- ➔ ["Säkerhetsinställningar" på sidan 28](#)

Introduktion till skrivaranslutning

Följande två metoder är tillgängliga för skrivarens nätverk direkt via båda metoderna.

- Server/klientanslutning (skrivardelning med Windows-server)
- Peer to peer-anslutning (direkt utskrift)

Relaterad information

- ➔ ["Server-/klientanslutningsinställningar" på sidan 11](#)
- ➔ ["Peer to Peer-anslutningsinställningar" på sidan 11](#)

Förberedelse

Server-/klientanslutningsinställningar

Anslutningssätt:

Anslut skrivaren till nätverket via hubben (L2-brytare). Du kan även ansluta skrivaren direkt till servern med en USB-kabel.

Skrivardrivrutin:

Installera skrivardrivrutinen på Windows-servern, beroende på klientdatorernas OS. Genom att öppna Windows-servern och länka skrivaren installeras skrivardrivrutinen på klientdatorn och kan användas.

Funktioner:

- Hantera skrivaren och skrivardrivrutinen gemensamt.
- Beroende på serverspecifikationer kan det ta tid att starta utskriftsjobbet eftersom alla utskriftsjobb går genom utskriftsservern.
- Du kan inte skriva ut när Windows-servern stängts av.

Relaterad information

➔ ["Definition av termer som används i den här handboken" på sidan 8](#)

Peer to Peer-anslutningsinställningar

Anslutningssätt:

Anslut skrivaren till nätverket via hubben (L2-switch).

Skrivardrivrutin:

Installera skrivardrivrutinen på varje klientdator. Den kan levereras som ett paket med EpsonNet SetupManager eller automatiskt genom att använda gruppolicyn för Windows-servern.

Funktioner:

- Utskriftsjobbet startar omedelbart, eftersom det skickas direkt till skrivaren.
- Du kan skriva ut så länge skrivaren körs.

Relaterad information

➔ ["Definition av termer som används i den här handboken" på sidan 8](#)

Förbereda anslutningen för ett nätverk

Samla information i anslutningsinställningarna

Du behöver en IP-adress, gateway-adress etc. för nätverksanslutningen. Kontrollera följande i förväg.

Förberedelse

Avdelningar	Alternativ	Obs
Enhetsanslutningsmetod	<input type="checkbox"/> Ethernet	Använd en kategori 5e- eller högre STP-kabel (Shielded twisted pair).
LAN-anslutningsinformation	<input type="checkbox"/> IP-adress <input type="checkbox"/> Nätmask <input type="checkbox"/> Standard-gateway	Om du automatiskt konfigurerar IP-adressen med DHCP-funktionen för routern krävs det inte.
DNS-serverinformation	<input type="checkbox"/> IP-adress för primär DNS <input type="checkbox"/> IP-adress för sekundär DNS	Om du använder en statisk IP-adress som IP-adress, ska du konfigurera DNS-servern. Konfigurera automatiskt vid tilldelning av IP-adresser med DHCP-funktionen och när DNS-servern inte kan tilldelas automatiskt.

Skrivarspecifikationer

Specifikationen som skrivaren stöder i standard- eller anslutningsläge, se *Användarhandbok*.

Typ av IP-adresstilldelning

Det finns två typer för tilldelning av en IP-adress till skrivaren.

Statisk IP-adress:

Tilldela förutbestämd unik IP-adress för skrivaren.

IP-adressen ändras inte även när skrivaren slås på eller routern stängs av, så du kan hantera enheten via IP-adressen.

Den här typen är tillämplig för ett nätverk där många skrivare hanteras, såsom ett stort företag eller en skola.

Automatisk tilldelning via DHCP-funktion:

Den korrekta IP-adressen tilldelas automatiskt när kommunikationen mellan skrivaren och routern som stöder DHCP-funktion fungerar.

Om det är besvärligt att ändra IP-adressen för en viss enhet, reservera IP-adressen i förväg och tilldela den sedan.

Obs!

För utskriftsköns port kan du välja protokoll som automatiskt kan detektera IP-adressen, såsom *EpsonNet Print Port*.

Metod för inställning av nätverksanslutning

För anslutningsinställningar för skrivarens IP-adress, nätmask och standardgateway, fortsätt enligt följande.

Använda EpsonNet Config:

Använd EpsonNet Config från administratörens dator. Du kan konfigurera många skrivare, men de behöver anslutas fysiskt med Ethernet-kabeln före inställning. Om du kan bygga en Ethernet för inställningen, och du ställer in nätverksinställningar för skrivaren och sedan ansluter skrivaren till det vanliga nätverket, kan du hålla säkerhetsrisken låg.

Förberedelse

Använda installationsprogrammet:

Om installationsprogrammet används ställs skrivarens och klientdatorns nätverk in automatiskt. Inställningarna är tillgängliga enligt installationsprogrammets instruktioner, även om du inte har djupgående kunskaper om nätverket. Det här rekommenderas vid inställning av skrivaren och några klientdatorer genom att använda server-/klientanslutning (dela skrivaren med Windows-servern).

Relaterad information

- ➔ ["Tilldela en IP-adress med EpsonNet Config" på sidan 14](#)
- ➔ ["Ansluta till nätverket med installationsprogrammet" på sidan 18](#)

Installera EpsonNet Config

Hämta EpsonNet Config från Epson-supportens webbplats och installera det sedan genom att följa instruktionerna på skärmen.

Kör EpsonNet Config

Välj **All Programs (Alla program) > EpsonNet > EpsonNet Config SE > EpsonNet Config**.

Obs!

Om en brandväggsvarning visas, tillåt åtkomst för EpsonNet Config.

Anslutning

I det här kapitlet beskrivs miljön eller proceduren för att ansluta skrivaren till nätverket.

Ansluta till nätverket

Ansluta till LAN



Anslut skrivaren till nätverket via Ethernet.

Relaterad information

➔ [”Ansluta till nätverket med installationsprogrammet”](#) på sidan 18

Tilldela en IP-adress med EpsonNet Config

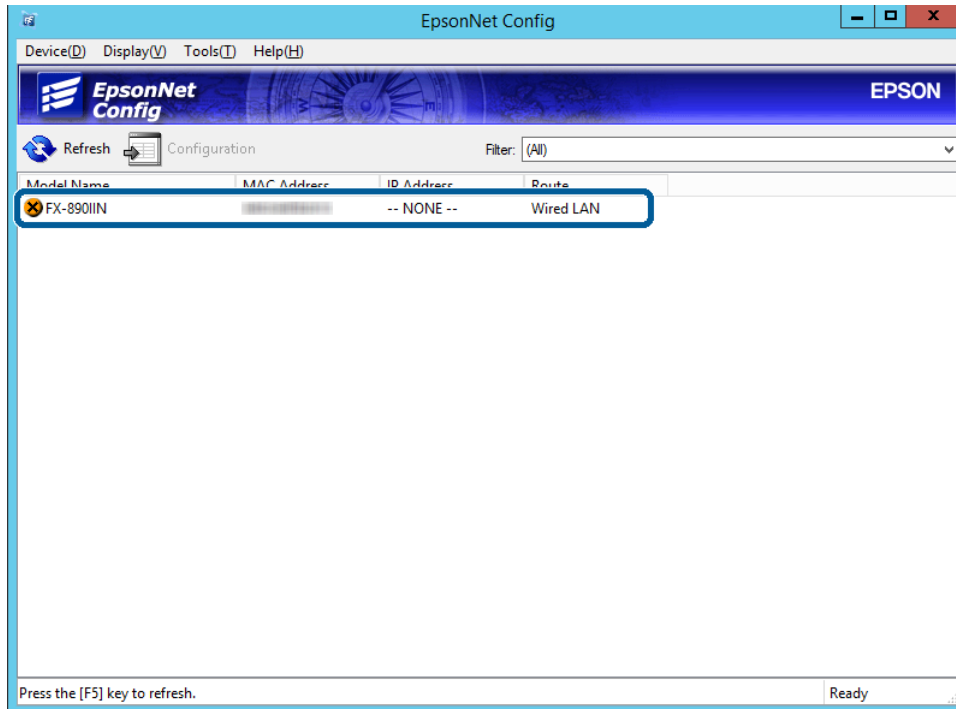
Tilldela en IP-adress till skrivaren med EpsonNet Config.

- 1 Starta skrivaren.
- 2 Anslut skrivaren till nätverket med en Ethernet-kabel.
- 3 Starta EpsonNet Config.
En lista över skrivarna i nätverket visas. Det kan ta en stund innan de visas.
- 4 Dubbelklicka på  skrivaren som du vill tilldela.
Om du ansluter skrivaren till ett nätverk med en tillgänglig DHCP-funktion, tilldelas IP-adressen via DHCP-funktionen och sedan visas .

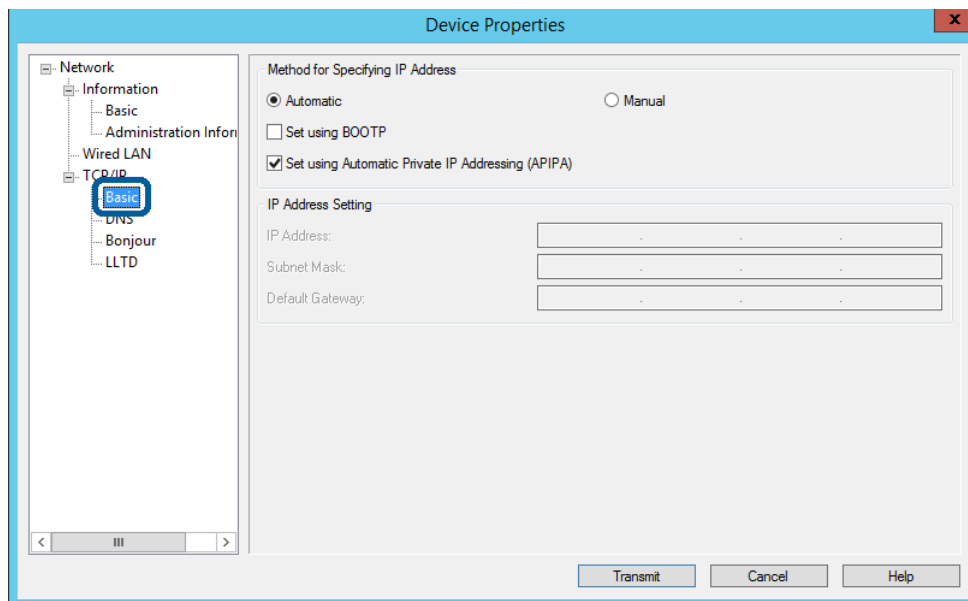
Obs!

- Om du har anslutit flera skrivare av samma modell kan du identifiera skrivaren med MAC-adressen.
- Efter att skrivaren är ansluten till nätverket kan du ändra IP-adressens tilldelningsmetod.

Anslutning

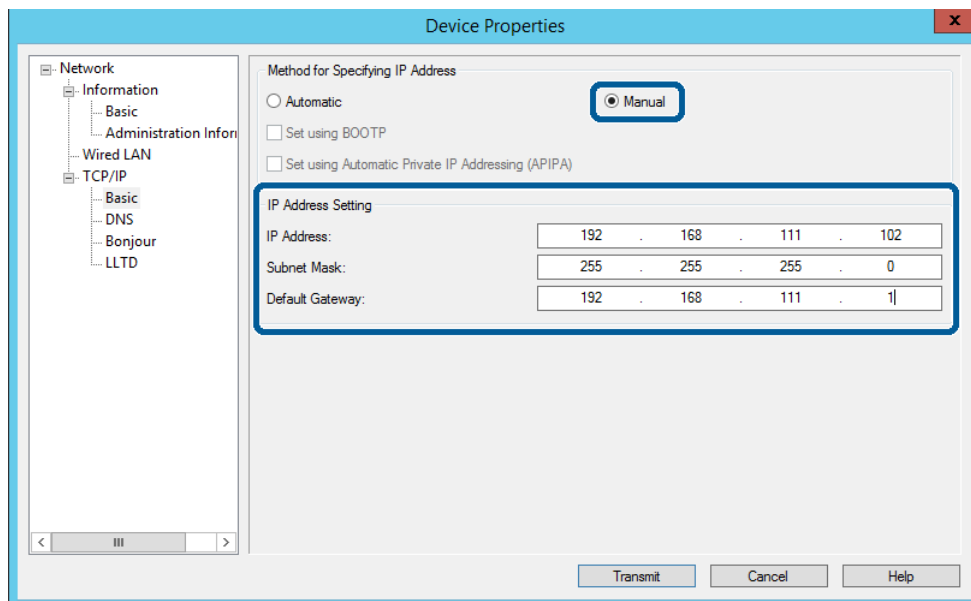
**5**

Välj **Network (Nätverk) > TCP/IP > Basic (Grundläggande)**.



Anslutning

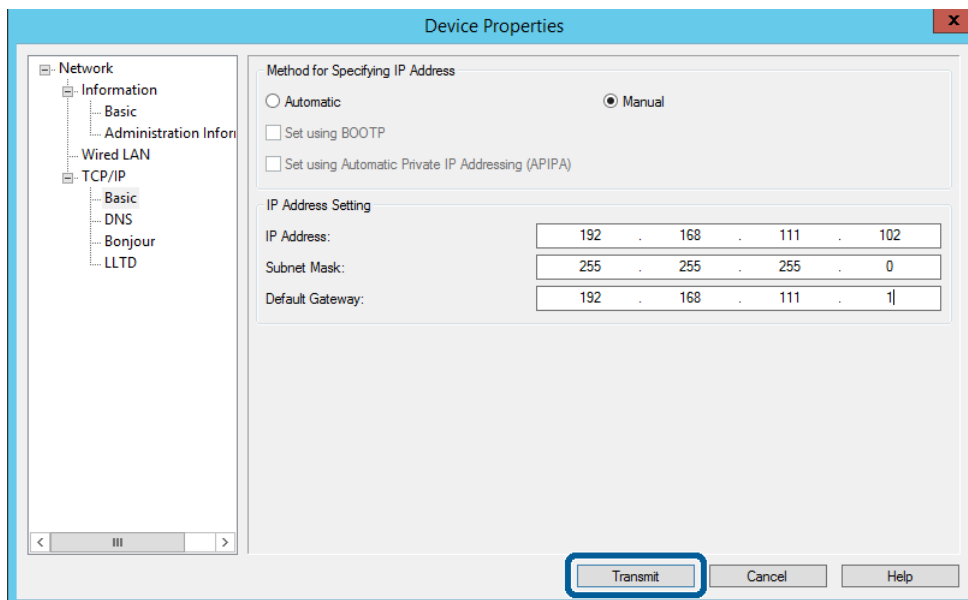
- 6** Ange adresser för **IP Address (IP-adress)**, **Subnet Mask (Nätmask)** och **Default Gateway (Standard-gateway)**.



Obs!

- Ange en fast adress när du ansluter skrivaren till ett säkert nätverk.
- I menyn **TCP/IP** kan du utföra DNS-inställningar på **DNS**-skärmen.

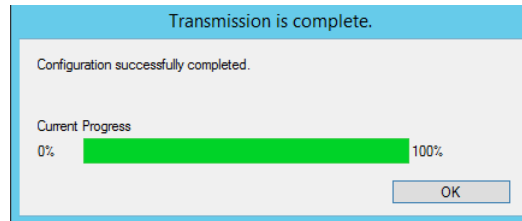
- 7** Klicka på **Transmit (Överför)**.



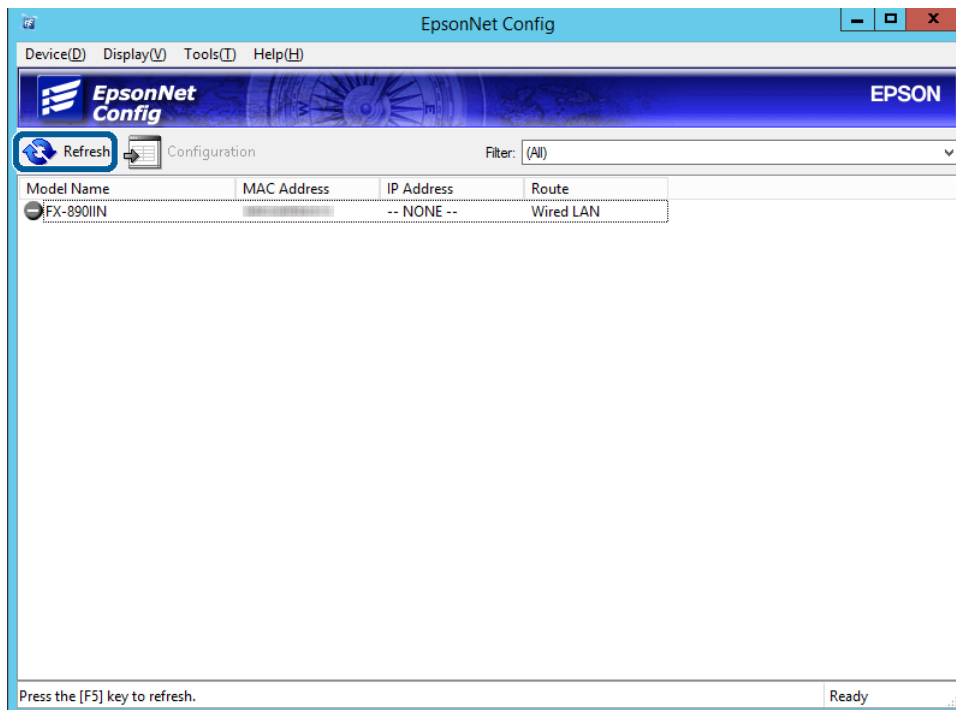
- 8** Tryck på **OK** på bekräftelseskärmen.

Anslutning

9 Klicka på **OK**.

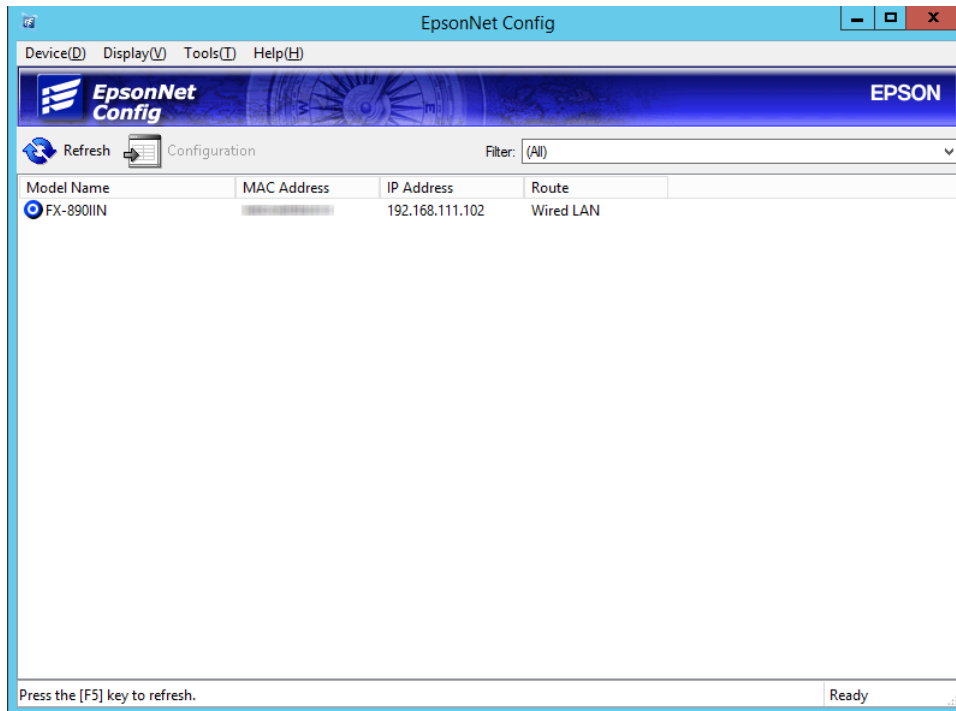


10 Klicka på **Refresh (Uppdatera)**.



Anslutning

Kontrollera att en IP-adress har tilldelats.



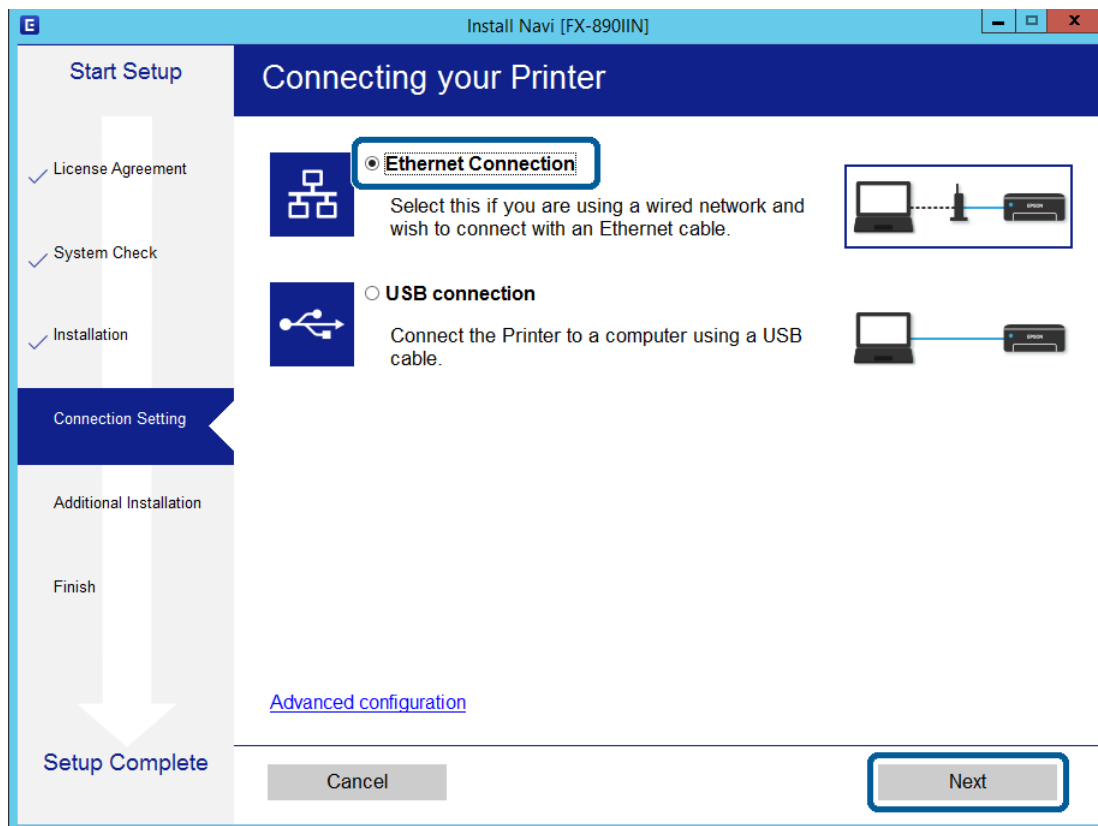
Ansluta till nätverket med installationsprogrammet

Vi rekommenderar att du använder installationsprogrammet för att ansluta skrivaren till en dator.

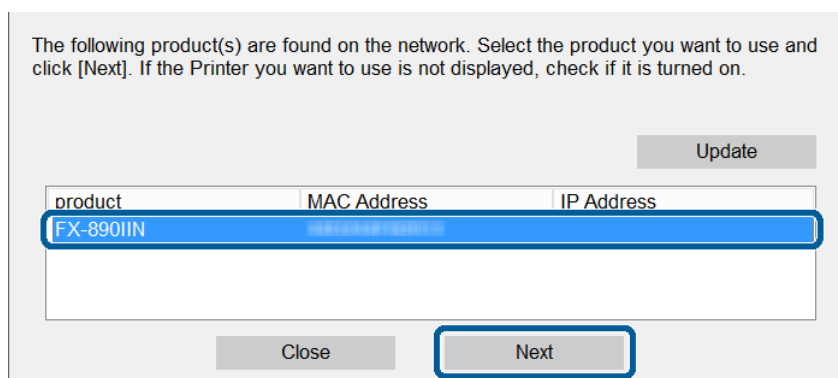
- 1 Sätt i programvaruskivan i datorn och följ sedan instruktionerna på skärmen.

Anslutning

- 2 Följ instruktionerna på skärmen tills följande skärm visas, välj **Ethernet Connection (Ethernet-anslutning)** och klicka sedan på **Next (Nästa)**.



Om du ansluter skrivaren till nätverket via en Ethernet-kabel visas följande skärm. Välj skrivare och klicka sedan på **Next (Nästa)**.



- 3 Följ instruktionerna på skärmen.

Funktionsinställningar

I det här kapitlet beskrivs de första inställningarna som måste utföras för att använda varje funktion på enheten.

I det här kapitlet beskrivs proceduren för att utföra inställningar från administratörens dator med Web Config.

Web Config (Webbsida för enhet)

Om Web Config

Web Config är ett webbläsarbaserat program för konfigurering av skrivarens inställningar.

För att öppna Web Config måste du först tilldela en IP-adress till skrivaren.

Obs!

Du kan spärra inställningarna genom att konfigurera ett administratörlösenord på skrivaren.

Öppna Web Config

Det finns två metoder för att öppna Web Config. JavaScript måste vara aktiverat i webbläsaren.

Ange IP-adress

Starta EpsonNet Config och dubbelklicka sedan på skrivaren i listan.

Ange skrivarens IP-adress i en webbläsare. När Web Config öppnas via HTTPS, visas ett varningsmeddelande i webbläsaren eftersom ett självsignerat certifikat som lagrats i skrivaren används.

- Åtkomst via HTTPS
IPv4: `https://<skrivarens IP-adress>` (utan `< >`)
IPv6: `https://[skrivarens IP-adress]` (med `[]`)
- Åtkomst via HTTP
IPv4: `http://<skrivarens IP-adress>` (utan `< >`)
IPv6: `http://[skrivarens IP-adress]` (med `[]`)

Obs!

- Exempel*
IPv4:
`https://192.0.2.111/`
`http://192.0.2.111/`
IPv6:
`https://[2001:db8::1000:1]/`
`http://[2001:db8::1000:1]/`
- Om skrivarens namn är registrerat med DNS-servern kan du använda skrivarnamnet i stället för skrivarens IP-adress.
- Alla menyer visas inte när Web Config öppnas via HTTP. För att se alla menyer, öppna Web Config via HTTPS.

Funktionsinställningar

Relaterad information

- ➔ ”SSL-/TLS-kommunikation med skrivaren” på sidan 34
- ➔ ”Om digital certifiering” på sidan 34

Använda utskriftsfunktionerna

Gör det möjligt att använda skrivarens utskriftsfunktion.

Krav för utskrift över ett nätverk

Följande krävs för utskrift över ett nätverk. Du kan konfigurera följande inställningar med skrivardrivrutinen och funktionerna i operativsystemet.

- Installera skrivardrivrutinen
- Skicka utskriftskön till en dator
- Konfigurera porten till ett nätverk

Inställning av skrivardrivrutinen med server-/klientanslutning

Konfigurera skrivaren för att aktivera utskrift från en dator som tidigare konfigurerats som utskriftsserver och dela skrivaren. Installera skrivardrivrutinen för både servern och klienten på utskriftsservern. Om installationsprogrammet används görs inställning av skrivarens nätverk eller dator, installation av drivrutin och utskriftskön automatiskt.

Ställa in TCP/IP-standardportar - Windows

Ställ in TCP/IP-standardporten på utskriftsservern, och skapa utskriftskön för nätverksutskrift.

- 1 Öppna skärmen för enheter och skrivare.
 - Windows 10/Windows Server 2016
Högerklicka på startknappen eller tryck ned och håll in den och välj sedan **Control Panel (Kontrollpanelen) > Hardware and Sound (Hårdvara och ljud)** i **Devices and Printers (Enheter och skrivare)**.
 - Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
Desktop (Skrivbordet) > Settings (Inställningar) > Control Panel (Kontrollpanelen) > Hardware and Sound (Maskinvara och ljud) eller **Hardware (Maskinvara) > Devices and Printers (Enheter och skrivare)**.
 - Windows 7/Windows Server 2008 R2
Klicka på start > **Control Panel (Kontrollpanel) > Hardware and Sound (Maskinvara och ljud)** (eller **Hardware (Maskinvara) > Devices and Printers (Enheter och skrivare)**).
 - Windows Vista/Windows Server 2008
Klicka på Start > **Control Panel (Kontrollpanelen) > Hardware and Sound (Maskinvara och ljud) > Printers (Skrivare)**.

Funktionsinställningar

- ❑ Windows XP/Windows Server 2003 R2/Windows Server 2003
Klicka på startknappen och välj **Control Panel (Kontrollpanelen) > Printers and Other Hardware (Skrivare och annan hårdvara) > Printers and Faxes (Skrivare och faxar)**.

2

Lägg till en skrivare.

- ❑ Windows 10/Windows 8.1/Windows 8/Windows Server 2016/Windows Server 2012 R2/Windows Server 2012
Klicka på **Add printer (Lägg till skrivare)** och markera **The printer that I want isn't listed (Skrivaren jag vill ha anges inte)**.
- ❑ Windows 7/Windows Server 2008 R2
Klicka på **Add printer (Lägg till skrivare)**.
- ❑ Windows Vista/Windows Server 2008
Klicka på **Install Printer (Installera skrivare)**.
- ❑ Windows XP/Windows Server 2003 R2/Windows Server 2003
Klicka på **Install Printer (Installera skrivare)** och sedan på **Next (Nästa)**.

3

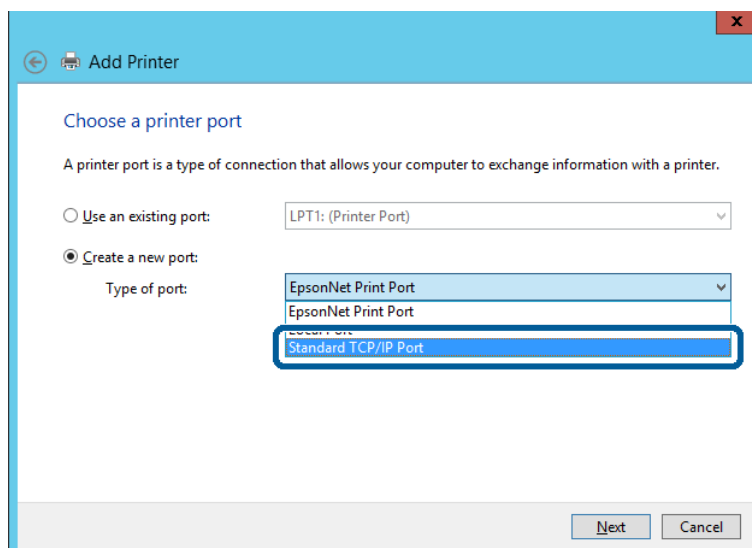
Lägg till en lokal skrivare.

- ❑ Windows 10/Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
Välj **Add a local printer or network printer with manual settings (Lägg till en lokal skrivare eller nätverksskrivare med manuella inställningar)** och klicka på **Next (Nästa)**.
- ❑ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008
Klicka på **Add a local printer (Lägg till en lokal skrivare)**.
- ❑ Windows XP/Windows Server 2003 R2/Windows Server 2003
Välj **Local printer attached to this computer (Lokal skrivare ansluten till den här datorn)** och klicka på **Next (Nästa)**.

4

Välj **Create a new port (Skapa en ny port)**, välj **Standard TCP/IP Port (Standard-TCP/IP-port)** som porttyp och klicka på **Next (Nästa)**.

För Windows XP/Windows Server 2003 R2/Windows Server 2003, klicka på **Next (Nästa)** på skärmen **Add Standard TCP/IP Printer Port Wizard (Guiden Lägg till standard-TCP/IP-skrivarport)**.



Funktionsinställningar

- 5** Ange skrivarens IP-adress eller skrivarnamn i **Host Name or IP Address (Värddatornamn eller IP-adress)** eller **Printer Name or IP Address (Skrivarnamn eller IP-adress)** och klicka på **Next (Nästa)**.

Ändra inte **Port name (Portnamn)**.

Klicka på **Continue (Fortsätt)** när skärmen **User Account Control (User Account Control)** visas.

För Windows XP/Windows Server 2003 R2/Windows Server 2003, klicka på **Done (Klar)** på skärmen **Standard TCP/IP Printer Port (Standard-TCP/IP-skrivarport)**.

Obs!

Om du specificerar skrivarnamnet i nätverket där namnmatchning är tillgängligt spåras IP-adressen även om skrivarens IP-adress har ändrats av DHCP. Det går att kontrollera skrivarens namn på nätverkets statusskärm, på skrivarens kontrollpanel eller genom att skriva ut ett statusark för nätverket.

- 6** Ställ in skrivardrivrutinen.

- Om skrivardrivrutinen redan är installerad:
Välj **Manufacturer (Tillverkare)** och **Printers (Skrivare)**. Klicka på **Next (Nästa)**.
- Om skrivardrivrutinen inte är installerad:
Klicka på **Have Disc (Har skiva)** och sätt in programvaruskivan som medföljde skrivaren. Klicka på **Browse (Bläddra)** och välj mappen på skivan som innehåller skrivardrivrutinen. Se till att du väljer rätt mapp. Mappens placering kan variera beroende på ditt operativsystem.
32-bitars version av Windows: WINX86
64-bitars version av Windows: WINX64

- 7** Följ instruktionerna på skärmen.

För Windows XP/Windows Server 2003 R2/Windows Server 2003 är konfigurationen slutförd. För Windows Vista/Windows Server 2008 och senare, kontrollera portkonfigurationen.

Vid användning av skrivaren under server-/klientanslutningen (skrivardelning med Windows-server), görs konfiguration av skrivardelning efter detta.

Funktionsinställningar

Relaterad information

➔ ”Dela skrivaren” på sidan 25

Kontrollera portkonfigurationen - Windows

Kontrollera om rätt port är inställd för utskriftskön.

1

Öppna skärmen för enheter och skrivare.

- Windows 10/Windows Server 2016
Högerklicka på startknappen eller tryck ned och håll in den och välj sedan **Control Panel (Kontrollpanelen) > Hardware and Sound (Hårdvara och ljud) i Devices and Printers (Enheter och skrivare)**.
- Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
Desktop (Skrivbordet) > Settings (Inställningar) > Control Panel (Kontrollpanelen) > Hardware and Sound (Maskinvara och ljud) eller Hardware (Maskinvara) > Devices and Printers (Enheter och skrivare).
- Windows 7/Windows Server 2008 R2
Klicka på start > **Control Panel (Kontrollpanel) > Hardware and Sound (Maskinvara och ljud) (eller Hardware (Maskinvara)) > Devices and Printers (Enheter och skrivare)**.
- Windows Vista/Windows Server 2008
Klicka på Start > **Control Panel (Kontrollpanelen) > Hardware and Sound (Maskinvara och ljud) > Printers (Skrivare)**.

2

Öppna skärmen för skrivaregenskaper.

- Windows 10/Windows 8.1/Windows 8/Windows 7/Windows Server 2016/Windows Server 2012 R2/Windows Server 2012/ Windows Server 2008 R2
Högerklicka på skrivarikonen och klicka på **Printer properties (Skrivaregenskaper)**.
- Windows Vista
Högerklicka på skrivarikonen och välj **Run as administrator (Kör som administratör) > Properties (Egenskaper)**.
- Windows Server 2008
Högerklicka på skrivarikonen och klicka på **Properties (Egenskaper)**.

3

Klicka på fliken **Ports (Portar)**, välj **Standard TCP/IP Port (Standard-TCP/IP-port)** och klicka på **Configure Port (Konfigurera port)**.

4

Kontrollera portkonfigurationen.

- För RAW
Kontrollera att **Raw** är valt i **Protocol (Protokoll)** och klicka på **OK**.
- För LPR
Kontrollera att **LPR** är valt i **Protocol (Protokoll)**. Ange "PASSTHRU" i **Queue name (Könamn)** från **LPR Settings (LPR-inställningar)**. Välj **LPR Byte Counting Enabled (Byte-räkning för LPR är aktiverad)** och klicka på **OK**.

Funktionsinställningar

Dela skrivaren

Vid användning av skrivaren under servern/klientanslutningen (skrivardelning med Windows-server), konfigureras skrivardelning från utskriftsservern.

- 1 Välj **Control Panel (Kontrollpanelen) > View devices and printers (Visa enheter och skrivare)** på utskriftsservern.
- 2 Högerklicka på skrivarikonen (utskriftskön) som du vill dela med och välj sedan **Printer Properties (Skrivaregenskaper) > fliken Sharing (Delning)**.
- 3 Välj **Share this printer (Dela den här skrivaren)** och ange sedan **Share name (Delningsnamn)**.
För Windows Server 2012, klicka på **Change Sharing Options (Ändra delningsalternativ)** och konfigurera sedan inställningarna.

Installera flera drivrutiner

Om Windows-versionerna för en server och klienterna skiljer sig åt rekommenderar vi att du installerar ytterligare drivrutiner till utskriftsservern.

- 1 Välj **Control Panel (Kontrollpanelen) > View devices and printers (Visa enheter och skrivare)** på utskriftsservern.
- 2 Högerklicka på skrivarikonen som du vill dela med klienterna och klicka på **Printer Properties (Skrivaregenskaper) > fliken Sharing (Delning)**.
- 3 Klicka på **Additional Drivers (Ytterligare drivrutiner)**.
För Windows Server 2012, klicka på **Change Sharing Options (Ändra delningsalternativ)** och konfigurera sedan inställningarna.
- 4 Välj Windows-versioner för klienterna och klicka på **OK**.
- 5 Välj informationsfil för skrivardrivrutinen (*.inf) och installera drivrutinen.

Relaterad information

➔ ["Använda en delad skrivare"](#) på sidan 25

Använda en delad skrivare

Administratören måste tala om datornamnet som tilldelats skrivarservern och hur den ska läggas till på klientdatorerna. Om extra drivrutiner inte har konfigurerats ännu ska du tala om för klienterna hur den delade skrivaren läggs till med **Devices and Printers (Enheter och skrivare)**.

Följ stegen nedan om extra drivrutiner redan har konfigurerats på skrivarservern:

- 1 Välj namnet som tilldelats skrivarservern i **Windows Explorer (Windows Utforskaren)**.
- 2 Dubbelklicka på skrivaren som du vill använda.

Funktionsinställningar

Relaterad information

- ➔ ”Dela skrivaren” på sidan 25
- ➔ ”Installera flera drivrutiner” på sidan 25

Skrivardrivrutinsinställningar för Peer to Peer-anslutning

För peer to peer-anslutning (direkt utskrift), måste skrivardrivrutinen installeras på varje klientdator.

Relaterad information

- ➔ ”Ställa in skrivardrivrutinen” på sidan 26

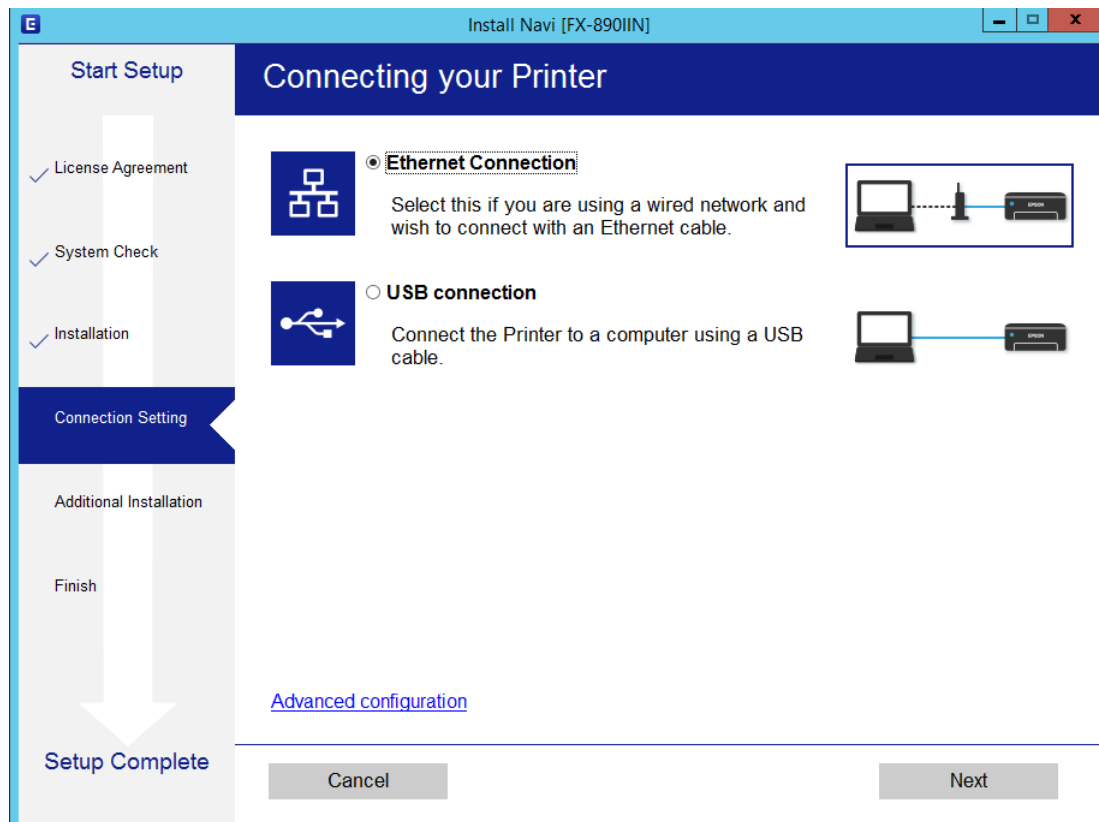
Ställa in skrivardrivrutinen

För små organisationer rekommenderar vi att du installerar skrivardrivrutinen på varje klientdator.

Obs!

När skrivaren används med många klientdatorer kan installationsdriftstiden minskas kraftigt genom att använda EpsonNet SetupManager och leverera drivrutinen som ett paket.

- 1 Kör installationsprogrammet.
- 2 Välj anslutningssätt för skrivaren och klicka sedan på **Next (Nästa)**.



Funktionsinställningar

Obs!

Om *Select Software Installation (Välj programvaruinstallation)* visas, välj *Change or re-set the connection method (Ändra eller återställa anslutningsmetod)* och klicka sedan på *Next (Nästa)*.

3

Följ instruktionerna på skärmen.

Relaterad information

➔ ["EpsonNet SetupManager"](#) på sidan 61

Säkerhetsinställningar

Detta kapitel förklarar säkerhetsinställningarna.

Säkerhetsinställningar och förebyggande av fara

När en enhet är ansluten till ett nätverk kan du öppna den från en fjärrstyrd plats. Dessutom kan många människor dela enheten, vilket är praktiskt vid förbättring av operationell effektivitet och bekvämlighet. Risker, såsom olaglig åtkomst, olaglig användning och modifiering av data ökar.

För att undvika dessa risker har Epson en rad olika säkerhetstekniker. Konfigurera enheten efter behov enligt miljövillkoren som har byggts in i kundens miljöinformation.

Funktionsnamn	Funktionstyp	Vad du kan konfigurera	Vad du kan förhindra
Konfiguration för administratörslösenord	Låser systeminställningarna, exempelvis anslutningskonfiguration för nätverk eller USB.	En administratör konfigurerar ett lösenord för enheten. Konfiguration eller uppdatering är tillgängligt överallt från Web Config och Epson Device Admin.	Förhindra olaglig läsning och ändring av information som finns lagrad i enheten, såsom ID, lösenord, nätverksinställningar och kontakter. Minskar även ett brett utbud av säkerhetsrisker, såsom informationsläckage för nätverksmiljön eller säkerhetspolicy.
Protokoll och tjänstekontroll	Kontrollerar protokoll och tjänster som ska användas för kommunikation mellan enheter och datorer, och aktiverar och inaktiverar funktioner, såsom utskrift.	Ett protokoll eller en tjänst som verkställs för funktioner tillåts eller förbjuds separat.	Genom att minska säkerhetsrisker som kan uppstå vid oavsiktlig användning där användare förhindras från att använda onödiga funktioner.
SSL/TLC-kommunikation	Kommunikationssökvägen för en dator och en skrivare krypteras med SSL-/TLS-kommunikation. Innehållet i kommunikationen skyddas av skivarinställningarna och av IPPS-protokollutskriften via en webb-läsare.	Få ett CA-signerat certifikat och importera det sedan till skrivaren.	Genom att rensa en identifiering av enheten med CA-signerad certifiering förhindras impersonifiering och obehörig åtkomst. Dessutom skyddas kommunikationsinnehållet i SSL/TLS och innehållsläckage förhindras för utskriftsdata och konfigurationsinformation.
IPsec/IP Filtering	Du kan göra inställningar för att tillåta beskärning och urklipp av data som kommer från en viss klient eller är av en viss typ. Eftersom IPsec skyddar data via IP-paketet (kryptering och autentisering), kan du säkert kommunicera osäkra utskriftsprotokoll och skanningprotokoll.	Skapa en grundläggande policy och individuell policy för att konfigurera klienten eller typen av data som kan få åtkomst till enheten.	Skydda från obehörig åtkomst och klåfingerskydd och störning av kommunikationsdata till enheten.

Säkerhetsinställningar

Funktionsnamn	Funktionstyp	Vad du kan konfigurera	Vad du kan förhindra
SNMPv3	Funktioner läggs till, såsom övervakning av anslutna enheter i nätverket, integriteten för data i SNMP-protokollet för styrning, kryptering, användarautentisering etc.	Aktivera SNMPv3 och konfigurera sedan autentisering och kryptering.	Se till att ändra inställningar via nätverket, med sekretess vid statusövervakning.

Relaterad information

- ➔ ["Konfigurera administratörslösenord" på sidan 29](#)
- ➔ ["Kontrollera protokoll och tjänster" på sidan 30](#)
- ➔ ["SSL-/TLS-kommunikation med skrivaren" på sidan 34](#)

Säkerhetsfunktionsinställningar

Vid inställning av IPsec/IP Filtring, rekommenderar vi att du får åtkomst till Web Config med SSL/TLS för att kommunicera inställningsinformation och minska säkerhetsrisker, såsom klåfingerskydd och avlyssning.

Konfigurera administratörslösenord

När du konfigurerar administratörslösenordet kan användare som inte är administratörer ändra inställningarna för systemadministration. Du kan ställa in och ändra administratörslösenord med Web Config.

Relaterad information

- ➔ ["Konfigurera administratörslösenord med Web Config" på sidan 29](#)

Konfigurera administratörslösenord med Web Config

Du kan ställa in administratörslösenord med Web Config.

- 1 Öppna Web Config och välj **Administrator Settings (Administratörsinställningar) > Change Administrator Password (Ändra Administratörslösenord)**.

Säkerhetsinställningar

- 2** Skriv ett lösenord i **New Password (Nytt Lösenord)** och **Confirm New Password (Bekräfta nytt Lösenord)**.

Om du vill ändra lösenordet till ett nytt anger du det aktuella lösenordet.

The screenshot shows the 'Administrator Settings > Change Administrator Password' page. On the left, there is a navigation menu with the following items: Status (with sub-links for Product Status and Network Status), Network Settings, Network Security Settings, Services, and Administrator Settings (with sub-links for Change Administrator Password, Administrator Name/Contact Information, and Information). The main content area has the following fields and text:

- Administrator Settings > Change Administrator Password
- Current password : [input field]
- New Password : [input field] Enter between 1 and 20 characters.
- Confirm New Password : [input field]
- Note: It is recommended to communicate via HTTPS for entering an administrator password.
- OK button

- 3** Välj **OK**.

Obs!

- För att konfigurera eller ändra låsta menyobjekt, klicka på **Administrator Login (Administratörsinloggning)** och ange administratörlösenordet.
- För att radera administratörlösenordet, klicka på **Administrator Settings (Administratörsinställningar) > Delete Administrator Authentication Information (Ta bort administratörs autentiseringsinformation)**, och ange sedan administratörlösenordet.

Relaterad information

➔ "Öppna Web Config" på sidan 20

Kontrollera protokoll och tjänster

Du kan skriva ut med hjälp av ett antal olika vägar och protokoll. Du kan sänka oönskade säkerhetsrisker genom att begränsa utskrift från särskilda vägar eller genom att kontrollera de olika funktionerna.

Kontrollera protokoll

Konfigurera protokollinställningar.

- 1** Öppna Web Config och välj **Services (Tjänster) > Protocol (Protokoll)**.
- 2** Konfigurera varje punkt.
- 3** Klicka på **Next (Nästa)**.

Säkerhetsinställningar

4

Klicka på OK.

Inställningarna aktiveras på skrivaren.

Relaterad information

- ➔ [”Öppna Web Config” på sidan 20](#)
- ➔ [”Protokoll som du kan aktivera eller inaktivera” på sidan 31](#)
- ➔ [”Inställningsalternativ för protokoll” på sidan 32](#)

Protokoll som du kan aktivera eller inaktivera

Protokoll	Beskrivning
Bonjour Settings (Bonjour-inställningar)	Du kan ange om du vill använda Bonjour. Bonjour används för att söka efter enheter, skriva ut (AirPrint) och så vidare.
SLP Settings (SLP-inställningar)	Du kan aktivera eller inaktivera SLP-funktionen. SLP används för nätverkssökning i EpsonNet Config.
LLTD Settings (LLTD-inställningar)	Du kan aktivera eller inaktivera LLTD-funktionen. När detta är aktiverat, visas det på Windows nätverkskarta.
LLMNR Settings (LLMNR-inställningar)	Du kan aktivera eller inaktivera LLMNR-funktionen. När det är aktiverat kan du använda namnmatchning utan NetBIOS, även om du inte kan använda DNS.
LPR Settings (LPR-inställningar)	Du kan ange om LPR-utskrift ska tillåtas eller inte. När det är aktiverat kan du skriva ut och skanna från LPR-porten.
RAW(Port9100) Settings (RAW(Port9100)-inställningar)	Du kan ange om du vill tillåta utskrift från RAW-porten (port 9100). När det är aktiverat kan du skriva ut från RAW-porten (port 9100).
RAW(Custom Port) Settings (RAW(Anpassad port)-inställningar)	Du kan ange om du vill tillåta utskrift från RAW-porten (anpassad port). När det är aktiverat kan du skriva ut från RAW-porten (anpassad port).
IPP Settings (IPP-inställningar)	Du kan ange om du vill tillåta utskrift från IPP. När det är aktiverat kan du skriva ut över Internet (inklusive AirPrint).
FTP Settings (FTP-inställningar)	Du kan ange om FTP-utskrift ska tillåtas eller inte. När det är aktiverat kan du skriva ut över en FTP-server.
SNMPv1/v2c Settings (SNMPv1/v2c-inställningar)	Du kan ange om du vill aktivera SNMPv1/v2c. Detta används för att ställa in enheter, övervakning och så vidare.
SNMPv3 Settings (SNMPv3-inställningar)	Du kan ange om du vill aktivera SNMPv3. Detta används för att ställa in krypterade enheter, övervakning och så vidare.

Relaterad information

- ➔ [”Kontrollera protokoll” på sidan 30](#)
- ➔ [”Inställningsalternativ för protokoll” på sidan 32](#)

Säkerhetsinställningar

Inställningsalternativ för protokoll

EPSON	FX-890IIN
Administrator Logout <input type="checkbox"/> Status Product Status Network Status <input checked="" type="checkbox"/> Network Settings <input checked="" type="checkbox"/> Network Security Settings <input type="checkbox"/> Services Protocol <input checked="" type="checkbox"/> Administrator Settings	Services > Protocol Note: If you need to change the Device Name used on each protocol and the Bonjour Name, change the Device Name in the Network Settings. If you need to change the Location used on each protocol, change it in the Network Settings. <div style="border: 1px solid gray; padding: 5px;"> Bonjour Settings <input checked="" type="checkbox"/> Use Bonjour Bonjour Name : <input type="text" value="EPSON [redacted].local"/> Bonjour Service Name : <input type="text" value="EPSON FX-890IIN"/> Location : <input type="text"/> Top Priority Protocol : <input type="text" value="IPP"/> </div> <div style="border: 1px solid gray; padding: 5px;"> SLP Settings <input checked="" type="checkbox"/> Enable SLP </div> <div style="border: 1px solid gray; padding: 5px;"> LLTD Settings <input checked="" type="checkbox"/> Enable LLTD Device Name : <input type="text" value="EPSON [redacted]"/> </div> <div style="border: 1px solid gray; padding: 5px;"> LLMNR Settings <input checked="" type="checkbox"/> Enable LLMNR </div> <div style="border: 1px solid gray; padding: 5px;"> LPR Settings <input checked="" type="checkbox"/> Allow LPR Port Printing Printing Timeout (sec) : <input type="text" value="300"/> </div> <input type="checkbox"/> RAW(Port9100) Settings

Alternativ	Inställningsvärde och beskrivning
Bonjour Settings (Bonjour-inställningar)	
Use Bonjour (Använd Bonjour)	Välj det här för att söka efter eller använda enheter via Bonjour. Du kan inte använda AirPrint om detta rensas.
Bonjour Name (Bonjour-namn)	Visar Bonjour-namn.
Bonjour Service Name (Tjänstenamn f. Bonjour)	Visar Bonjour-servicenamn.
Location (Plats)	Visar Bonjour-platsnamn.
Top Priority Protocol (Topprioritetsprotokoll)	Välj topprioritetsprotokoll för Bonjour-utskrift.
SLP Settings (SLP-inställningar)	
Enable SLP (Aktivera SLP)	Välj detta för att aktivera SLP-funktionen. Detta används för nätverkssökning i EpsonNet Config.
LLTD Settings (LLTD-inställningar)	
Enable LLTD (Aktivera LLTD)	Välj detta för att aktivera LLTD. Skrivaren visas i Windows nätverkskarta.
Device Name (Enhetsnamn)	Visar LLTD-enhetens namn.

Säkerhetsinställningar

Alternativ	Inställningsvärde och beskrivning
LLMNR Settings (LLMNR-inställningar)	
Enable LLMNR (Aktivera LLMNR)	Välj detta för att aktivera LLMNR. Du kan använda namnmatchning utan NetBIOS, även om du inte kan använda DNS.
LPR Settings (LPR-inställningar)	
Allow LPR Port Printing (Tillåt LPR-port-utskrift)	Välj att tillåta utskrift från LPR-porten.
Printing Timeout (sec) (Utskriftstimeout (sek))	Ange timeout-värde för LPR-utskrift från 0 till 3 600 sekunder. Om du inte vill ha timeout, ange 0.
RAW(Port9100) Settings (RAW(Port9100)-inställningar)	
Allow RAW(Port9100) Printing (Tillåt RAW(Port9100)-utskrift)	Välj att tillåta utskrift från RAW-port (port 9100).
Printing Timeout (sec) (Utskriftstimeout (sek))	Ange timeout-värdet för RAW (Port 9100)-utskrift mellan 0 till 3 600 sekunder. Om du inte vill ha timeout, ange 0.
RAW(Custom Port) Settings (RAW(Anpassad port)-inställningar)	
Allow RAW(Custom Port) Printing (Tillåt RAW(Anpassad port)-utskrift)	Välj att tillåta utskrift från RAW-port (anpassad port).
Port Number (Portnummer)	Ange portnummer för RAW (Anpassad port)-utskrift från 1024 till 65535, förutom 9100, 1865 och 2968.
Printing Timeout (sec) (Utskriftstimeout (sek))	Ange timeout-värdet för RAW (Anpassad port)-utskrift från 0 till 3 600 sekunder. Om du inte vill ha timeout, ange 0.
IPP Settings (IPP-inställningar)	
Enable IPP (Aktivera IPP)	Markera för att aktivera IPP-kommunikation. Endast skrivare som stöder IPP visas. Du kan inte använda AirPrint om detta inaktiveras.
Allow Non-secure Communication (Tillåt icke säker kommunikation)	Välj att tillåta skrivaren att kommunicera utan säkerhetsåtgärder (IPP).
Communication Timeout (sec) (Kommunikationstimeout (sek))	Ange timeout-värde för IPP-utskrift från 0 till 3 600 sekunder.
URL(Network (Nätverk))	Visar IPP-webbadresser (http och https) när skrivaren är ansluten med kabelanslutet LAN. Webbadressen är ett kombinerat värde av skrivarens IP-adress, portnummer och IPP-skrivarnamn.
Printer Name (Skrivarnamn)	Visar IPP-skrivarnamn.
Location (Plats)	Visar IPP-plats.
FTP Settings (FTP-inställningar)	
Enable FTP Server (Aktivera FTP-server)	Markera för att aktivera FTP-utskrift. Endast skrivare som stöder FTP-utskrift visas.
Communication Timeout (sec) (Kommunikationstimeout (sek))	Ange timeout-värde för FTP-kommunikation från 0 till 3 600 sekunder. Om du inte vill ha timeout, ange 0.
SNMPv1/v2c Settings (SNMPv1/v2c-inställningar)	
Enable SNMPv1/v2c (Aktivera SNMPv1/v2c)	Markera för att aktivera SNMPv1/v2c. Endast skrivare som stöder SNMPv3 visas.

Säkerhetsinställningar

Alternativ	Inställningsvärde och beskrivning
Access Authority (Åtkomstbehörighet)	Ställ in åtkomstbehörighet när SNMPv1/v2c är aktiverat. Välj Read Only (Skrivskyddad) eller Read/Write (Läs/Skriv) .
Community Name (Read Only) (Gemenskapsnamn (endast läsa))	Ange 0 till 32 ASCII (0x20 till 0x7E)-tecken.
Community Name (Read/Write) (Gemenskapsnamn (läsa/skriva))	Ange 0 till 32 ASCII (0x20 till 0x7E)-tecken.
SNMPv3 Settings (SNMPv3-inställningar)	
Enable SNMPv3 (Aktivera SNMPv3)	SNMPv3 är aktiverad när rutan markerats.
User Name (Användarnamn)	Ange mellan 1 och 32 tecken med 1 byte mellanslag.
Authentication Settings (Autentiseringsinställningar)	
Algorithm (Algoritm)	Välj en algoritm för autentisering av SNMPv3.
Password (Lösenord)	Ange lösenord för autentisering för SNMPv3. Ange mellan 8 och 32 tecken i ASCII (0x20–0x7E). Om du inte specificerar detta ska du lämna det blankt.
Confirm Password (Bekräfta lösenord)	Ange lösenordet som du konfigurerade som bekräftelse.
Encryption Settings (Krypteringsinställningar)	
Algorithm (Algoritm)	Välj en algoritm för kryptering av SNMPv3.
Password (Lösenord)	Ange lösenord för kryptering för SNMPv3. Ange mellan 8 och 32 tecken i ASCII (0x20–0x7E). Om du inte specificerar detta ska du lämna det blankt.
Confirm Password (Bekräfta lösenord)	Ange lösenordet som du konfigurerade som bekräftelse.
Context Name (Kontextnamn)	Ange max 32 tecken i Unicode (UTF-8). Om du inte specificerar detta ska du lämna det blankt. Antalet tecken som kan anges varierar beroende på språk.

Relaterad information

- ➔ ["Kontrollera protokoll" på sidan 30](#)
- ➔ ["Protokoll som du kan aktivera eller inaktivera" på sidan 31](#)

SSL-/TLS-kommunikation med skrivaren

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

Om digital certifiering

- Certifikat signerat av en CA
Ett certifikat signerat av en certifikatutfärdare (CA) måste hämtas från en certifikatutfärdare. Du kan säkra kommunikationen genom att använda ett CA-signerat certifikat. Du kan använda ett CA-signerat certifikat för varje säkerhetsfunktion.

Säkerhetsinställningar

- ❑ CA-certifikat
Ett CA-certifikat innebär att en tredje part har verifierat identiteten hos en server. Detta är en huvudkomponent i web-of-trust-säkerhet. Du måste hämta ett CA-certifikat för serverautentisering från en CA som utfärdar sådana.
- ❑ Självsignerat certifikat
Ett självsignerat certifikat är ett certifikat som skrivaren utfärdar och signerar. Detta certifikat är inte tillförlitligt och kan inte förhindra bedrägerier. Om du använder detta certifikat som SSL/TLS-certifikat kan en säkerhetsvarning visas i webbläsare. Du kan bara använda detta certifikat för SSL/TLS-kommunikation.

Relaterad information

- ➔ [”Hämta och importera ett CA-signerat certifikat” på sidan 35](#)
- ➔ [”Radera ett CA-signerat certifikat” på sidan 38](#)
- ➔ [”Uppdatera ett självsignerat certifikat” på sidan 39](#)

Hämta och importera ett CA-signerat certifikat

Hämta ett CA-signerat certifikat

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

Följ stegen för att skapa en CSR och hämta ett CA-signerat certifikat med Web Config. Certifikatet får formatet PEM/DER när du skapar det med Web Config.

- 1** Öppna Web Config och välj sedan **Network Security Settings (Nätverkets säkerhetsinställningar)**. Välj sedan **SSL/TLS > Certificate (Certifikat)**.
- 2** Klicka på **Generate (Generera)** för CSR.
En sida där du kan skapa en CSR öppnas.
- 3** Ange ett värde för varje alternativ.

Obs!

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

- 4** Klicka på **OK**.
Ett meddelande om slutförande visas.
- 5** Välj **Network Security Settings (Nätverkets säkerhetsinställningar)**. Välj sedan **SSL/TLS > Certificate (Certifikat)**.
- 6** Klicka på en av hämtningsknapparna för CSR beroende på certifikatutfärdarens specificerade format när du vill hämta en CSR till en dator.

**Viktigt!**

Skapa inte ett CSR igen. Om du gör det kanske du inte kan importera ett utfärdat CA-signed Certificate.

Säkerhetsinställningar

- 7 Skicka en CSR till en certifikatutfärdare och skaffa ett CA-signerat certifikat.
Följ reglerna för de olika certifikatutfärdarna angående sändningsmetod och format.
- 8 Spara det utfärdade CA-signerade certifikatet på en dator som är ansluten till skrivaren.
Hämtningen av det CA-signerade certifikatet är klar när du sparar certifikatet på en måldestination.

Relaterad information

- ➔ ”Öppna Web Config” på sidan 20
- ➔ ”Inställningsalternativ för CSR” på sidan 36
- ➔ ”Importerera ett CA-signerat certifikat” på sidan 37

Inställningsalternativ för CSR

Alternativ	Inställningar och beskrivning
Key Length (Nyckellängd)	Välj nyckellängd för CSR.
Common Name (Nätverksnamn)	Du kan uppge mellan 1 och 128 tecken. Om det är en IP-adress ska det vara en statisk IP-adress. Exempel: URL för åtkomst till Web Config: https://10.152.12.225 Nätverksnamn: 10.152.12.225
Organization (Organisation)/ Organizational Unit (Organisationsenhet)/ Locality (Plats)/ State/Province (Stat/provins)	Du kan ange från 0 till 64 tecken i ASCII (0x20-0x7E). Du kan dela upp unika namn med komman.
Country (Land)	Skriv en landskod med ett tvåsiffrigt nummer enligt ISO-3166.

Relaterad information

- ➔ ”Hämta ett CA-signerat certifikat” på sidan 35

Säkerhetsinställningar

Importera ett CA-signerat certifikat

**Viktigt!**

- Kontrollera att rätt datum och klockslag är inställt på skrivaren.
- Om du hämtar ett certifikat med en CSR som skapats i Web Config kan du importera ett certifikat i taget.

1

Öppna Web Config och välj sedan **Network Security Settings (Nätverkets säkerhetsinställningar)**. Välj sedan **SSL/TLS > Certificate (Certifikat)**.

2

Klicka på **Import (Importera)**.

En sida där du kan importera certifikat öppnas.

3

Ange ett värde för varje alternativ.

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

- Ett certifikat i formatet PEM/DER som hämtats från Web Config
 - **Private Key (Privat nyckel)**: Konfigureras inte eftersom skrivaren innehåller en privat nyckel.
 - **Password (Lösenord)**: Konfigureras inte.
 - **CA Certificate 1 (CA-certifikat 1)/CA Certificate 2 (CA-certifikat 2)**: Valfritt
- Ett certifikat i formatet PEM/DER som hämtats från en dator
 - **Private Key (Privat nyckel)**: Måste anges.
 - **Password (Lösenord)**: Konfigureras inte.
 - **CA Certificate 1 (CA-certifikat 1)/CA Certificate 2 (CA-certifikat 2)**: Valfritt
- Ett certifikat i formatet PKCS#12 som hämtats från en dator
 - **Private Key (Privat nyckel)**: Konfigureras inte.
 - **Password (Lösenord)**: Valfritt
 - **CA Certificate 1 (CA-certifikat 1)/CA Certificate 2 (CA-certifikat 2)**: Konfigureras inte.

4

Klicka på **OK**.

Ett meddelande om slutförande visas.

Obs!

Verifiera certifikatinformationen genom att klicka på **Confirm (Bekräfta)**.

Relaterad information

- ➔ ["Öppna Web Config" på sidan 20](#)
- ➔ ["Inställningsalternativ för import av CA-signerat certifikat" på sidan 38](#)

Säkerhetsinställningar

Inställningsalternativ för import av CA-signerat certifikat

EPSON FX-890IIN

Administrator Logout

- Status
 - [Product Status](#)
 - [Network Status](#)
- Network Settings
- Network Security Settings
 - SSL/TLS
 - [Basic](#)
 - [Certificate](#)
 - IPsec/IP Filtering
 - Services
 - Administrator Settings

Network Security Settings > SSL/TLS > Certificate

Server Certificate : Certificate (PEM/DER) No file selected.

Private Key : No file selected.

Password :

CA Certificate 1 : No file selected.

CA Certificate 2 : No file selected.

Note: It is recommended to communicate via HTTPS for importing a certificate.

Alternativ	Inställningar och beskrivning
Server Certificate (Servercertifikat) eller Client Certificate (Klientcertifikat)	Välj ett certifikatformat.
Private Key (Privat nyckel)	Om du hämtat ett certifikat med formatet PEM/DER med en CSR som skapats på en dator ska du ange en privat nyckelfil som matchar certifikatet.
Password (Lösenord)	Skriv ett lösenord för kryptering av en privat nyckel.
CA Certificate 1 (CA-certifikat 1)	Om certifikatets format är Certificate (PEM/DER) (Certifikat (PEM/DER)) ska du importera ett certifikat från en certifikatutfärdare som utfärdar ett servercertifikat. Ange en fil om det behövs.
CA Certificate 2 (CA-certifikat 2)	Om certifikatets format är Certificate (PEM/DER) (Certifikat (PEM/DER)) ska du importera ett certifikat från en certifikatutfärdare som utfärdar CA Certificate 1 (CA-certifikat 1) . Ange en fil om det behövs.

Relaterad information

➔ ["Importera ett CA-signerat certifikat" på sidan 37](#)

Radera ett CA-signerat certifikat

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

**Viktigt!**

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

1

Öppna Web Config och välj sedan **Network Security Settings (Nätverkets säkerhetsinställningar)**. Välj sedan **SSL/TLS > Certificate (Certifikat)**.

2

Klicka på **Delete (Radera)**.

Säkerhetsinställningar

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

Relaterad information

➔ ”Öppna Web Config” på sidan 20

Uppdatera ett självsignerat certifikat

Om skrivaren har stöd för HTTPS-serverfunktion kan du uppdatera ett självsignerat certifikat. Ett varningsmeddelande visas när du öppnar Web Config med ett självsignerat certifikat.

Använd ett självsignerat certifikat tills du hämtat och importerat ett CA-signerat certifikat.

- 1 Öppna Web Config och välj **Network Security Settings (Nätverkets säkerhetsinställningar) > SSL/TLS > Certificate (Certifikat)**.
- 2 Klicka på **Update (Uppdatera)**.
- 3 Ange **Common Name (Nätverksnamn)**.

Skriv en IP-adress eller en identifierare som t.ex. ett FQDN-namn för skrivaren. Du kan uppges mellan 1 och 128 tecken.

Obs!

Du kan skilja unika namn (CN) åt med komman.

- 4 Ange en giltighetsperiod för certifikatet.

EPSON	FX-890IIN										
<p>Administrator Logout</p> <ul style="list-style-type: none"> <input type="checkbox"/> Status <ul style="list-style-type: none"> Product Status Network Status <input checked="" type="checkbox"/> Network Settings <input checked="" type="checkbox"/> Network Security Settings <ul style="list-style-type: none"> <input type="checkbox"/> SSL/TLS <ul style="list-style-type: none"> Basic Certificate <input checked="" type="checkbox"/> IPsec/IP Filtering <input checked="" type="checkbox"/> Services <input checked="" type="checkbox"/> Administrator Settings 	<p>Network Security Settings > SSL/TLS > Certificate</p> <table border="1"> <tr> <td>Key Length :</td> <td>RSA 2048bit - SHA-256</td> </tr> <tr> <td>Common Name :</td> <td>EPSONXXXXXX,EPSONXXXXXX.local,192.0.2.102</td> </tr> <tr> <td>Organization :</td> <td>SEIKO EPSON CORP.</td> </tr> <tr> <td>Valid Date (UTC) :</td> <td>2017-04-11 06:22:56 UTC</td> </tr> <tr> <td>Certificate Validity (year) :</td> <td>10</td> </tr> </table> <p style="text-align: center;"> <input type="button" value="Next"/> <input type="button" value="Back"/> </p>	Key Length :	RSA 2048bit - SHA-256	Common Name :	EPSONXXXXXX,EPSONXXXXXX.local,192.0.2.102	Organization :	SEIKO EPSON CORP.	Valid Date (UTC) :	2017-04-11 06:22:56 UTC	Certificate Validity (year) :	10
Key Length :	RSA 2048bit - SHA-256										
Common Name :	EPSONXXXXXX,EPSONXXXXXX.local,192.0.2.102										
Organization :	SEIKO EPSON CORP.										
Valid Date (UTC) :	2017-04-11 06:22:56 UTC										
Certificate Validity (year) :	10										

- 5 Klicka på **Next (Nästa)**.
Ett bekräftelsemeddelande visas.
- 6 Klicka på **OK**.
Skrivaren uppdateras.

Säkerhetsinställningar

Obs!

Verifiera certifikatinformationen genom att klicka på *Confirm (Bekräfta)*.

Relaterad information

➔ ["Öppna Web Config" på sidan 20](#)

Krypterad kommunikation med IPsec/IP Filtering

Om IPsec/IP Filtering

Om skrivaren har stöd för IPsec/IP Filtering kan du filtrera trafiken baserat på IP-adresser, tjänster och port. Genom att kombinera filter kan du konfigurera skrivaren att acceptera eller blockera angivna klienter och data. Du kan även höja säkerhetsnivån genom att använda en IPsec.

Konfigurera en standardprincip när du vill filtrera trafiken. Standardprincipen gäller alla användare och grupper som ansluter till skrivaren. Konfigurera gruppprinciper om du vill ha mer exakt kontroll över användare och grupper. En gruppprincip är en eller flera regler som gäller en användare eller användargrupp. Skrivaren styr IP-paketen i enlighet med de principer som konfigurerats. IP-paket autentiseras i ordningsföljden gruppprincip 1 till 10 och därefter en standardpolicy.

Obs!

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

Konfigurera standardpolicy

- 1 Öppna Web Config och välj **Network Security Settings (Nätverkets säkerhetsinställningar) > IPsec/IP Filtering > Basic (Grundläggande)**.
- 2 Ange ett värde för varje alternativ.
- 3 Klicka på **Next (Nästa)**.
Ett bekräftelsemeddelande visas.
- 4 Klicka på **OK**.
Skrivaren uppdateras.

Relaterad information

➔ ["Öppna Web Config" på sidan 20](#)

➔ ["Inställningsalternativ för standardpolicy" på sidan 41](#)

Säkerhetsinställningar

Inställningsalternativ för standardpolicy

EPSON **FX-890IIN**

Administrator Logout
 Status
 Product Status
 Network Status
 Network Settings
 Network Security Settings
 SSL/TLS
 IPsec/IP Filtering
 Basic
 Services
 Administrator Settings

Network Security Settings > IPsec/IP Filtering > Basic

Each policy is applied with following priorities:
 Group Policy 1 > Group Policy 2 > ... > Group Policy 10 > Default Policy

Default Policy 1 2 3 4 5 6 7 8 9 10

IPsec/IP Filtering : Enable Disable

Default Policy

Access Control : IPsec

Authentication Method : Pre-Shared Key

Pre-Shared Key : ●●●●●●

Confirm Pre-Shared Key : ●●●●●●

Encapsulation : Transport Mode

Remote Gateway(Tunnel Mode) :

Security Protocol : ESP

Next

Alternativ	Inställningar och beskrivning	
IPsec/IP Filtering	Du kan aktivera och inaktivera funktioner för IPsec/IP Filtering.	
Access Control (Åtkomstkontroll)	Permit Access (Tillåt åtkomst)	Välj detta när du vill att konfigurerade IP-paket ska få passera.
	Refuse Access (Neka åtkomst)	Välj detta när du inte vill att konfigurerade IP-paket ska få passera.
	IPsec	Välj detta när du vill att konfigurerade IPsec-paket ska få passera.
Authentication Method (Autentiseringsmetod)	Visar kompatibla autentiseringsmetoder.	
Pre-Shared Key (I förväg delad nyckel)	Ange en i förväg delad nyckel mellan 1 och 127 tecken.	
Confirm Pre-Shared Key (Bekräfta I förväg delad nyckel)	Ange nyckeln som du konfigurerade som bekräftelse.	
Encapsulation (Inkapsling)	Om du väljer IPsec för Access Control (Åtkomstkontroll) måste du konfigurera en inkapslingsmetod.	
	Transport Mode (Transportläge)	Välj detta om du bara använder skrivaren i samma lokala nätverk. IP-paket lager 4 eller senare krypteras.
	Tunnel Mode (Tunnelläge)	Om du använder skrivaren i det Internet-förberedda nätverket, såsom IPsec-VPN, ska du markera det här alternativet. Rubriker och data i IP-paket krypteras.
Remote Gateway(Tunnel Mode) (Fjärrgateway(Tunnelläge))	Om du väljer Tunnel Mode (Tunnelläge) för Encapsulation (Inkapsling) , ange en gateway-adress från 1 till 39 tecken.	

Säkerhetsinställningar

Alternativ	Inställningar och beskrivning	
Security Protocol (Säkerhetsprotokoll)	Om du väljer IPsec för Access Control (Åtkomstkontroll) , välj ett alternativ.	
	ESP	Välj detta när du vill säkerställa integriteten hos autentiseringen och data samt kryptera data.
	AH	Välj detta när du vill säkerställa integriteten hos autentiseringen och data. Du kan fortfarande använda IPsec även om kryptering av data är förbjudet.

Relaterad information

➔ ["Konfigurera standardpolicy" på sidan 40](#)

Konfigurera Gruppolicy

- 1** Öppna skrivarens Web Config och välj **Network Security Settings (Nätverkets säkerhetsinställningar) > IPsec/IP Filtering > Basic (Grundläggande)**.
- 2** Klicka på en numrerad flik du vill konfigurera.
- 3** Ange ett värde för varje alternativ.
- 4** Klicka på **Next (Nästa)**.
Ett bekräftelsemeddelande visas.
- 5** Klicka på **OK**.
Skrivaren uppdateras.

Relaterad information

➔ ["Öppna Web Config" på sidan 20](#)

➔ ["Inställningsalternativ för gruppolicy" på sidan 43](#)

Säkerhetsinställningar

Inställningsalternativ för gruppolicy

EPSON **FX-890IIN**

Administrator Logout
 Status
 Product Status
 Network Status
 Network Settings
 Network Security Settings
 SSL/TLS
 IPsec/IP Filtering
 Basic
 Services
 Administrator Settings

Network Security Settings > IPsec/IP Filtering > Basic

Each policy is applied with following priorities:
 Group Policy 1 > Group Policy 2 > ... > Group Policy 10 > Default Policy

Default Policy | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10

Enable this Group Policy

Access Control : IPsec

Local Address(Printer) : Any addresses

Remote Address(Host) :

Method of Choosing Port : Port Number

Service Name :

- Any
- ENPC
- SNMP
- LPR
- RAW (Port9100)
- RAW (Custom Port)
- IPP/IPPS
- WSD
- WS-Discovery
- Network Scan
- Network Push Scan
- Network Push Scan Discovery
- FTP Data (Local)
- FTP Control (Local)
- FTP Data (Remote)
- FTP Control (Remote)
- CIFS (Local)
- CIFS (Remote)
- HTTP (Local)
- HTTPS (Local)
- HTTP (Remote)
- HTTPS (Remote)

Transport Protocol : Any Protocol

Alternativ	Inställningar och beskrivning	
Enable this Group Policy (Aktivera denna Gruppolicy)	Du kan aktivera och inaktivera en gruppolicy.	
Access Control (Åtkomstkontroll)	Konfigurera en metod för styrning av trafiken av IP-paket.	
	Permit Access (Tillåt åtkomst)	Välj detta när du vill att konfigurerade IP-paket ska få passera.
	Refuse Access (Neka åtkomst)	Välj detta när du inte vill att konfigurerade IP-paket ska få passera.
	IPsec	Välj detta när du vill att konfigurerade IPsec-paket ska få passera.
Local Address(Printer) (Lokal adress(skrivare))	Välj en IPv4-adress eller IPv6-adress som matchar din nätverksmiljö. Om en IP-adress tilldelats automatiskt kan du välja Use auto-obtained IPv4 address (Använda automatiskt erhållen IPv4-adress) .	
Remote Address(Host) (Fjärradress(värd))	Ange IP-adressen till en enhet för att styra åtkomsten. IP-adressen måste innehålla mellan 0 och 43 tecken. Alla adresser styrs om du inte anger en IP-adress. Obs! Om en IP-adress tilldelas automatiskt (dvs. med DHCP) kanske anslutningen inte är tillgänglig. Konfigurera en statisk IP-adress.	

Säkerhetsinställningar

Alternativ	Inställningar och beskrivning	
Method of Choosing Port (Metod för att välja port)	Välj en metod för att specificera portar.	
Service Name (Tjänstnamn)	Ställ in ett alternativ om du väljer Service Name (Tjänstnamn) som Method of Choosing Port (Metod för att välja port) .	
Transport Protocol (Transportprotokoll)	Om du väljer Port Number (Portnummer) som Method of Choosing Port (Metod för att välja port) måste du konfigurera en inkapslingsmetod.	
	Any Protocol (Valfritt protokoll)	Välj detta när du vill styra alla protokolltyper.
	TCP	Välj detta när du vill styra data för unicast.
	UDP	Välj detta när du vill styra data för broadcast och multicast.
	ICMPv4	Välj detta när du vill styra ping-kommandot.
Local Port (Lokal port)	Om du väljer Port Number (Portnummer) för Method of Choosing Port (Metod för att välja port) och om du väljer TCP eller UDP för Transport Protocol (Transportprotokoll) , ange portnummer för att styra paketmottagning och separera dem med komma. Du kan ange högst 10 portnummer. Exempel: 20,80,119,5220 Alla portar styrs om du inte anger ett portnummer.	
Remote Port (Fjärrport)	Om du väljer Port Number (Portnummer) för Method of Choosing Port (Metod för att välja port) och om du väljer TCP eller UDP för Transport Protocol (Transportprotokoll) , ange portnummer för att styra paketsändning och separera dem med komma. Du kan ange högst 10 portnummer. Exempel: 25,80,143,5220 Alla portar styrs om du inte anger ett portnummer.	
Authentication Method (Autentiseringsmetod)	Om du väljer IPsec för Access Control (Åtkomstkontroll) , välj ett alternativ.	
Pre-Shared Key (I förväg delad nyckel)	Ange en i förväg delad nyckel mellan 1 och 127 tecken.	
Confirm Pre-Shared Key (Bekräfta I förväg delad nyckel)	Ange nyckeln som du konfigurerade som bekräftelse.	
Encapsulation (Inkapsling)	Om du väljer IPsec för Access Control (Åtkomstkontroll) måste du konfigurera en inkapslingsmetod.	
	Transport Mode (Transportläge)	Välj detta om du bara använder skrivaren i samma lokala nätverk. IP-paket lager 4 eller senare krypteras.
	Tunnel Mode (Tunnelläge)	Om du använder skrivaren i det Internet-förberedda nätverket, såsom IPsec-VPN, ska du markera det här alternativet. Rubriker och data i IP-paket krypteras.
Remote Gateway(Tunnel Mode) (Fjärrgateway(Tunnelläge))	Om du väljer Tunnel Mode (Tunnelläge) för Encapsulation (Inkapsling) , ange en gateway-adress från 1 till 39 tecken.	

Säkerhetsinställningar

Alternativ	Inställningar och beskrivning	
Security Protocol (Säkerhetsprotokoll)	Om du väljer IPsec för Access Control (Åtkomstkontroll) , välj ett alternativ.	
	ESP	Välj detta när du vill säkerställa integriteten hos autentiseringen och data samt kryptera data.
	AH	Välj detta när du vill säkerställa integriteten hos autentiseringen och data. Du kan fortfarande använda IPsec även om kryptering av data är förbjudet.

Relaterad information

- ➔ ”Konfigurera Gruppolicy” på sidan 42
- ➔ ”Kombination av Lokal adress (Skrivare) och Fjärradress (Värd) i gruppolicy” på sidan 45
- ➔ ”Referenser för tjänstenamn enligt gruppolicy” på sidan 45

Kombination av Lokal adress (Skrivare) och Fjärradress (Värd) i gruppolicy

		Inställning för Lokal adress (Skrivare)		
		IPv4	IPv6*2	Valfria adresser*3
Inställning av Fjärradress(värd)	IPv4*1	✓	-	✓
	IPv6*1*2	-	✓	✓
	Tom	✓	✓	✓

*1: Om **IPsec** har valts för **Access Control (Åtkomstkontroll)**, kan du inte specificera i någon prefixlängd.

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

*3: Förutom IPv6 länkllokala adresser.

Referenser för tjänstenamn enligt gruppolicy

Obs!

Otillgängliga tjänster visas, men kan inte väljas.

Tjänstenamn	Protokolltyp	Lokalt portnummer	Fjärrportnummer	Kontrollerade funktioner
Any (Valfria)	-	-	-	Alla tjänster
ENPC	UDP	3289	Valfri port	Söker efter en skrivare från olika applikationer, såsom EpsonNet Config, en skrivardrivrutin och en skannerdrivrutin
SNMP	UDP	161	Valfri port	Hämta och konfigurera MIB från applikationer, såsom EpsonNet Config, Epson-skrivardrivrutin och Epson skannerdrivrutin.

Säkerhetsinställningar

Tjänstenamn	Protokolltyp	Lokalt portnummer	Fjärrportnummer	Kontrollerade funktioner
LPR	TCP	515	Valfri port	Vidarebefordra LPR-data
RAW (Port9100)	TCP	9100	Valfri port	Vidarebefordra RAW-data
RAW (Custom Port) (RAW (Anpassad port))	TCP	2501(standard)	Valfri port	Vidarebefordra RAW-data
IPP/IPPS	TCP	631	Valfri port	Vidarebefordra Air-Print-data (IPP-/IPPS-utskrift)
WSD	TCP	Valfri port	5357	Kontrollera WSD
WS-Discovery	UDP	3702	Valfri port	Söka efter en skrivare från WSD
Network Scan (Nätverkspushskanning)	TCP	1865	Valfri port	Vidarebefordra skanningsdata från Document Capture Pro
Network Push Scan (Nätverkspushskanning)	TCP	Valfri port	2968	Hämta jobbinformation för pushskanning från Document Capture Pro
Network Push Scan Discovery	UDP	2968	Valfri port	Söker efter en dator när push-skanning från Document Capture Pro körs
FTP Data (Local) (FTP-data (lokal))	TCP	20	Valfri port	FTP-server (datavidarebefordran för FTP-utskrift)
FTP Control (Local) (FTP-styrning (lokal))	TCP	21	Valfri port	FTP-server (styr FTP-utskrift)
FTP Data (Remote) (FTP-data (fjärr))	TCP	Valfri port	20	FTP-klient (vidarebefordran av skanningdata och mottagna faxdata) Detta kan dock endast styra en FTP-server som använder fjärrportnummer 20.
FTP Control (Remote) (FTP-styrning (fjärr))	TCP	Valfri port	21	FTP-klient (kontroll för vidarebefordran av skanningdata och mottagna faxdata)
CIFS (Local) (CIFS (lokal))	TCP	445	Valfri port	CIFS-server (Dela en nätverksmapp)

Säkerhetsinställningar

Tjänstenamn	Protokolltyp	Lokalt portnummer	Fjärrportnummer	Kontrollerade funktioner
CIFS (Remote) (CIFS (fjärr))	TCP	Valfri port	445	CIFS-klient (vidarebefordran av skanning-data och mottagna faxdata till en mapp)
HTTP (Local) (HTTP (lokal))	TCP	80	Valfri port	HTTP(S)-server (vidarebefordran av data för Web Config och WSD)
HTTPS (Local) (HTTPS (lokal))	TCP	443	Valfri port	
HTTP (Remote) (HTTP (fjärr))	TCP	Valfri port	80	HTTP(S)-klient (kommunikation mellan Epson Connect eller Google Cloud Print, firmware-uppdatering och rotcertifikat-uppdatering)
HTTPS (Remote) (HTTPS (fjärr))	TCP	Valfri port	443	

Exempel på konfigurering av IPsec/IP Filtering

Endast mottagning av IPsec-paket

Det här exemplet visar hur du enbart konfigurerar en standardpolicy.

Standardpolicy:

- IPsec/IP Filtering: Enable (Aktivera)
- Access Control (Åtkomstkontroll): IPsec
- Authentication Method (Autentiseringsmetod): Pre-Shared Key (I förväg delad nyckel)
- Pre-Shared Key (I förväg delad nyckel): Ange högst 127 tecken.

Gruppolicy:

Konfigurera inte.

Ta emot utskriftsdata och skrivarinställningar

Det här exemplet tillåter kommunikation för utskriftsdata och skrivarkonfiguration från specificerade tjänster.

Standardpolicy:

- IPsec/IP Filtering: Enable (Aktivera)
- Access Control (Åtkomstkontroll): Refuse Access (Neka åtkomst)

Gruppolicy:

- Enable this Group Policy (Aktivera denna gruppolicy): Markera rutan.
- Access Control (Åtkomstkontroll): Permit Access (Tillåt åtkomst)
- Remote Address(Host) (Fjärradress(Värd)): IP-adressen till en klient

Säkerhetsinställningar

- Method of Choosing Port (Metod för att välja port): Service Name (Tjänstenamn)**
- Service Name (Tjänstenamn):** Markera rutan för ENPC, SNMP, HTTP (Local) (HTTP (lokal)), HTTPS (Local) (HTTPS (lokal)) och RAW (Port9100).

Endast mottagning från en angiven IP-adress fungerar

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

Standardpolicy:

- IPsec/IP Filtering: Enable (Aktivera)**
- Access Control (Åtkomstkontroll): Refuse Access (Neka åtkomst)**

Gruppolicy:

- Enable this Group Policy (Aktivera denna gruppolicy):** Markera rutan.
- Access Control (Åtkomstkontroll): Permit Access (Tillåt åtkomst)**
- Remote Address(Host) (Fjärradress(Värd)):** IP-adressen till en administratörs klient

Obs!

Oavsett den konfigurerade principen kan klienten få tillgång till skrivaren och konfigurera den.

Använda SNMPv3-protokoll

Om SNMPv3

SNMP är ett protokoll som utför övervakning och styr informationsinsamling för enheter som är anslutna till nätverket. SNMPv3 är versionen för hanteringssäkerhet som har utvecklats.

Vid användning av SNMPv3, ska du ange ändringar för övervakning och inställningsändringar för SNMP-kommunikation (paket) som kan autentiseras och krypteras för att skydda SNMP-kommunikation (paket) från nätverksrisker, såsom kabeltappning, modifiering och modifiering.

Konfigurera SNMPv3

Om skrivaren stöder SNMPv3-protokoll, kan du övervaka och kontrollera åtkomsten till skrivaren.

- 1** Öppna Web Config och välj **Services (Tjänster) > Protocol (Protokoll)**.
- 2** Ange ett värde för varje alternativ för **SNMPv3 Settings (SNMPv3-inställningar)**.
- 3** Klicka på **Next (Nästa)**.
Ett bekräftelsemeddelande visas.

Säkerhetsinställningar

4

Klicka på **OK**.

Skrivaren uppdateras.

Relaterad information

- ➔ ”Öppna Web Config” på sidan 20
- ➔ ”Inställningsalternativ för SNMPv3” på sidan 49

Inställningsalternativ för SNMPv3

EPSON
FX-890IIN

[Administrator Logout](#)

- Status
 - [Product Status](#)
 - [Network Status](#)
- Network Settings
- Network Security Settings
- Services
 - [Protocol](#)
- Administrator Settings

Communication Timeout (sec) :

SNMPv1/v2c Settings

Enable SNMPv1/v2c

Access Authority :

Community Name (Read Only) :

Community Name (Read/Write) :

SNMPv3 Settings

Enable SNMPv3

User Name :

Authentication Settings

Algorithm :

Password :

Confirm Password :

Encryption Settings

Algorithm :

Password :

Confirm Password :

Context Name :

Alternativ	Inställningar och beskrivning
Enable SNMPv3 (Aktivera SNMPv3)	SNMPv3 är aktiverad när rutan markerats.
User Name (Användarnamn)	Ange mellan 1 och 32 tecken med 1 byte mellanslag.
Authentication Settings (Autentiseringsinställningar)	
Algorithm (Algoritm)	Välj en algoritm för en autentisering.
Password (Lösenord)	Ange mellan 8 och 32 tecken i ASCII (0x20–0x7E).
Confirm Password (Bekräfta lösenord)	Ange lösenordet som du konfigurerade som bekräftelse.
Encryption Settings (Krypteringsinställningar)	
Algorithm (Algoritm)	Välj en algoritm för en kryptering.

Säkerhetsinställningar

Alternativ	Inställningar och beskrivning
Password (Lösenord)	Ange mellan 8 och 32 tecken i ASCII (0x20–0x7E).
Confirm Password (Bekräfta lösenord)	Ange lösenordet som du konfigurerade som bekräftelse.
Context Name (Kontextnamn)	Ange mellan 1 och 32 tecken med 1 byte mellanslag.

Relaterad information

➔ ["Konfigurera SNMPv3" på sidan 48](#)

Lösa problem

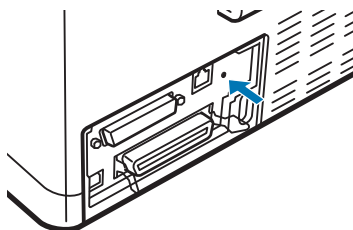
Kontrollera loggen för server- och nätverksenheten

Om det uppstår fel i nätverksanslutningen kan du identifiera orsaken genom att kontrollera loggen för mejlservern eller LDAP-servern eller status genom att använda systemloggen för nätverksenheten, såsom en router, eller kommandon.

Skriva ut ett statusark för nätverket

Du kan skriva ut och kontrollera detaljerad nätverksinformation.

- 1 Lägg i papper.
- 2 Håll ner Statusark-knappen i cirka tre sekunder.
Statusarken för nätverket skrivs ut.



Initiera nätverksinställningar

Återställa nätverksinställningar från skrivaren

Du kan återställa alla nätverksinställningar till standardinställningarna.

- 1 Stäng av skrivaren.
- 2 Håll in Statusark-knappen medan skrivaren slås på.

Återställa nätverksinställningar med EpsonNet Config

Du kan återställa nätverksinställningarna till standardinställningarna med EpsonNet Config.

- 1 Starta EpsonNet Config.

Lösa problem

- 2 Välj den skrivare som du vill återställa nätverksinställningarna för.
- 3 Högerklicka på skrivarens namn och välj sedan **Default Settings (Standardinställningar) > Network Interface (Nätverksgränssnitt)**.
- 4 Tryck på **OK** på bekräftelseskärmen.
- 5 Klicka på **OK**.

Kontrollera kommunikationen mellan enheter och datorer

Kontrollera anslutningen med Ping-kommandot

Du kan använda ett Ping-kommando för att säkerställa att datorn är ansluten till skrivaren. Följ stegen nedan för att kontrollera anslutningen med ett Ping-kommando.

- 1 Kontrollera skrivarens IP-adress för den anslutning som du vill kontrollera.
Du kan kontrollera detta i kolumnen **IP Address (IP-adress)** på nätverkets statusark.
- 2 Öppna skärmen med kommandotolken på datorn.
 - Windows 10
Högerklicka på startknappen eller tryck och håll in den och välj sedan **Command Prompt (Kommandotolk)**.
 - Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
Öppna programskärmen och välj **Command Prompt (Kommandotolk)**.
 - Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 eller tidigare
Klicka på startknappen, välj **All Programs (Alla program)** eller **Programs (Program) > Accessories (Tillbehör) > Command Prompt (Kommandotolk)**.
- 3 Ange följande på kommandoraden och tryck sedan på Enter.
ping 192.0.2.111 (om IP-adressen för den dator du vill kontrollera är 192.0.2.111)
- 4 Om följande visas är bekräftelsen klar. Stäng **Command Prompt (Kommandotolk)**.
Ping-statistik för 192.0.2.111:
Paket: Skickade = 4, Mottagna = 4, Tappade = 0 (0 % förlust),
Tidsfördröjning för svar: (ms):
Min. = 0 ms, Max. = 0 ms, Genomsnitt = 0 ms

Lös problem

Problem att använda nätverksprogram

Kan inte öppna Web Config

Är skrivarens IP-adress rätt konfigurerad?

Konfigurera IP-adressen med EpsonNet Config eller skrivarens kontrollpanel. Du kan kontrollera de aktuella inställningarna genom att skriva ut ett statusark för nätverket eller via skrivarens kontrollpanel.

Stöder webbläsaren bulkkrypteringar för Encryption Strength för SSL/TLS?

Bulkkrypteringar för Encryption Strength för SSL/TLS är följande. Web Config kan bara öppnas i en webbläsare som stöder följande bulkkrypteringar. Kontrollera krypteringen som webbläsaren stöder.

- 80 bitar: AES256/AES128/3DES
- 112 bitar: AES256/AES128/3DES
- 128 bitar: AES256/AES128
- 192 bitar: AES256
- 256 bitar: AES256

Meddelandet "Ej uppdaterad" visas när du öppnar Web Config via SSL-kommunikation (https).

Hämta ett nytt certifikat om certifikatet har gått ut. Om meddelandet visas innan certifikatet har gått ut ska du kontrollera att skrivarens datum är rätt konfigurerat.

Meddelandet "Namnet på säkerhetscertifikatet matchar inte..." visas när du öppnar Web Config via SSL-kommunikation (https).

Skrivarens IP-adress som angetts för Common Name (Nätverksnamn) när du skapar ett självsignerat certifikat eller en CSR matchar inte adressen i webbläsaren. Hämta och importera ett certifikat igen eller ändra skrivarnamnet.

En proxyserver används för åtkomst till skrivaren.

Om du använder en proxyserver med skrivaren måste du konfigurera webbläsarens proxyinställningar.

Välj **Control Panel (Kontrollpanelen) > Network and Internet (Nätverk och Internet) > Internet Options (Internetalternativ) > Connections (Anslutningar) > LAN settings (LAN-inställningar) > Proxy server (Proxyserver)** och ange att proxyservern inte ska användas för lokala adresser.

Exempel:

192.168.1.*: Lokal adress 192.168.1.XXX, nätmask 255.255.255.0
192.168.*.*: Lokal adress 192.168.XXX.XXX, nätmask 255.255.0.0

Relaterad information

- ➔ "Öppna Web Config" på sidan 20
- ➔ "Tilldela en IP-adress med EpsonNet Config" på sidan 14

Lösa problem

Modellnamn och/eller IP-adress visas inte i EpsonNet Config

Valde du **Blockera**, **Avbryt** eller **Stäng av** när Windows säkerhetsfönster eller brandväggsskärm visades?

Om du väljer **Block** (**Blockera**), **Cancel** (**Avbryt**) eller **Shut down** (**Stäng av**) kommer IP-adressen och modellnamnet inte att visas i EpsonNet Config eller EpsonNet Setup.

Du kan korrigerera detta genom att registrera EpsonNet Config som ett undantag i Windows-brandväggen och kommersiella säkerhetsprogram. Om du använder ett antivirus- eller säkerhetsprogram, stäng av det och testa sedan att använda EpsonNet Config.

Är timeoutinställningen för kommunikationsfel för kort?

Kör EpsonNet Config och välj **Tools (Verktyg) > Options (Alternativ) > Timeout (Tidsgräns)** och öka tidslängden i inställningen **Communication Error (Kommunikationsfel)**. Observera att det kan göra att EpsonNet Config fungerar långsammare.

Lösa problem med avancerad säkerhet

Återställa säkerhetsinställningarna

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

Inaktivering av säkerhetsfunktionen från skrivaren

Du kan inaktivera IPsec/IP Filtrering från skrivaren.

- 1 Se till att papper är laddat.
- 2 Tryck på knapparna **Menu (Pitch och Tear Off/Bin)** tills skrivaren piper en gång och **Menu-lamporna (båda Tear Off/Bin-lamporna)** tänds.

Skrivaren försätts i standardinställningsläget och skriver ut ett meddelande som ber dig välja språk för standardinställningsmenyn. Det understrykta språket visar nuvarande inställning.
- 3 Om önskat språk inte är valt, tryck på knappen **Item**↓ (Font) tills utskriften visar önskat språk.
- 4 Tryck på knappen **Set (Tear Off/Bin)** för att välja önskat språk.
- 5 Om du vill skriva ut nuvarande inställningar, tryck på knappen **Set**. Om du vill förbigå att skriva ut nuvarande inställningar, tryck på knappen **Item**↓ eller **Item**↑.

Skrivaren skriver ut den första menyn och det nuvarande värdet för menyn.

Lösa problem

- 6 Tryck på knappen **Item**↓ eller **Item**↑ för att välja menyparametrar för **IPsec/IP Filtering**. Tryck på knappen **Set** för att skrolla igenom värdena inom den valda parametern tills du hittar **Off**.
- 7 När inställningarna är klara, tryck på knapparna **Menu** (**Pitch** och **Tear Off/Bin**).
Menu-lampan (båda **Tear Off/Bin**-lamporna) slocknar och skrivaren avslutar standardinställningsläget. De utförda inställningarna sparas som ett nytt värde.

Obs!

Om du stänger av skrivaren innan standardinställningsläget avslutas kommer de ändringar som utförts att avbrytas och inte sparas.

Återställa säkerhetsfunktionen med Web Config

Du kan inaktivera funktionen om du kan öppna enheten från datorn.

Inaktivera IPsec/IP Filtering med Web Config

- 1 Öppna Web Config och välj **Network Security Settings (Nätverkets säkerhetsinställningar) > IPsec/IP Filtering > Basic (Grundläggande)**.
- 2 Välj **Disable (Inaktivera)** för **IPsec/IP Filtering** i **Default Policy (Standardpolicy)**.
- 3 Klicka på **Next (Nästa)**, och rensa sedan **Enable this Group Policy (Aktivera denna Gruppolicy)** för alla gruppolicies.
- 4 Klicka på **OK**.

Relaterad information

➔ ["Öppna Web Config" på sidan 20](#)

Problem att använda funktionerna för nätverkssäkerhet

Bortglömd I förhand –delad nyckel

Konfigurera nyckeln igen med Web Config.

För att ändra nyckel, öppna Web Config och välj **Network Security Settings (Nätverkets säkerhetsinställningar) > IPsec/IP Filtering > Basic (Grundläggande) > Default Policy (Standardpolicy)** eller **Group Policy (Gruppolicy)**.

Relaterad information

➔ ["Öppna Web Config" på sidan 20](#)

Det går inte att kommunicera med IPsec-kommunikation

Använder du en algoritm som saknar stöd för datorinställningarna?

Skrivaren har stöd för följande algoritmer.

Lösa problem

Säkerhetsmetoder	Algoritmer
Krypterad algoritm	AES-CBC 128,AES-CBC 192,AES-CBC 256,3DES-CBC,DES-CBC
Hash-algoritm	SHA-1,SHA2-256,SHA2-384,SHA2-512,MD5
Algoritm för nyckelutbyte	Diffi e-Hellman Group2,Diffi e-Hellman Group1*,Diffi e-Hellman Group14* Elliptic Curve Diffi e- Hellman P-256*,Elliptic Curve Diffi e-Hellman P-384*

* Tillgängliga metoder kan variera beroende på modell.

Relaterad information

➔ ["Krypterad kommunikation med IPsec/IP Filtering" på sidan 40](#)

Plötsligt går det inte att kommunicera

Är skrivarens IP-adress ogiltig eller har den ändrats?

Inaktivera IPsec med skrivarens kontrollpanel.

Om DHCP inte är uppdaterad, har startats om eller om IPv6-adressen inte är uppdaterad eller erhållits, kanske det inte går att hitta IP-adressen som registrerats i Web Config (**Network Security Settings (Nätverkets säkerhetsinställningar) > IPsec/IP Filtering > Basic (Grundläggande) > Group Policy (Gruppolicy) > Local Address(Printer) (Lokal adress(skrivare))**). Använd en statisk IP-adress.

Är datorns IP-adress ogiltig eller har den ändrats?

Inaktivera IPsec med skrivarens kontrollpanel.

Om DHCP inte är uppdaterad, har startats om eller om IPv6-adressen inte är uppdaterad eller erhållits, kanske det inte går att hitta IP-adressen som registrerats i Web Config (**Network Security Settings (Nätverkets säkerhetsinställningar) > IPsec/IP Filtering > Basic (Grundläggande) > Group Policy (Gruppolicy) > Remote Address(Host) (Fjärradress (Värd))**). Använd en statisk IP-adress.

Relaterad information

➔ ["Öppna Web Config" på sidan 20](#)

➔ ["Krypterad kommunikation med IPsec/IP Filtering" på sidan 40](#)

Det går inte att skapa en säker IPP-utskriftsport

Är rätt certifikat angett som servercertifikat för SSL/TLS-kommunikation?

Om fel certifikat har angetts kanske det inte går att skapa en port. Kontrollera att du använder rätt certifikat.

Är ett CA-certifikat importerat på datorn som har åtkomst till skrivaren?

Om ett CA-certifikat inte har importerats på datorn kanske det inte går att skapa en port. Kontrollera att ett CA-certifikat har importerats.

Relaterad information

➔ ["Öppna Web Config" på sidan 20](#)

Lösa problem

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

Det inställda värdet kan vara felaktigt.

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

Relaterad information

➔ [”Krypterad kommunikation med IPsec/IP Filtering” på sidan 40](#)

Problem att använda ett digitalt certifikat

Det går inte att importera ett CA-signerat certifikat

Matchar det CA-signerade certifikatet och informationen i CSR varandra?

Det går inte att importera en CSR om det CA-signerade certifikatet och CSR inte innehåller samma information. Kontrollera följande:

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

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

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

Hämta det CA-signerade certifikatet igen med ditt CSR.

Överstiger det CA-signerade certifikatet 5 KB?

Du kan inte importera ett CA-signerat certifikat som överstiger 5 KB.

Används rätt lösenord för import av certifikatet?

Du kan inte importera certifikatet om du har glömt bort lösenordet.

Relaterad information

➔ [”Importera ett CA-signerat certifikat” på sidan 37](#)

Det går inte att uppdatera ett självsignerat certifikat

Har Common Name (Nätverksnamn) angetts?

Du måste ange Common Name (Nätverksnamn).

Används tecken som inte stöds i Common Name (Nätverksnamn)? Exempelvis så stöds inte japanska tecken.

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

Finns det ett komma eller mellanslag i Common Name (Nätverksnamn)?

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

Lösa problem

Relaterad information

➔ [”Uppdatera ett självsignerat certifikat” på sidan 39](#)

Det går inte att skapa en CSR

Har Common Name (Nätverksnamn) angetts?

Du måste ange **Common Name (Nätverksnamn)**.

Används tecken som inte stöds i **Common Name (Nätverksnamn)**, **Organization (Organisation)**, **Organizational Unit (Organisationsenhet)**, **Locality (Plats)**, **State/Province (Stat/provins)**? Exempelvis så stöds inte japanska tecken.

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

Finns det ett komma eller mellanslag i Common Name (Nätverksnamn)?

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

Relaterad information

➔ [”Hämta ett CA-signerat certifikat” på sidan 35](#)

Varningar om ett digitalt certifikat visas

Meddelanden	Orsak/åtgärd
Enter a Server Certificate. (Ange ett Servercertifikat.)	<p>Orsak: Du har inte valt en fil som ska importeras.</p> <p>Åtgärd: Välj en fil och klicka på Import (Importera).</p>
CA Certificate 1 is not entered. (CA-certifikat 1 är inte angivet.)	<p>Orsak: CA-certifikat 1 har inte angetts, endast CA-certifikat 2 har angetts.</p> <p>Åtgärd: Importera CA-certifikat 1 först.</p>
Invalid value below. (Ogiltigt värde nedan.)	<p>Orsak: Filers sökväg och/eller lösenordet innehåller tecken som inte stöds.</p> <p>Åtgärd: Kontrollera att rätt tecken angetts i posten.</p>
Invalid date and time. (Ogiltigt datum och tid.)	<p>Orsak: Datum och klockslag har inte ställts in på skrivaren.</p> <p>Åtgärd: Ställ in datum och tid med Web Config eller Epson Device Admin.</p>

Lösa problem

Meddelanden	Orsak/åtgärd
Invalid password. (Ogiltigt lösenord.)	<p>Orsak: Lösenordet som angetts för CA-certifikatet och det angivna lösenordet matchar inte varandra.</p> <p>Åtgärd: Ange rätt lösenord.</p>
Invalid file. (Ogiltig fil.)	<p>Orsak: Du importerar inte en certifikatfil med X509-format.</p> <p>Åtgärd: Mer information om certifikatet finns på certifikatutfärdarens webbplats.</p>
	<p>Orsak: Filen som du importerade är för stor. Den maximala filstorleken är 5 KB.</p> <p>Åtgärd: Om du valt rätt fil kan certifikatet vara skadat eller förfalskat.</p>
	<p>Orsak: Kedjan i certifikatet är inte giltig.</p> <p>Åtgärd: Mer information om certifikatet finns på certifikatutfärdarens webbplats.</p>
Cannot use the Server Certificates that include more than three CA certificates. (Kan inte använda Servercertifikat som innehåller fler än tre CA-certifikat.)	<p>Orsak: Certifikatfilen i PKCS#12-format innehåller mer än 3 CA-certifikat.</p> <p>Åtgärd: Importera varje certifikat som konverterats från PKCS#12-format till PEM-format eller importera en certifikatfil i PKCS#12-format som innehåller högst 2 CA-certifikat.</p>
The certificate has expired. Check if the certificate is valid, or check the date and time on your printer. (Certifikatet har upphört att gälla. Kontrollera om certifikat är giltigt eller kontrollera datum och tid på din skrivare.)	<p>Orsak: Certifikatet har gått ut.</p> <p>Åtgärd:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Om certifikatet har gått ut ska du hämta och importera ett nytt certifikat. <input type="checkbox"/> Om certifikatet inte har gått ut ska du kontrollera att rätt datum och klockslag ställts in på skrivaren.
Private key is required. (Privat nyckel är obligatoriskt.)	<p>Orsak: Det finns ingen privat nyckel kopplad till certifikatet.</p> <p>Åtgärd:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Om certifikatet är i PEM/DER-formatet och det hämtats med en CSR via en dator ska du ange den privata nyckelfilen. <input type="checkbox"/> Om certifikatet är i PKCS#12-formatet och det hämtats med en CSR via en dator ska du skapa en fil som innehåller den privata nyckeln.
	<p>Orsak: Du har importerat ett PEM/DER-certifikat som hämtats med en CSR med Web Config på nytt.</p> <p>Åtgärd: Om certifikatet är i PEM/DER-format och erhållits med en CSR via Web Config kan du bara importera det en gång.</p>

Lösa problem

Meddelanden	Orsak/åtgärd
Setup failed. (Fel vid inställning.)	Orsak: Det går inte att avsluta konfigurationen eftersom det blev fel i kommunikationen mellan skrivaren och datorn eller filen inte går att läsa på grund av fel. Åtgärd: Importerera filen igen när du har kontrollerat den angivna filen och kommunikationen.

Relaterad information

➔ ["Om digital certifiering" på sidan 34](#)

Ett CA-signerat certifikat har raderats av misstag

Finns det en säkerhetskopia av filen?

Importerera certifikatet igen om du inte har en säkerhetskopia.

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

Relaterad information

➔ ["Radera ett CA-signerat certifikat" på sidan 38](#)

➔ ["Importerera ett CA-signerat certifikat" på sidan 37](#)

Bilaga

Introduktion till nätverksmjukvara

Nedan beskrivs programvaran som konfigurerar och hanterar enheter.

Epson Device Admin

Epson Device Admin är en applikation som gör det möjligt för dig att installera enheter i nätverket och sedan konfigurera och hantera enheterna. Du kan inhämta detaljerad information om enheter, såsom status och förbrukning, skicka varningsmeddelanden och skapa rapporter för enhetsanvändning. Du kan skapa en mall med konfigurationsalternativ och använda den i andra enheter som delade inställningar. Du kan hämta Epson Device Admin från Epsons supportwebbplats. Mer information finns i dokumentationen eller hjälpen för Epson Device Admin.

Kör Epson Device Admin (endast för Windows)

Välj **All Programs (Alla program) > EPSON > Epson Device Admin > Epson Device Admin**.

Obs!

Om en brandväggsvarning visas, tillåt åtkomst för Epson Device Admin.

EpsonNet Print

EpsonNet Print är en programvara för att skriva ut på TCP/IP-nätverket. Programmet har de funktioner och begränsningar som anges nedan.

- Skrivarens status visas på mellanlagringskärmen.
- Skrivaren kan fortfarande identifieras även om skrivarens IP-adress ändras med DHCP.
- Du kan använda en skrivare som är placerad i ett annat nätverkssegment.
- Du kan skriva ut med ett av följande protokoll.
- IPv6-adresser stöds inte.

EpsonNet SetupManager

EpsonNet SetupManager är ett program som skapar ett paket för enkel skrivarinstallation som t.ex. installerar skrivardrivrutinen, installerar EPSON Status Monitor och skapar en skrivarport. Med programmet kan administratörer skapa unika programpaket och distribuera dem till grupper.

För mer information, besök din regionala webbplats för Epson.