EPSON
EXCEED YOUR VISION

# Administratörshandbok

NPD5668-00 SV

# Innehållsförteckning

## *Bilaga*



## *Avancerade säkerhetsinställningar för företag*

# Upphovsrätt

# Varumärken

- ❏ EPSON® är ett registrerat varumärke och EPSON EXCEED YOUR VISION och EXCEED YOUR VISION är varumärken som tillhör Seiko Epson Corporation.
- ❏ Epson Scan 2 software is based in part on the work of the Independent JPEG Group.
- ❏ Google Cloud Print™, Chrome™, Chrome OS™, and Android™ are trademarks of Google Inc.
- ❏ Microsoft®, Windows®, Windows Server®, and Windows Vista® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Macintosh, Mac OS, OS X, AirMac, Bonjour, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint is a trademark of Apple Inc.
- ❏ Allmänt: Andra produktnamn som förekommer i detta dokument används endast i identifieringssyfte och kan vara varumärken som tillhör respektive ägare. Epson frånsäger sig all rätt till dessa varumärken.

# Om den här handboken

## Markeringar och symboler

> ⚠ ***Obs!***
> *Instruktioner som måste följas noga för att undvika kroppsskador.*

> ***Viktigt:***
> *Instruktioner som måste följas för att undvika skador på utrustningen.*

***Anmärkning:***
*Instruktioner som innehåller praktiska råd och information om begränsningar när skannern används.*

### Relaterad information

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

## Beskrivningar som används i den här användarhandboken

❏ Skärmbilder av skannerdrivrutinen och Epson Scan 2 (skannerdrivrutin) är från Windows 10 eller OS X El Capitan. Innehållet som visas på skärmarna varierar beroende på modell och situation.

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

❏ Vissa menyobjekt på LCD-skärmen kan variera beroende på modell och inställningar.

## Referenser för operativsystem

### Windows

I den här handboken avser ord som ”Windows 10”, ”Windows 8.1”, ”Windows 8”, ”Windows 7”, ”Windows Vista”, ”Windows XP”, ”Windows Server 2016”, ”Windows Server 2012 R2”, ”Windows Server 2012”, ”Windows Server 2008 R2”, ”Windows Server 2008”, ”Windows Server 2003 R2”, och ”Windows Server 2003” 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
- ❏ Microsoft® Windows Server® 2016 operativsystem
- ❏ Microsoft® Windows Server® 2012 R2 operativsystem
- ❏ Microsoft® Windows Server® 2012 operativsystem
- ❏ Microsoft® Windows Server® 2008 R2 operativsystem
- ❏ Microsoft® Windows Server® 2008 operativsystem
- ❏ Microsoft® Windows Server® 2003 R2 operativsystem
- ❏ Microsoft® Windows Server® 2003 operativsystem

### Mac OS

I denna handbok används ”Mac OS” som referens till macOS Sierra, OS X El Capitan, OS X Yosemite, OS X Mavericks, OS X Mountain Lion, Mac OS X v10.7.x och Mac OS X v10.6.8.

# Introduktion

## Manuell komponent

Den här manualen är för enhetsadministratören som ansvarar för att ansluta skrivaren eller skannern till nätverket och innehåller information om hur du gör inställningar för att använda funktionerna.

Se *Användarhandbok* för funktionsanvändningsinformation.

#### Förberedelse

Beskriver administratörens uppgifter, hur du konfigurerar enheter och mjukvara för hantering.

#### Anslutning

Beskriver hur du ansluter en enhet till nätverket eller telefonlinjen. Den beskriver även nätverksmiljön, exempelvis användning av en port för enheten, DNS och proxyserverinformation.

#### Funktionsinställningar

Förklarar inställningarna för varje enhetens funktion.

#### Grundläggande säkerhetsinställningar

Beskriver inställningar för varje funktion, såsom utskrift, skanning och faxning.

#### Funktions- och administrationsinställningar

Beskriver funktionerna efter att du börjat använda enheterna, såsom informationskontroll och underhåll.

#### Lösa problem

Beskriver återställning av inställningar och felsökning av nätverket.

#### Avancerade säkerhetsinställningar för företag

Beskriver inställningsmetod för att förbättra enhetens säkerhet, såsom användning av CA-certifikat, SSL/TLS-kommunikation och IPsec-/IP-filtering.

Beroende på modell stöds inte vissa funktioner i det här kapitlet.

## 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 ansvarar 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.

### Web Config(enhetens webbsida)

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

### Verktyg

En generisk term för mjukvaran för att konfigurera eller hantera en enhet, såsom Epson Device Admin, EpsonNet Config, EpsonNet SetupManager etc.

### Push-skanning

En generisk term för skanning från enhetens kontrollpanel.

### 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 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

I det här kapitlet beskrivs rollen för administratören och förberedelsen innan du gör inställningarna.

## Flöde för skannerinställningar och hantering

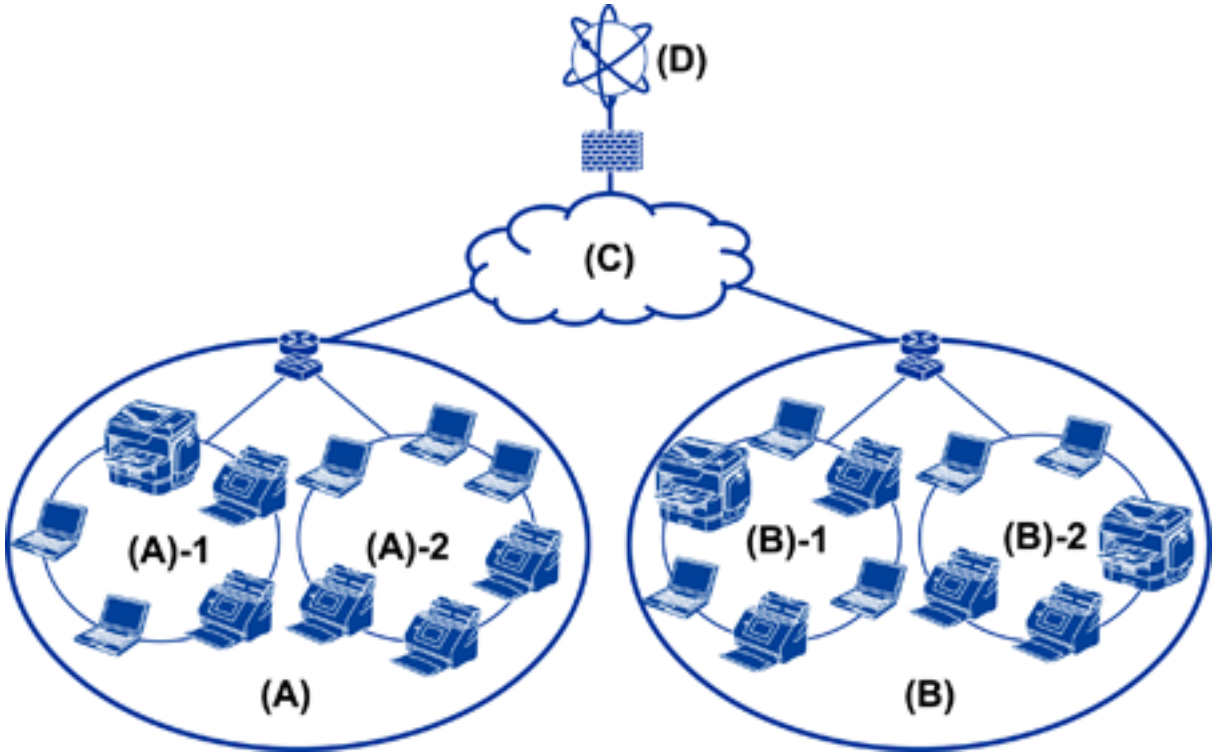
Administratören gör nätverksanslutningsinställningar, initial konfiguration och underhåll av skanner så den kan vara tillgänglig för användare.

1. Förberedelse
   - ❏ Samla in information om anslutningsinställningar
   - ❏ Beslut för anslutningsmetod
2. Anslutning
   - ❏ Nätverksanslutning från skannerns kontrollpanel
3. Konfigurera funktioner
   - ❏ Skannerdrivrutinsinställningar
   - ❏ Övriga avancerade inställningar
4. Säkerhetsinställningar
   - ❏ Administratörsinställningar
   - ❏ SSL/TLS
   - ❏ Protokollstyrning
   - ❏ Avancerade säkerhetsinställningar (tillbehör)
5. Användning och hantering
   - ❏ Kontrollera enhetens status
   - ❏ Hantering vid eventutveckling
   - ❏ Säkerhetskopiering av enhetsinställningar

### Relaterad information

➡ ”Förberedelse” på sidan 10
➡ ”Anslutning” på sidan 15
➡ ”Funktionsinställningar” på sidan 22
➡ ”Grundläggande säkerhetsinställningar” på sidan 32
➡ ”Funktions- och administrationsinställningar” på sidan 40

# Exempel på nätverksmiljö




(A): Office 1

❏ (A) – 1: LAN 1

❏ (A) – 2: LAN 2

(B): Office 2

❏ (B) – 1: LAN 1

❏ (B) – 2: LAN 2

(C): WAN

(D): Internet

## Introduktion till exempel på skanneranslutningsinställning

Det finns huvudsakligen två anslutningstyper beroende av hur du använder skannern. Båda ansluter skannern till nätverket och dator med hubben.

❏ Server-/klientanslutning (skanner som använder Windows-server, jobbhantering)

❏ Peer to peer-anslutning (direkt anslutning till klientens datorn)

### Relaterad information

➡ ”Server-/klientanslutning” på sidan 12

➡ ”Peer to Peer-anslutning” på sidan 12

## Server-/klientanslutning

Centralisera skanner- och jobbhantering med Document Capture Pro Server som finns installerad på servern. Det är mest lämpat för arbete som använder flera skannrar för att skanna ett stort antal dokument i ett visst format.

### Relaterad information

➡ ”Definition av termer som används i den här handboken” på sidan 8

## Peer to Peer-anslutning

Använd en individuell skanner med skannerdrivrutin som Epson Scan 2 som finns installerad på klientdatorn. Om du installerar Document Capture Pro (Document Capture) på klientdatorn kan du utföra jobb på skannerns individuella klientdatorer.

### 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.

| Avdelningar | Alternativ | Anmärkning |
|---|---|---|
| Enhetsanslutningsmetod | ❏ Ethernet | Använd en kategori 5e- (eller högre) STP-kabel (Shielded twisted pair) för Ethernet-anslutning. |
| LAN-anslutningsinformation | ❏ IP-adress<br>❏ Nätmask<br>❏ Standard-gateway | Om du automatiskt konfigurerar IP-adressen med DHCP-funktionen för routern krävs det inte. |
| DNS-serverinformation | ❏ IP-adress för primär DNS<br>❏ IP-adress för sekundär DNS | Om du använder en statisk IP-adress som IP-adress, ska du konfigurera DNS-servern.<br>Konfigurera automatiskt vid tilldelning med DHCP-funktionen och när DNS-servern inte kan tilldelas automatiskt. |
| Proxy-serverinformation | ❏ Proxy-servernamn<br>❏ Portnummer | Konfigurera vid användning av en proxy-server för Internet-anslutning och vid användning av Epson Connect-tjänsten eller den automatiska firmware-uppdateringsfunktionen. |

## Skannerspecifikationer

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

# Använda portnummer

Se ”Bilaga” för portnumret som skannern använder.

### Relaterad information

➡ ”Använda port för skannern” på sidan 60

# Typ av IP-adresstilldelning

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

### Statisk IP-adress:

Tilldela förutbestämd unik IP-adress för skannern.

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

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

### Automatisk tilldelning via DHCP-funktion:

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

Det är obekvämt att ändra IP-adressen för en viss enhet, reservera IP-adressen i förväg och sedan tilldela den.

# DNS-server och Proxy-server

Om du använder en Internet-anslutningstjänst ska du konfigurera DNS-servern. Om du inte konfigurerar den kan du behöva specificera IP-adressen för åtkomst, eftersom du inte kan hantera namnupplösning.

Proxyservern placeras i gatewayen mellan nätverket och Internet och kommunicerar med datorn, skannern och Internet (motsatt server) för var och en av dem. Motsatt server kommunicerar endast med proxyservern. Därför kan skannerinformation, såsom IP-adress och portnummer inte läsas och en ökad säkerhet förväntas.

Du kan hindra åtkomst för en specifik URL genom att använda filtreringsfunktion, eftersom proxyservern kan kontrollera kommunikationsinnehållet.

# Metod för inställning av nätverksanslutning

För anslutningsinställnignar för skannerns IP-adress, nätmask och standardgateway, fortsätt enligt följande.

### Skanna med hjälp av kontrollpanelen:

Konfigurera inställningarna med skannerns kontrollpanel för varje skanner. Anslut till nätverket efter konfiguration av skannerns anslutningsinställningar.

### Använda installationsprogrammet:

Om installationsprogrammet används ställs skannerns och klientdatorns nätverk in automatiskt. Inställningarna är tillgängliga enligt installationsprogrammets instruktioner, även om du inte har djupgående kunskaper om nätverket.

### Använda ett verktyg:

Använd ett verktyg från administratörens dator. Du kan hitta en skanner och sedan konfigurera skannern, eller skapa en SYLK-fil för att skapa batch-inställningar för skannrar. Du kan konfigurera många skannrar, men de behöver anslutas fysiskt till Ethernet-kabeln före inställning. Vi rekommenderar därför att du kan skapa Ethernet för inställningen.

### Relaterad information

➡ ”Ansluta till nätverket från kontrollpanelen” på sidan 15

➡ ”Ansluta till nätverket med installationsprogrammet” på sidan 19

➡ ”Tilldela en IP-adress med EpsonNet Config” på sidan 56

# Anslutning

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

## Ansluta till nätverket

### Ansluta till nätverket från kontrollpanelen

Anslut skannern till nätverket via skannerns kontrollpanel.

För skannerns kontrollpanel, se *Användarhandbok* för mer information.

#### Tilldela IP-adress

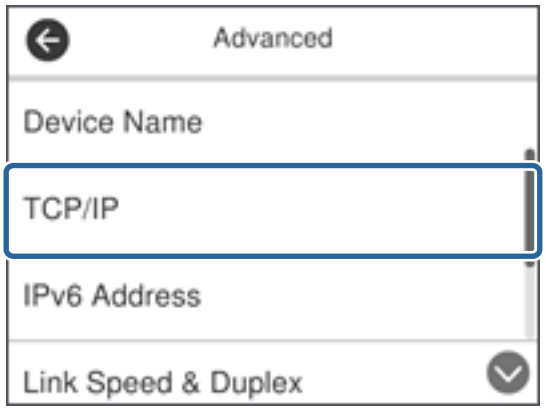
Konfigurera de grundläggande objekten, såsom IP-adress, Subnetmask och Standardgateway.

1. Starta skannern.
2. Snärta till åt vänster på skärmen för skannerns kontrollpanel och tryck sedan på **Inst.**.

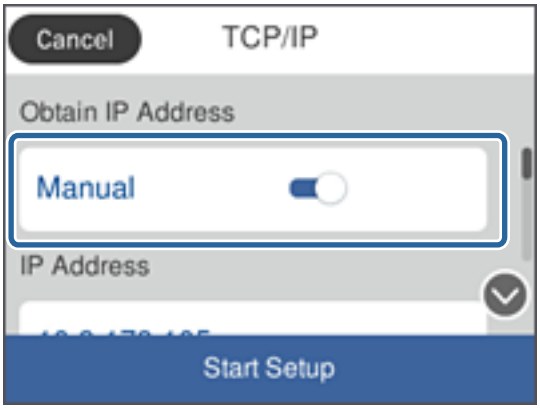

3. Tryck på **Nätverksinställningar** > **Ändra inställningar**.

   Om alternativet inte visas snärtar du uppåt på skärmen för att visa den.

4. Tryck på **TCP/IP**.

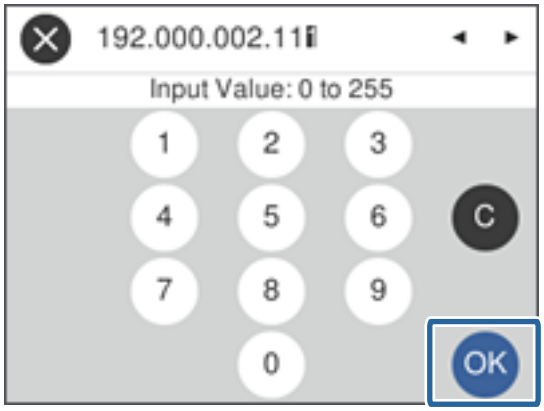



5. Välj **Manuell** för **Erhåll IP-adress**.




***Anmärkning:***
*När du konfigurerar IP-adressen automatiskt genom att använda DHCP-funktionen för routern, väljer du **Auto**. I så fall ställs **IP-adress**, **Subnetmask** och **Standardgateway** i steg 6 till 7 in automatiskt, så gå vidare till steg 8.*

6. Tryck på **IP-adress**-fältet, ange IP-adressen med tangentbordet som visades på skärmen och tryck sedan på **OK**.




Kontrollera värdet som visas på föregående skärm.

7. Konfigurera **Subnetmask** och **Standardgateway**.

   Kontrollera värdet som visas på föregående skärm.

   ***Anmärkning:***
   *Om kombinationen av IP-adress, Subnetmask och Standardgateway är felaktiga, är **Börja konfiguration** inaktiv och kan inte fortsätta med inställningarna. Kontrollera att det inte finns något fel i inmatningen.*

8. Tryck på **Primär DNS**-fältet för **DNS-server**, ange IP-adressen för primär DNS-server med tangentbordet som visas på skärmen och tryck sedan på **OK**.

   Kontrollera värdet som visas på föregående skärm.

   ***Anmärkning:***
   *När du väljer **Auto** för IP-adresstilldelningsinställningar kan du välja DNS-serverinställningar från **Manuell** eller **Auto**. Om du inte kan erhålla DNS-serveradressen automatiskt ska du välja **Manuell** och ange DNS-serveradressen. Ange sedan den sekundära DNS-serveradressen direkt. Om du väljer **Auto** går du till steg 10.*

9. Tryck på **Sekundär DNS**-fältet, ange IP-adressen för primär DNS-server med tangentbordet som visas på skärmen och tryck sedan på **OK**.

   Kontrollera värdet som visas på föregående skärm.

10. Tryck på **Börja konfiguration**.

11. Tryck på **Stäng** på bekräftelseskärmen.

    Skärmen stängs av automatiskt efter en viss tid om du inte trycker på **Stäng**.

## Ansluta till Ethernet

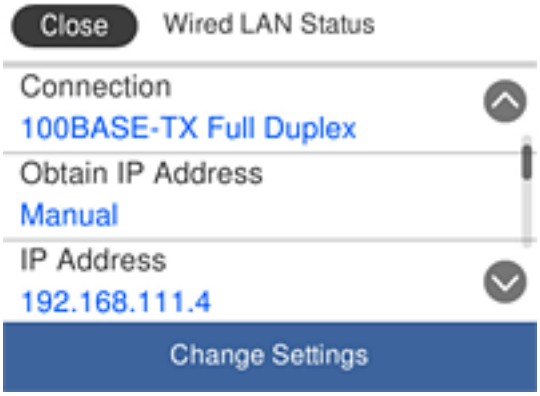
Anslut skannern till nätverket med Ethernet-kabeln och kontrollera anslutningen.

1. Anslut skannern och hubben (L2-brytare) med Ethernet-kabeln.

   Ikonen på startskärmen ändras till  .

2. Tryck på  på startskärmen.

3. Bläddra upp på skärmen och kontrollera att anslutningsstatusen och IP-adressen är rätt.



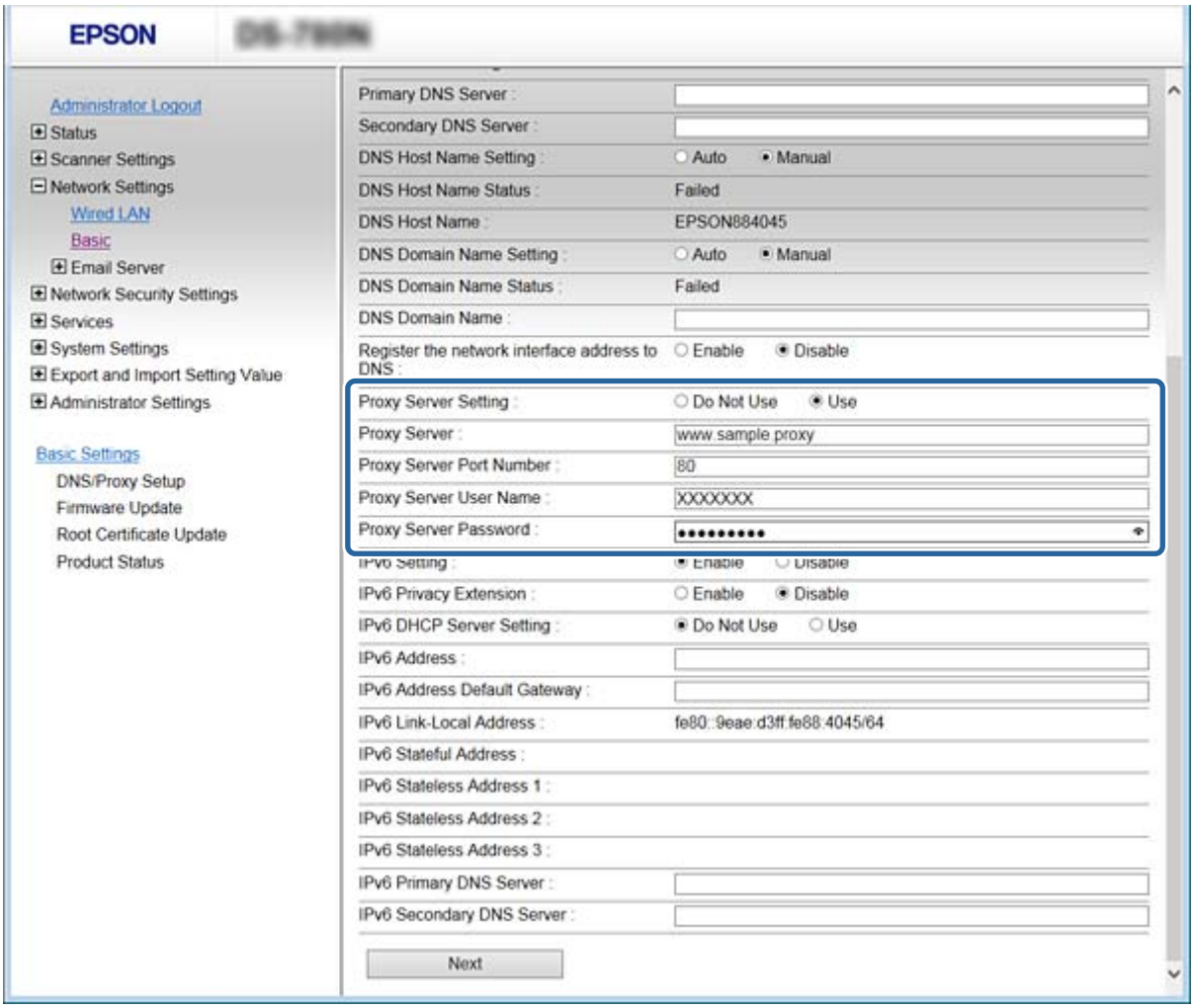

## Inställning av proxyserver

Proxyservern kan inte ställas in via panelen. Konfigurera med Web Config.

1. Öppna Web Config och välj **Network Settings** > **Basic**.
2. Välj **Use** i **Proxy Server Setting**.
3. Specificera proxyservern i IPv4-adress eller FQDN-format under **Proxy-server** och ange sedan portnumret i **Proxy Server Port Number**.

   För proxyservrar som kräver autentisering, ange användarnamnet för autentisering av proxyservern och lösenordet för autentisering av proxyservern.

4. Klicka på knappen **Next**.




5. Bekräfta inställningarna och klicka sedan på **Inst.**.

### Relaterad information

➡ ”Öppna Web Config” på sidan 23

## Ansluta till nätverket med installationsprogrammet

Vi rekommenderar att du använder installationsprogrammet för att ansluta skannern till en dator. Du kan köra installationsprogrammet med en av metoderna nedan.

❏ Ställa in via webbplatsen

Gå till följande webbplats och ange sedan produktens namn. Gå till **Inställning** och starta konfigurationen.

http://epson.sn

❏ Körs från mjukvaruskivan (endast för modeller som levereras med en mjukvaruskiva och användare med datorer med skivenheter.)

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

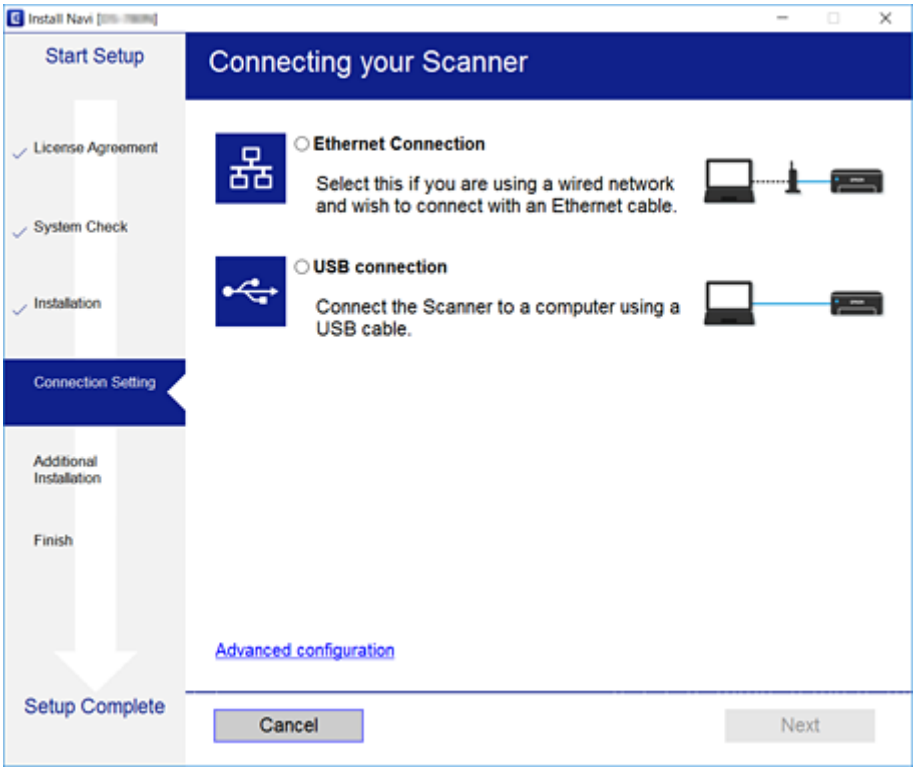
**Anslutning**

### Välja anslutningsmetoder

Följ instruktionerna på skärmen tills följande skärm visas och välj sedan anslutningssätt för skanner till dator.

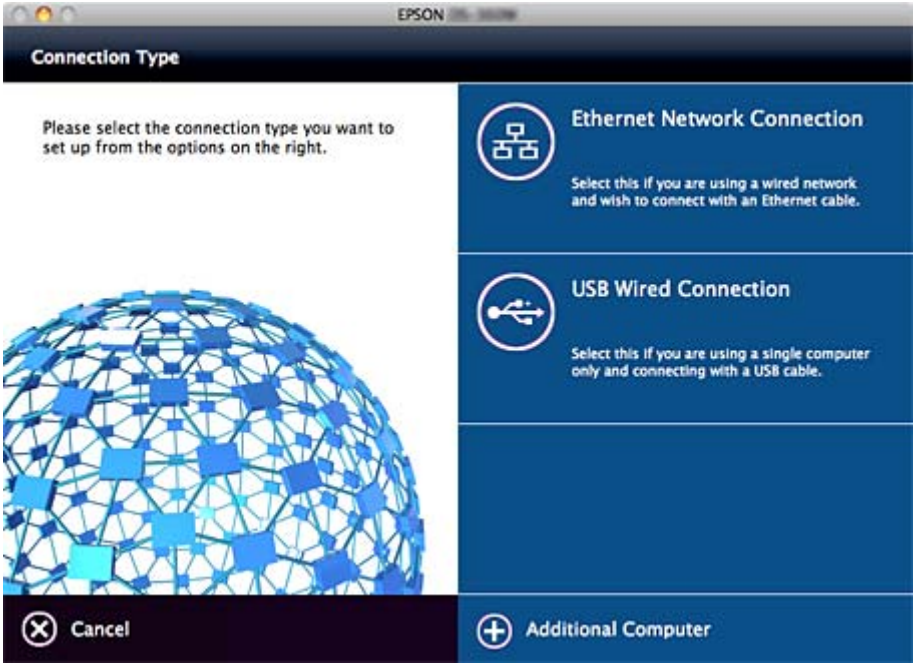
❏ Windows

Välj anslutningstypen och klicka på **Nästa**.




❏ Mac OS

Välj anslutningstyp.



## Anslutning

Följ instruktionerna på skärmen. Nödvändig mjukvara installeras.

# Funktionsinställningar

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

# Mjukvara för inställning

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

## Web Config (webbsida för enhet)

### Om Web Config

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

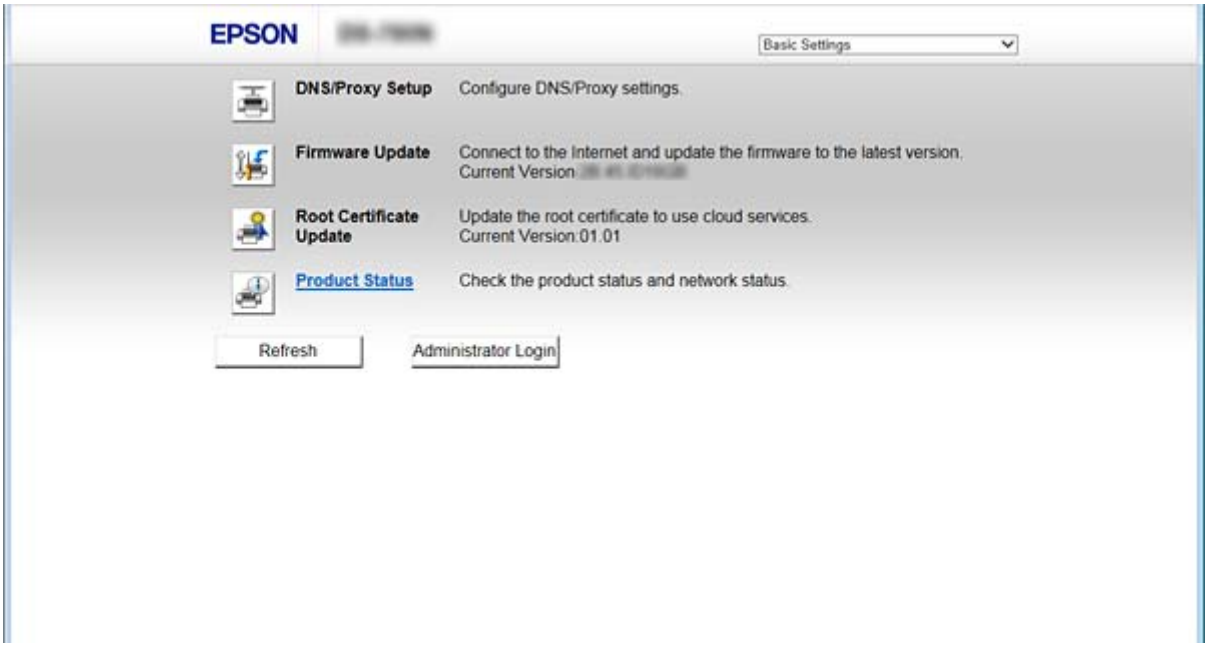
När du vill öppna Web Config måste du först tilldela en IP-adress till skannern.

***Anmärkning:***
*Du kan spärra inställningarna genom att konfigurera ett administratörslösenord på skannern.*

Det finns två inställningssidor som visas nedan.

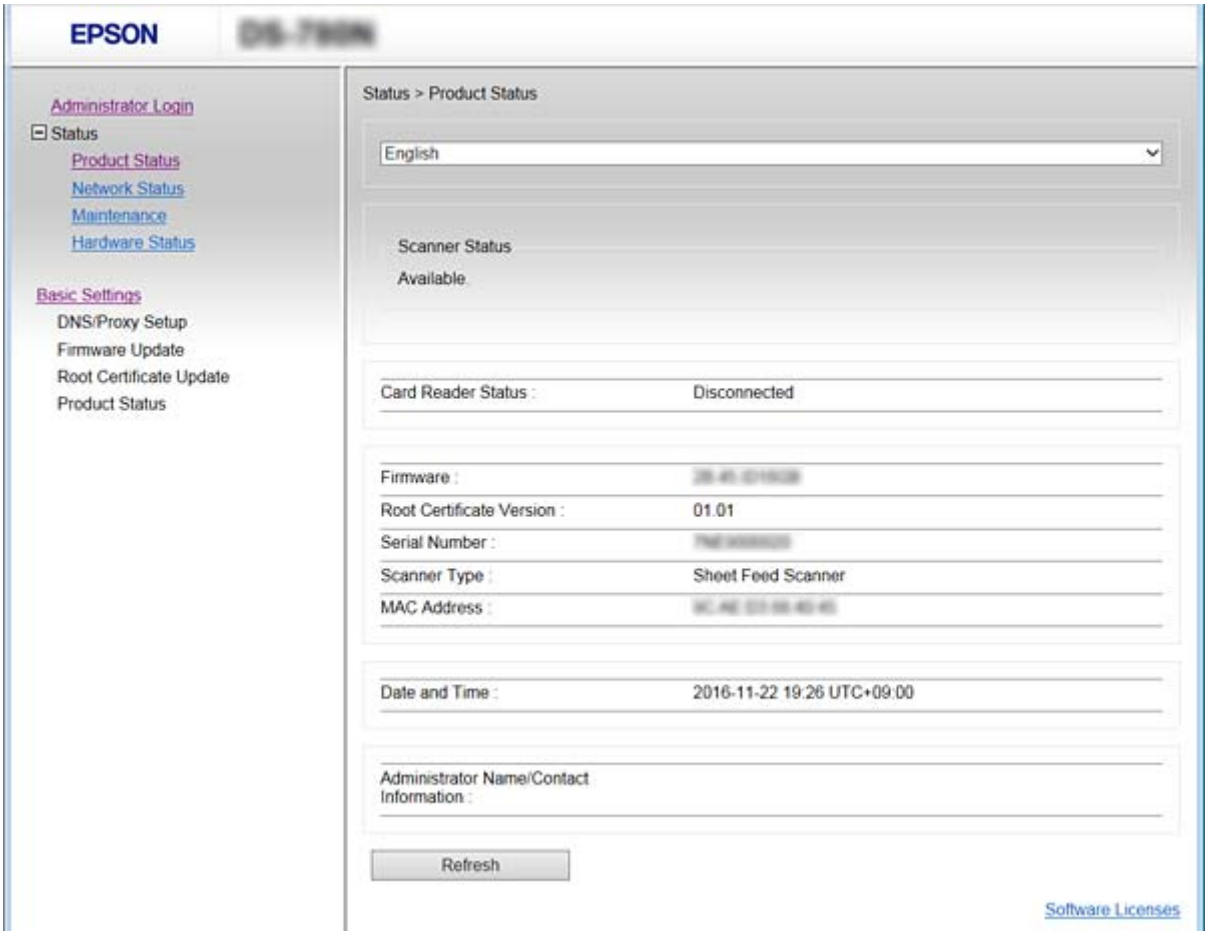
❏ **Basic Settings**

Du kan konfigurera grundläggande inställningar för skannern.



❏ **Advanced Settings**

Du kan konfigurera avancerade inställningar för skannern. Den här sidan är främst avsedd för administratörer.




## Öppna Web Config

Ange skannerns IP-adress i en webbläsare. JavaScript måste vara aktiverat. När du öppnar Web Config via HTTPS, visas ett varningsmeddelande i webbläsaren, eftersom ett självsignerat certifikat, som lagrats i skannern, används.

❏ Åtkomst via HTTPS

IPv4: https://<skannerns IP-adress> (utan < >)

IPv6: https://[skannerns IP-adress] (med [ ])

❏ Åtkomst via HTTP

IPv4: http://<skannerns IP-adress> (utan < >)

IPv6: http://[skannerns IP-adress] (med [ ])

***Anmärkning:***

❏ *Exempel*

*IPv4:*

*https://192.0.2.111/*

*http://192.0.2.111/*

*IPv6:*

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

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

❏ *Om skannerns namn är registrerat med DNS-servern kan du använda skannernamnet i stället för skannerns IP-adress.*

**Relaterad information**

➡ ”SSL-/TLS-kommunikation med skannern” på sidan 63

➡ ”Om digital certifiering” på sidan 63

# Använda skanningfunktionerna

Beroende av hur du använder skannern, installera följande programvara och utför inställningar med den.

❏ **Skanna från dator**

❏ Bekräfta validiteten av nätverksskanningstjänsten med Web Config (giltig fabriksleverans).

❏ Installera Epson Scan 2 på din dator och konfigurera IP-adressen

❏ När du skannar med jobb,installera Document Capture Pro (Document Capture) och ställ in jobbinställningar.

❏ **Skanna från kontrollpanel**

❏ När du använder Document Capture Pro eller Document Capture Pro Server:

Installera Document Capture Pro eller Document Capture Pro Server

DCP-inställning (serverläge, klientläge).

❏ Om du använder WSD-protokollet:

Bekräfta validiteten av WSD på Web Config eller kontrollpanel (giltig fabriksleverans)

Ytterligare enhetsinställning (dator med Windows).

## Skanna från en dator

Installera mjukvaran och gör det möjligt för nätverksskanningtjänsten att skanna via ett nätverk från datorn.

**Relaterad information**

➡ ”Mjukvara som ska installeras” på sidan 25

➡ ”Aktivera nätverksskanning” på sidan 25

## Mjukvara som ska installeras

❏ Epson Scan 2

Det här är skannerdrivrutinen. Om du använder enheten från en dator installerar du drivrutinen på varje klientdator. Om Document Capture Pro/Document Capture har installerats kan du utföra funktionerna som tilldelats till enhetens knappar.

Med EpsonNet SetupManager, kan skrivardrivrutiner distribueras tillsammans i paket.

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

Installera på klientdatorn. Du kan ta fram och utföra jobb registrerade på en dator med Document Capture Pro/Document Capture som finns installerad i nätverken från datorns och skannerns kontrollpanel.

Du kan också skanna från datorn via nätverket. Epson Scan 2 behöver skannas.

### Relaterad information

➡ ”EpsonNet SetupManager” på sidan 56

## Konfigurera skannerns IP-adress för Epson Scan 2

Specificera skannerns IP-adress, så att skannern kan användas i nätverket.

1. Starta **Epson Scan 2 Utility** via **Start** > **Alla program** > **EPSON** > **Epson Scan 2**.

   Om en annan skanner redan finns registrerad, gå till steg 2.

   Om ingen finns registrerad, gå till steg 4.

2. Klicka ▼ på **Skanner**.

3. Klicka på **Inställningar**.

4. Klicka på **Aktivera redigering** och klicka sedan på **Lägg till**.

5. Välj skannerns modellnamn från **Modell**.

6. Välj skannerns IP-adress som ska användas från **Adress** i **Sök efter nätverk**.

   Klicka på  och klicka på  för att uppdatera listan. Om du inte kan hitta skannerns IP-adress, välj **Ange adress** och ange IP-adressen.

7. Klicka på **Lägg till**.

8. Klicka på **OK**.

## Aktivera nätverksskanning

Du kan konfigurera tjänsten för nätverksskanning när du skannar från en klientdator över nätverket. Standardinställningarna aktiveras.

1. Öppna Web Config och välj **Services** > **Network Scan**.

2. Se till att **Enable scanning** för **EPSON Scan**väljs.

   Om det har valts, är denna uppgift slutförd. Stäng Web Config.

   Om det har rensats, välj det och gå till nästa steg.

3. Klicka på **Next**.

4. Klicka på **OK**.

   Nätverket kopplas upp på nytt och inställningarna aktiveras.

### Relaterad information

➡ ”Öppna Web Config” på sidan 23

## Skanna med hjälp av kontrollpanelen

Funktionen skanna till en mapp och skanna till e-post med skannerns kontrollpanel samt överföring av skanningsresultat till e-post, mappar o.s.v. utförs genom att genomföra ett jobb från datorn.

Konfigurera jobbet med Document Capture Pro Server eller Document Capture Pro när du överför skanningsresultat.

För mer information om inställningar och hur du konfigurerar jobbet, se dokumentationer eller hjälpen för Document Capture Pro Server eller Document Capture Pro.

### Relaterad information

➡ ”Document Capture Pro Server/Document Capture Pro-inställningar” på sidan 26

➡ ”Inställningar av servrar och mappar” på sidan 27

## Programvara att installeras på datorn

❏ **Document Capture Pro Server**

Detta är serverversionen av Document Capture Pro. Installera den på en Windows-server. Flera enheter och jobb kan hanteras centralt via servern. Jobb kan utföras samtidigt från flera skannrar.

Genom att använda den certifierade versionen av Document Capture Pro Server, kan du hantera jobb- och skanningshistorik som är länkad till användare och grupper.

För mer information omDocument Capture Pro Server, kontakta ditt lokala Epson-kontor.

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

Precis som skanning från en dator, kan du ta fram jobb registrerade på datorn från kontrollpanelen och genomföra dem. Det är inte möjligt att köra datorjobb samtidigt från flera skannrar.

## Document Capture Pro Server/Document Capture Pro-inställningar

Utför inställningar för att använda skanningfunktionen via skannerns kontrollpanel.

1. Öppna Web Config och välj **Services** > **Document Capture Pro**.

2. Välj **Driftsläge**.
   - ❏ Server Mode:

     Välj detta om du använder Document Capture Pro Server eller om du använder Document Capture Pro endast för jobb som kan ställts in för en specifik dator.
   - ❏ Client Mode:

     Ställ in detta om du väljer jobbinställningar avDocument Capture Pro (Document Capture) som finns installerade på varje klientdator i nätverket utan att specificera datorn.
3. Ställ in följande enligt det valda läget.
   - ❏ Server Mode:

     Under **Server Address**, specificera servern där Document Capture Pro Server är installerad. Det kan vara mellan 2 och 252 tecken med IPv4-, IPv6-, värdnamns- eller FQDN-format. I FQDN-format kan US-ASCII-bokstäver, siffror, alfabet och bindestreck (förutom främre och bakre) användas.
   - ❏ Client Mode:

     Specificera **Group Settings** för att använda en skannergrupp som specificerades i Document Capture Pro (Document Capture).
4. Klicka på **Inst.**.

### Relaterad information

➡ ”Öppna Web Config” på sidan 23

## Inställningar av servrar och mappar

Document Capture Pro och Document Capture Pro Server sparar skannade data på servern eller klientdatorn en gång och använder överföringsfunktionen för att utföra funktionen skanna till en mapp eller funktionen skanna till e-post.

Du behöver auktoriteten och informationen för att överföra från datorn på vilken Document Capture Pro, Document Capture Pro Server är installerad till datorn eller molntjänsten.

Förbered informationen för funktionen du kommer att använda, ta hänsyn till följande.

Du kan utföra inställningar för dessa funktioner med Document Capture Pro eller Document Capture Pro Server. För mer information om inställningarna, se dokumentationen eller hjälpen till Document Capture Pro Server eller Document Capture Pro.

| Namn | Inställningar | Krav |
|---|---|---|
| Skanna till nätverksmapp (SMB) | Skapa och konfigurera delning av mapp för sparande | Det administrativa användarkontot till datorn som skapar mappar för sparande. |
| | Destination för Skanna till nätverksmapp (SMB) | Användarnamn och lösenord för att logga in på datorn som har en mapp för sparande och behörighet att uppdatera mappen för sparande. |
| Skanna till nätverksmapp (FTP) | Konfiguration för inloggning på FTP-server | Inloggningsinformation till FTP-servern och behörighet att uppdatera mappen för sparande. |

| Namn | Inställningar | Krav |
|---|---|---|
| Skanna till e-post | Konfiguration för e-postserver | Konfigurationsinformation för e-post-server |
| Skanna till Document Capture Pro (vid användning av Document Capture Pro Server) | Konfigurera för inloggning till moln-tjänster | Internet-anslutningsmiljö<br>Registrering av kontot för molntjänster |

### Använd WSD-skanning (endastWindows)

Om datorn kör med Windows Vista eller senare, kan du använda WSD-skanning.

Om WSD-protokollet kan användas, kommer **Dator (WSD)**-menyn att visas på skannerns kontrollpanel.

1. Öppna Web Config och välj **Services** > **Protocol**.
2. Bekräfta att **Enable WSD** har kontrollerats i **WSD Settings**.
   Om den har kontrollerats, är din uppgift slutförd och du kan stänga Web Config.
   Om den inte har kontrollerats, kontrollera den och fortsätt till nästa steg.
3. Klicka på knappen **Next**.
4. Bekräfta inställningarna och klicka på **Inst.**.

# Göra systeminställningar

## Göra systeminställningar från kontrollpanelen

### Ställa in skärmens ljusstyrka

Ställa in LCD-skärmens ljusstyrka.

1. Tryck på **Inst.** på startskärmen.
2. Tryck på **Standardinställningar** > **LCD-ljusstyrka**.
3. Klicka på  eller  för att justera ljusstyrkan.
   Du kan justera från 1 till 9.
4. Tryck på **OK**.

### Ställa in ljud

Ställa in ljud för panelåtgärder och ljud vid fel.

1. Tryck på **Inst.** på startskärmen.
2. Tryck på **Standardinställningar** > **Ljud**.
3. Ställ in följande objekt efter behov.
   - ❏ Åtgärdsljud
     Ställ in volymen av åtgärdsljudet för kontrollpanelen.
   - ❏ Felljud
     Ställ in volymen av felljudet.
4. Tryck på **OK**.

### Relaterad information

➡ ”Öppna Web Config” på sidan 23

## Identifiera dubbelmatning av original

Bestäm funktionen som ska identifiera dubbelmatning av dokumentet som ska skannas och stoppa skanningen om det matas flera gånger.

För att skanna original som tycks vara matade flera gånger, som kuvert eller papper med klistermärken, ställ in dem till av.

***Anmärkning:***
*Det kan också ställs in via Web Config eller Epson Scan 2.*

1. Tryck på **Inst.** på startskärmen.
2. Tryck på **Externa Skanningsinställningar** > **Ultraljudsidentifiering av dubbelmatn.**.
3. Tryck på **Ultraljudsidentifiering av dubbelmatn.** för att sätta på och stänga av det.
4. Tryck på **Stäng**.

## Ställa in låghastighetsläge

Ställ in för att skanna med låg hastighet, så att papperet inte fastnar när du skannar tunna dokument som remsor.

1. Tryck på **Inst.** på startskärmen.
2. Tryck på **Externa Skanningsinställningar** > **Långsam**.
3. Tryck på **Långsam** för att sätta på och stänga av det.
4. Tryck på **Stäng**.

# Göra systeminställningar med Web Config

## Energisparinställningar under inaktivitet

Gör inställningar för energibesparing för skannerns inaktivitetsperiod. Ställ in tiden beroende på användarmiljö.

***Anmärkning:***
*Du kan också utföra inställningar för energibesparing via skanners kontrollpanel.*

1. Öppna Web Config och välj **System Settings** > **Power Saving**.
2. Ange tiden för **Sleep Timer** för att växla till energisparläge när inaktiviteten uppstår.

   Du kan ange upp till 240 minuter per minut.
3. Välj avstängningstid för **Power Off Timer**.
4. Klicka på **OK**.

### Relaterad information

➡ ”Öppna Web Config” på sidan 23

## Konfigurera kontrollpanelen

Konfiguration för skannerns kontrollpanel. Du kan göra följande konfigurationer.

1. Öppna Web Config och välj **System Settings** > **Control Panel**.
2. Ställ in andra alternativ efter behov.
   - ❏ Language

     Välj det språk som visas på kontrollpanelen.
   - ❏ Panel Lock

     Om du väljer **ON** krävs administratörslösenordet när du utför en åtgärd som kräver administratörens behörighet. Om administratörslösenordet inte har konfigurerats inaktiveras panellåset.
   - ❏ Operation Timeout

     Om du väljer **ON**, när du loggar in som administratör, loggas du automatiskt ut och går till den initiala skärmen om det inte förekommer någon aktivitet under en viss tidsperiod.

     Du kan ange mellan 10 sekunder och 240 minuter per sekund.
3. Klicka på **OK**.

### Relaterad information

➡ ”Öppna Web Config” på sidan 23

## Ställa in begränsningar i det externa gränssnittet

Du kan begränsa USB-anslutningen via datorn. Ställ in det för att begränsa skanning på ett annat sätt än via nätverket.

1. Öppna Web Config och välj **System Settings** > **External Interface**.
2. Välj **Enable** eller **Disable**.

   För att begränsa, välj **Disable**.
3. Tryck på **OK**.

## Synkronisera datum och tid med tidsservern

Om du använder ett CA-certifikat kan du förhindra problem med tiden.

1. Öppna Web Config och välj **System Settings** > **Date and Time** > **Time Server**.
2. Välj **Use** för **Use Time Server**.
3. Ange tidsserveradress för **Time Server Address**.

   Du kan använda IPv4-, IPv6- eller FQDN-format. Ange 252 tecken eller mindre. Om du inte specificerar detta ska du lämna det blankt.
4. Ange **Update Interval (min)**.

   Du kan ange upp till 10 800 minuter per minut.
5. Klicka på **OK**.

   ***Anmärkning:***
   *Du kan bekräfta anslutningsstatus med tidsservern på* ***Time Server Status****.*

### Relaterad information

➡ ”Öppna Web Config” på sidan 23

# Grundläggande säkerhetsinställningar

Det här kapitlet beskriver de grundläggande säkerhetsinställningarna som inte kräver en speciell miljö.

## Introduktion till grundläggande säkerhetsfunktioner

Vi introducerar de grundläggande säkerhetsfunktionerna för Epsons enheter.

| Funktionsnamn | Funktionstyp | Vad du kan konfigurera | Vad du kan förhindra |
|---|---|---|---|
| Konfiguration för administratörslösenord | Lås inställningarna som tillhör till systemet, som nätverksanslutningsinställningar och inställningar för USB-anslutning, så att ingen kan ändra dem förutom administratören. | En administratör konfigurerar ett lösenord för enheten.<br>Konfiguration eller uppdatering finns tillgängligt överallt via Web Config, kontrollpanelen, Epson Device Admin, och EpsonNet Config. | 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 säkerhetspolicyn. |
| SSL/TLS-kommunikation | När du gå till en Epson-server på Internet från en enhet, som att kommunicera med en datorn via en webbläsare eller firmware-uppdatering, är kommunikationsinnehåller krypterat med SSL/TLS-kommunikation. | Få ett CA-signerat certifikat och importera det sedan till skannern. | 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. |
| Kontrollprotokoller | Kontrollprotokoller används för kommunikation mellan enheter och datorer och aktiverar/inaktiverar funktioner. | Ett protokoll eller en tjänst som verkställs för funktioner tillåts eller förbjuds separat. | Genom att minska säkerhetsrisker som kan uppstå vid oavsiktlig användning där användare förhindras från att använda onödiga funktioner. |

### Relaterad information

➡ ”Om Web Config” på sidan 22
➡ ”EpsonNet-konfig” på sidan 55
➡ ”Epson Device Admin” på sidan 55
➡ ”Konfigurera administratörslösenord” på sidan 33
➡ ”Kontrollera protokoll” på sidan 35

# Konfigurera administratörslösenord

När du konfigurerar administratörslösenordet kan användare som inte är administraröer ändra inställningarna för systemadministration. Du kan konfigurera och ändra administratörslösenordet med Web Config, skannerns kontrollpanel, eller mjukvaran (Epson Device Admin eller EpsonNet Config). Vid användning av mjukvaran, se dokumentationen för varje mjukvara.

### Relaterad information

➡ ”Konfigurera administratörslösenordet från kontrollpanelen” på sidan 33

➡ ”Konfigurera administratörslösenord med Web Config” på sidan 33

➡ ”EpsonNet-konfig” på sidan 55

➡ ”Epson Device Admin” på sidan 55

## Konfigurera administratörslösenordet från kontrollpanelen

Du kan konfigurera administratörslösenordet från skannerns kontrollpanel.

1. Tryck på **Inst.** på startskärmen.
2. Tryck på **Systemadministration** > **Admin. inställningar**.

   Om alternativet inte visas snärtar du uppåt på skärmen för att visa det.
3. Tryck på **Administratörslösenord** > **Registrera**.
4. Ange det nya lösenordet och tryck sedan på **OK**.
5. Ange lösenordet igen och tryck sedan på **OK**.
6. Tryck på **OK** på bekräftelseskärmen.

   Skärmen för administratörsinställningar visas.
7. Tryck på **Låsinställning**, och sedan på **OK** på bekräftelseskärmen.

   Låsinställning är inställt på **På**, och administratörslösenordet krävs när du använder det låsta menyobjektet.

***Anmärkning:***

❏ *Om du konfigurerar **Inst.** > **Standardinställningar** > **Åtgärdens avbröts** till **På**, loggar skannern ut dig efter en periods inaktivitet på kontrollpanelen.*

❏ *Du kan ändra eller radera administratörslösenordet när du väljer **Ändra** eller **Nollställ** på skärmen **Administratörslösenord** och ange administratörslösenordet.*

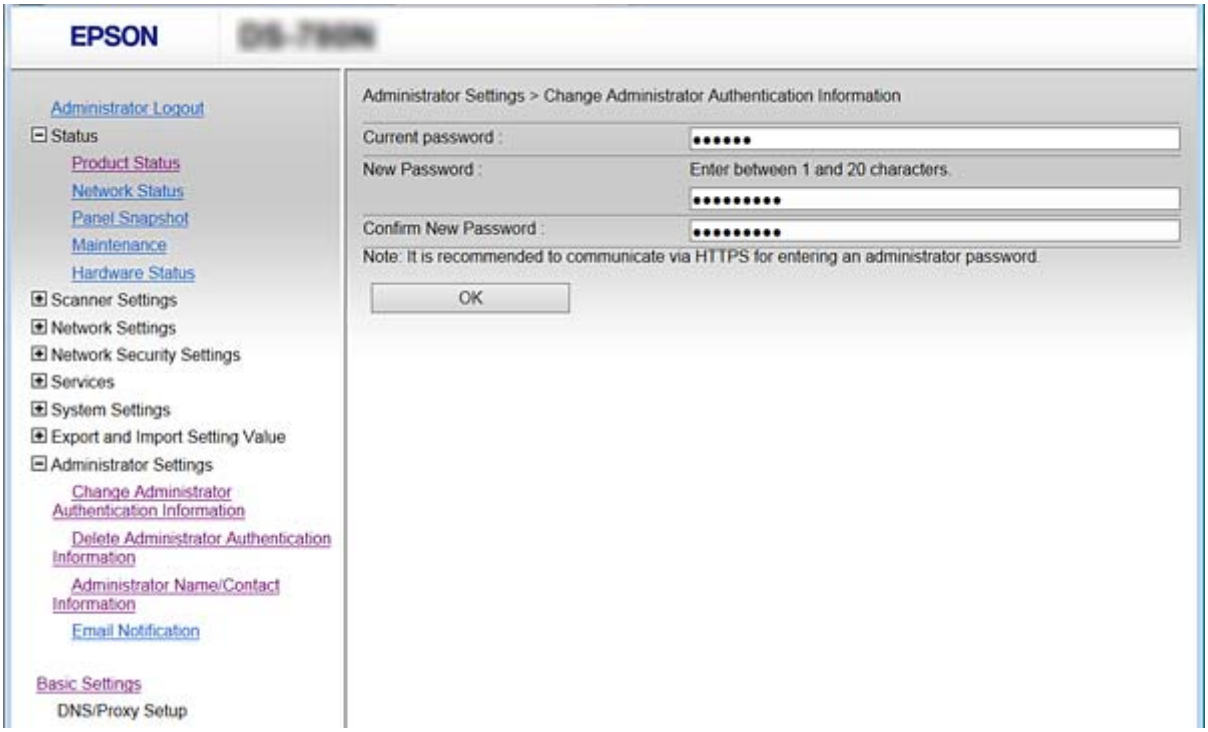
## Konfigurera administratörslösenord med Web Config

Du kan konfigurera administratörslösenordet med Web Config.

1. Öppna Web Config och välj **Administrator Settings** > **Change Administrator Authentication Information**.

2. Skriv ett lösenord i **New Password** och **Confirm New Password**. Ange användarnamnet, vid behov.

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




3. Välj **OK**.

   ***Anmärkning:***

   ❏ *För att konfigurera eller ändra låsta menyobjekt klickar du på **Administrator Login** och anger administratörslösenordet.*

   ❏ *För att radera administratörslösenordet klickar du på **Administrator Settings** > **Delete Administrator Authentication Information**, och ange sedan administratörslösenordet.*

### Relaterad information

➡ ”Öppna Web Config” på sidan 23

# Objekt som ska låsas med administratörslösenord

Administratörer har inställnings- och ändringsbehörighet för alla funktioner på enheterna.

Om du konfigurerar administratörslösenordet på enheten, kan du också låsa den, så att du inte kan ändra objekt som är relaterade till enhetshantering.

Nedan anges objekten som en administratör kan kontrollera.

| Alternativ | Beskrivning |
|---|---|
| Skannerinställningar | Konfigurera detektering av dubbel inmatning och lågshastighetsläge. |
| Ethernet-anslutningsinställningar | Ändra namn på enheter och IP-adress, konfiguration av DNS-server eller proxyserver och inställningsändringar relaterade till nätverksanslutningar. |

| Alternativ | Beskrivning |
|---|---|
| Serviceinställningar för användare | Konfiguration för kontroll av kommunikationsprotokoll, nätverksskanning och Document Capture Pro tjänster. |
| Inställningar för e-postserver | Konfiguration av en e-postserver som enheter kommunicerar direkt med. |
| Säkerhetsinställningar | Inställningar för nätverkssäkerhet, såsom SSL/TLS-kommunikation, IPsec-/IP-filtrering och IEEE802.1X. |
| Uppdatering av rotcertifikat | Uppdatering av rotcertifikatet krävs för Document Capture Pro Server autentisering och firmware-uppdatering från Web Config. |
| Firmware-uppdatering | Kontrollera och uppdatera firmware för enheter. |
| Tid, tidsinställningar | Viloövergångstid, automatisk avstängning, datum/tid, stilleståndstimer, övriga inställningar kopplade till en timer. |
| Återställ till standardinställningar | Konfigurera skannern till att ställas in på fabriksinställningar på nytt. |
| Administratörsinställningar | Konfigurera administratörslås eller -lösenord. |
| Certifierad enhetsinställning | ID-inställning för autentiseringsenhet. Konfigurerar när du använder skannern i ett autentiseringssystem som stödjer autentiseringsenheter. |

# Kontrollera protokoll

Du kan skanna med hjälp av ett antal olika vägar och protokoll. Du kan också använda nätverksinställningar från ett ospecificerat antal nätverksdatorer. Till exempel är det tillåtet att skanna med endast specificerade väga och protokoll. Du kan sänka oönskade säkerhetsrisker genom att begränsa skanning från särskilda vägar eller genom att kontrollera de tillgängliga funktionerna.

Konfigurera protokollinställningar.

1. Öppna Web Config och välj **Services** > **Protocol**.
2. Konfigurera varje punkt.
3. Klicka på **Next**.
4. Klicka på **OK**.

   Inställningarna aktiveras på skannern.

### Relaterad information

➡ ”Öppna Web Config” på sidan 23
➡ ”Protokoll som du kan aktivera eller avaktivera” på sidan 36
➡ ”Inställningsalternativ för protokoll” på sidan 37

# Protokoll som du kan aktivera eller avaktivera

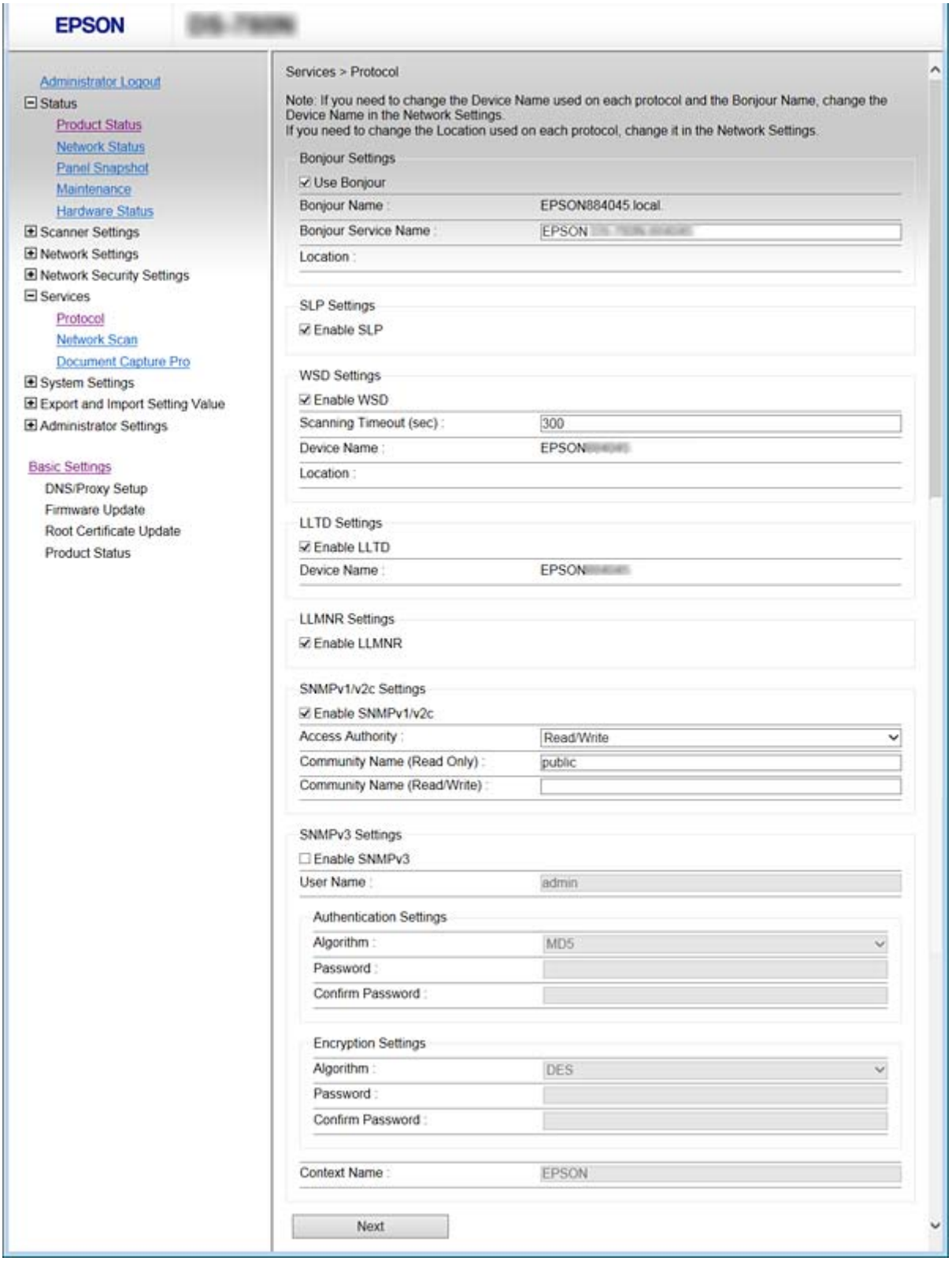
| Protokoll | Beskrivning |
|---|---|
| Bonjour Settings | Du kan ange om du vill använda Bonjour. Bonjour används för att söka efter enheter, skanna och så vidare. |
| SLP Settings | Du kan aktivera eller inaktivera SLP-funktionen. SLP används för Epson Scan 2 och nätverkssökning i EpsonNet Config. |
| WSD Settings | Du kan aktivera eller inaktivera WSD-funktionen. När det är aktiverat kan du lägga till WSD-enheter eller skanna från WSD-porten. |
| LLTD Settings | Du kan aktivera eller inaktivera LLTD-funktionen. När detta är aktiverat, visas det på Windows nätverkskarta. |
| LLMNR Settings | Du kan aktivera eller inaktivera LLMNR-funktionen. När det är aktiverat kan du använda namnmatchning utan NetBIOS, även om du inte kan använda DNS. |
| SNMPv1/v2c Settings | Du kan ange om du vill tillåta SNMPv1/v2c. Detta används för att ställa in enheter, övervakning och så vidare. |
| SNMPv3 Settings | Du kan ange om du vill tillåta SNMPv3. Detta används för att ställa in krypterade enheter, övervakning och så vidare. |

### Relaterad information

➡ ”Kontrollera protokoll” på sidan 35

➡ ”Inställningsalternativ för protokoll” på sidan 37

# Inställningsalternativ för protokoll




| Alternativ | Inställningsvärde och beskrivning |
|---|---|
| Bonjour Settings | |

## Grundläggande säkerhetsinställningar

| Alternativ | Inställningsvärde och beskrivning |
|---|---|
| Use Bonjour | Välj det här för att söka efter eller använda enheter via Bonjour. |
| Bonjour Name | Visar Bonjour-namn. |
| Bonjour Service Name | Du kan visa och ställa in Bonjour-servicenamnet. |
| Location | Visar Bonjour-platsnamn. |
| SLP Settings | |
| Enable SLP | Välj detta för att aktivera SLP-funktionen. Det används för nätverksidentifiering i Epson Scan 2 och EpsonNet Config. |
| WSD Settings | |
| Enable WSD | Välj detta för att göra det möjligt att lägga till enheter med WSS och skriva ut och skanna från WSD-porten. |
| Scanning Timeout (sec) | Ange kommunikationstimeout-värde för WSD-skanning mellan 3 till 3600 sekunder. |
| Device Name | Visar WSD enhetsnamn. |
| Location | Visar WSD-platsnamn. |
| LLTD Settings | |
| Enable LLTD | Välj detta för att möjliggöra LLTD. Skannern visas i Windows nätverkskarta. |
| Device Name | Visar LLTD enhetsnamn. |
| LLMNR Settings | |
| Enable LLMNR | Välj detta för att möjliggöra LLMNR. Du kan använda namnmatchning utan NetBIOS även om du inte kan använda DNS. |
| SNMPv1/v2c Settings | |
| Enable SNMPv1/v2c | Markera för att aktivera SNMPv1/v2c. Endast skannrar som stöder SNMPv3 visas. |
| Access Authority | Ställ in åtkomstauktoritet när SNMPv1/v2c är aktiverad. Välj **Read Only** eller **Read/Write**. |
| Community Name (Read Only) | Ange 0 till 32 ASCII (0x20 till 0x7E)-tecken. |
| Community Name (Read/Write) | Ange 0 till 32 ASCII (0x20 till 0x7E)-tecken. |
| SNMPv3 Settings | |
| Enable SNMPv3 | SNMPv3 är aktiverad när rutan har markerats. |
| User Name | Ange mellan 1 och 32 tecken med 1 byte mellanslag. |
| Authentication Settings | |
| Algorithm | Välj en algoritm för autentisering av SNMPv3. |

| Alternativ | Inställningsvärde och beskrivning |
|---|---|
| Password | Ange lösenordet för autentisering avSNMPv3.<br>Ange mellan 8 och 32 tecken i ASCII (0x20–0x7E). Om du inte specificerar detta ska du lämna det blankt. |
| Confirm Password | Ange lösenordet som du konfigurerade som bekräftelse. |
| Encryption Settings | |
| Algorithm | Välj en algoritm för kryptering av SNMPv3. |
| Password | Ange lösenordet för kryptering av SNMPv3.<br>Ange mellan 8 och 32 tecken i ASCII (0x20–0x7E). Om du inte specificerar detta ska du lämna det blankt. |
| Confirm Password | Ange lösenordet som du konfigurerade som bekräftelse. |
| Context Name | 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 35

➡ ”Protokoll som du kan aktivera eller avaktivera” på sidan 36

# Funktions- och administrationsinställningar

I det här kapitlet beskrivs objekten som är relaterade till daglig användning och hantering av enheten.

## Kontrollera information för en enhet

Du kan kontrollera följande information för den verksamma enheten från **Status** genom att använda Web Config.

❏ Product Status

Kontrollera språk, status, produktnummer, MAC-adress o.s.v.

❏ Network Status

Kontrollera informationen för nätverksanslutningsstatus, IP-adress, DNS server, etc.

❏ Panel Snapshot

Visa en skärmdump som visas på enhetens kontrollpanel.

❏ Maintenance

Kontrollera startdatum, skanningsinformation, o.s.v.

❏ Hardware Status

Kontrollera skannerns status.

### Relaterad information

➡ ”Öppna Web Config” på sidan 23

## Hantera enheter (Epson Device Admin)

Du kan hantera och använda många enheter med Epson Device Admin. Epson Device Admin gör det möjligt för dig att hantera enheter som finns på ett annat nätverk. Följande beskriver huvudhanteringsfunktionerna.

För mer information om funktioner och användning av mjukvaran, se dokumentationen eller hjälpavsnittet för Epson Device Admin.

❏ Upptäcka enheter

Du kan hitta enheter i nätverket och sedan registrera dem i en lista. Om Epsons enheter, såsom skrivare och skannrar, är anslutna till samma nätverkssegment som administratörens dator, kan du söka dem även om de inte har fått en IP-adress.

Du kan även se enheter som är anslutna till datorer i nätverket med USB-kablar. Du behöver installera Epson Device USB Agent på datorn.

❏ Konfigurera enheter

Du kan skapa en mall med konfigurationsalternativ, såsom nätverksgränssnitt och papperskälla, och använda den i andra enheter som delade inställningar. När den är ansluten till nätverket kan du tilldela en IP-adress på en enhet som inte har tilldelats en IP-adress.

❏ Övervaka enheter

Du kan regelbundet förvärva status och detaljerad information för enheter i nätverket. Du kan också övervaka enheter som är anslutna till datorer i nätverket med USB-kablar och enheter från andra företag som har registrerats i enhetslistan. För att övervaka enheter som anslutits via USB-kablar behöver du installera Epson Device USB Agent.

❏ Hantera varningsmeddelanden

Du kan övervaka varningsmeddelanden med status för enheter och förbrukningsmaterial. Systemet skickar automatiskt e-post till administratören baserat på konfigurerade villkor.

❏ Hantera rapporter

Du kan skapa standardrapporter när systemet samlar data för enhetsanvändning och förbrukningsmaterial. Du kan spara dessa skapade rapporter och skicka dem via e-post.

**Relaterad information**

➡ ”Epson Device Admin” på sidan 55

# Ta emot e-postmeddelanden när händelser inträffar

## Om e-postaviseringar

Du kan använda den här funktionen för att ta emot aviseringar via e-post när händelser inträffar. Du kan registrera upp till 5 e-postadresser och välja vilka händelser du vill ta emot aviseringar för.

Meddelandeservern måste konfigureras för att använda den här funktionen.

**Relaterad information**

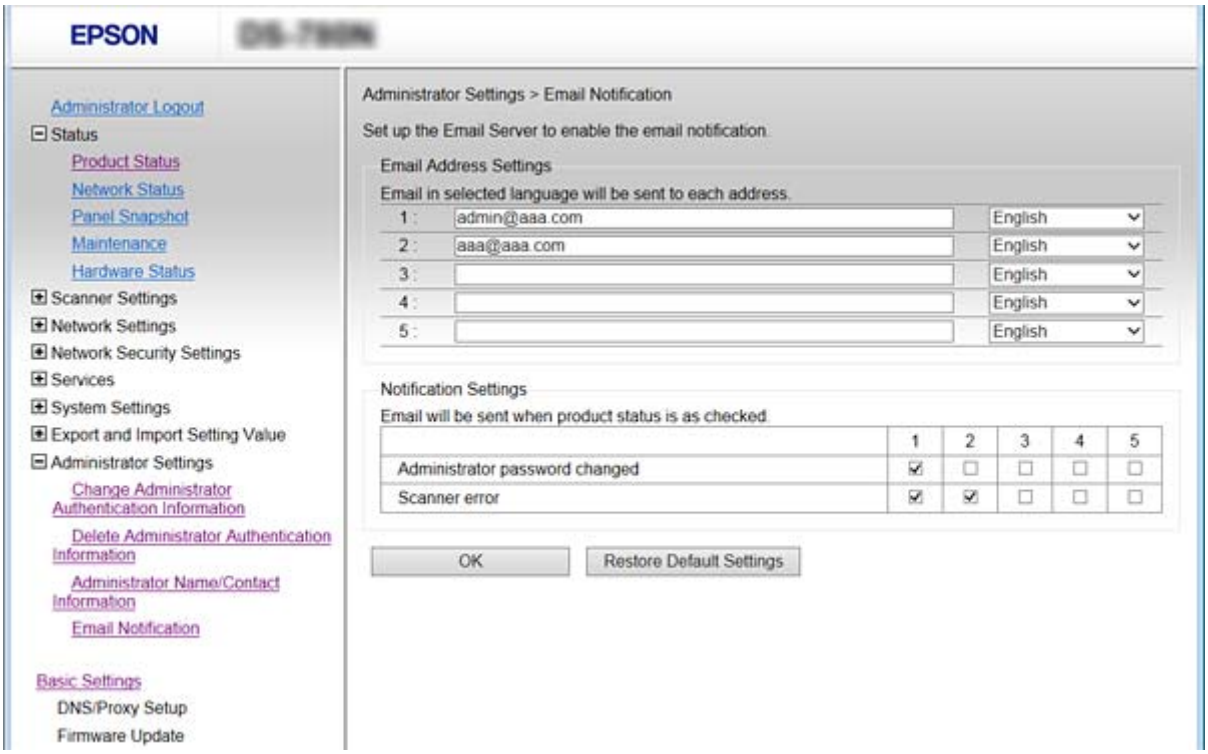
➡ ”Konfigurera en e-postserver” på sidan 42

## Konfigurera e-postavisering

Du måste konfigurera en e-postserver när du vill använda funktionen.

1. Öppna Web Config och välj **Administrator Settings** > **Email Notification**.
2. Ange en e-postadress som du vill ta emot e-postaviseringar till.
3. Välj språk för e-postaviseringar.

4. Markera rutorna för aviseringar du vill ta emot.




5. Klicka på **OK**.

### Relaterad information

➡ ”Öppna Web Config” på sidan 23
➡ ”Konfigurera en e-postserver” på sidan 42

## Konfigurera en e-postserver

Kontrollera följande innan du konfigurerar.

❏ Skannern är ansluten till ett nätverk.

❏ Datorns e-postserverinformation.

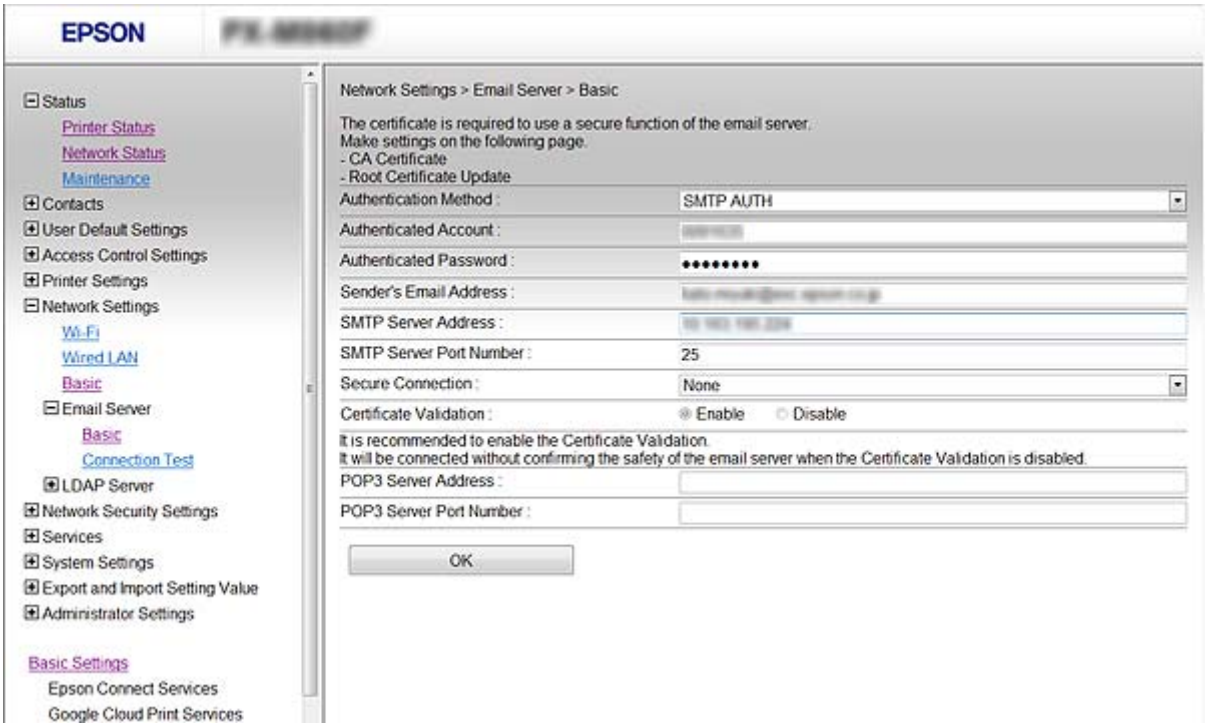
1. Öppna Web Config och välj **Network Settings** > **Email Server** > **Basic**.
2. Ange ett värde för varje alternativ.
3. Välj **OK**.

   Inställningarna du har valt visas.

### Relaterad information

➡ ”Öppna Web Config” på sidan 23
➡ ”Inställningsalternativ för e-postserver” på sidan 43

# Inställningsalternativ för e-postserver




| Alternativ | Inställningar och beskrivning | |
|---|---|---|
| Authentication Method | Ange autentiseringsmetoden som skannern ska använda för åtkomst till e-postservern. | |
| | Off | Autentisering är inaktiverad vid kommunikation med meddelandeservern. |
| | SMTP AUTH | Kräver att en mejlserver stöder SMTP-autentisering. |
| | POP before SMTP | Konfigurera en POP3-server när du väljer den här metoden. |
| Authenticated Account | Om du väljer **SMTP AUTH** eller **POP before SMTP** som **Authentication Method**, ange autentiserat kontonamn mellan 0 och 255 tecken i ASCII (0x20–0x7E). | |
| Authenticated Password | Om du väljer **SMTP AUTH** eller **POP before SMTP** som **Authentication Method**, ska du ange det autentiserade lösenordet med mellan 0 och 20 tecken med A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { \| } ~ @. | |
| Sender's Email Address | Ange avsändarens e-postadress. Ange mellan 0 och 255 tecken i ASCII (0x20–0x7E) förutom : ( ) < > [ ] ; ¥. Det första tecknet kan inte vara en punkt ".". | |
| SMTP Server Address | Ange mellan 0 och 255 tecken med A–Z a–z 0–9. - . Du kan använda IPv4- eller FQDN-format. | |
| SMTP Server Port Number | Ange ett nummer mellan 1 och 65535. | |

| Alternativ | Inställningar och beskrivning | |
|---|---|---|
| Secure Connection | Ange säker anslutningsmetod för e-postservern. | |
| | None | Om du väljer **POP before SMTP** i **Authentication Method**, är anslutningsmetoden inställd på **None**. |
| | SSL/TLS | Detta är tillgängligt när **Authentication Method** är satt till **Off** eller **SMTP AUTH**. |
| | STARTTLS | Detta är tillgängligt när **Authentication Method** är satt till **Off** eller **SMTP AUTH**. |
| Certificate Validation | Certifikatet är validerat när detta är aktiverat. Vi rekommenderar att detta är satt till **Enable**. | |
| POP3 Server Address | Om du väljer **POP before SMTP** som **Authentication Method**, anger du POP3-serveradress med mellan 0 och 255 tecken med A–Z a–z 0–9 . - . Du kan använda IPv4- eller FQDN-format. | |
| POP3 Server Port Number | Om du väljer **POP before SMTP** för **Authentication Method**, ska du ange ett nummer mellan 1 och 65535. | |

### Relaterad information

➡ ”Konfigurera en e-postserver” på sidan 42

## Kontrollera e-postserverns anslutning

1. Öppna Web Config och välj **Network Settings** > **Email Server** > **Connection Test**.
2. Välj **Start**.

   Anslutningstest för e-postservern startas. En rapport visas när testet är klart.

### Relaterad information

➡ ”Öppna Web Config” på sidan 23
➡ ”Referens för anslutningstest av e-postserver” på sidan 44

## Referens för anslutningstest av e-postserver

| Meddelanden | Förklaring |
|---|---|
| Connection test was successful. | Detta meddelande visas när anslutningen till servern är klar. |
| SMTP server communication error. Check the following. - Network Settings | Detta meddelande visas när<br>❏ Skannern inte är ansluten till ett nätverk<br>❏ SMTP-server är nere<br>❏ Nätverksanslutning är frånkopplad under kommunikation<br>❏ Mottagna ofullständiga data |

**Funktions- och administrationsinställningar**

| Meddelanden | Förklaring |
|---|---|
| POP3 server communication error. Check the following. - Network Settings | Detta meddelande visas när<br>❏ Skannern inte är ansluten till ett nätverk<br>❏ POP3-server är nere<br>❏ Nätverksanslutning är frånkopplad under kommunikation<br>❏ Mottagna ofullständiga data |
| An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server | Detta meddelande visas när<br>❏ Anslutning till en DNS-server misslyckades<br>❏ Namnmatchning för en SMTP-server misslyckades |
| An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server | Detta meddelande visas när<br>❏ Anslutning till en DNS-server misslyckades<br>❏ Namnmatchning för en POP3-server misslyckades |
| SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password | Detta meddelande visas när SMTP-serverautentisering misslyckades. |
| POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password | Detta meddelande visas när POP3-serverautentisering misslyckades. |
| Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number | Detta meddelande visas när du försöker kommunicera med protokoll som ej stöds. |
| Connection to SMTP server failed. Change Secure Connection to None. | Detta meddelande visas när en SMTP felmatchning uppstår mellan en server och en klient, eller när servern inte stöder SMTP säker anslutning (SSL-anslutning). |
| Connection to SMTP server failed. Change Secure Connection to SSL/TLS. | Detta meddelande visas när en SMTP felmatchning uppstår mellan en server och en klient, eller när server begär att använda en SSL/TLS-anslutning för en SMTP säker anslutning. |
| Connection to SMTP server failed. Change Secure Connection to STARTTLS. | Detta meddelande visas när en SMTP felmatchning uppstår mellan en server och en klient, eller när server begär att använda en STARTTLS-anslutning för en SMTP säker anslutning. |
| The connection is untrusted. Check the following. - Date and Time | Detta meddelande visas när skannerns inställning för datum och tid är felaktig eller certifikatet har upphört att gälla. |
| The connection is untrusted. Check the following. - CA Certificate | Detta meddelande visas när skannern inte har ett rotcertifikat som motsvarar server eller så har ett CA Certificate inte importerats. |
| The connection is not secured. | Detta meddelande visas när det erhållna certifikatet är skadat. |
| SMTP server authentication failed. Change Authentication Method to SMTP-AUTH. | Detta meddelande visas när en felmatchning för autentiseringsmetod uppstår mellan en server och en klient. Servern stöder SMTP AUTH. |
| SMTP server authentication failed. Change Authentication Method to POP before SMTP. | Detta meddelande visas när en felmatchning för autentiseringsmetod uppstår mellan en server och en klient. Servern stöder inte SMTP AUTH. |

| Meddelanden | Förklaring |
|---|---|
| Sender's Email Address is incorrect. Change to the email address for your email service. | Detta meddelande visas när den angivna avsändarens e-postadress är felaktig. |
| Cannot access the product until processing is complete. | Detta meddelande visas när skannern är upptagen. |

### Relaterad information

➡ ”Kontrollera e-postserverns anslutning” på sidan 44

# Uppdatera firmware

## Uppdatera firmware med Web Config

Uppdaterar firmware med Web Config. Enheten måste anslutas till Internet.

1. Öppna Web Config och välj **Basic Settings** > **Firmware Update**.
2. Klicka på **Start**.

   Firmware-bekräftelsen startar och firmware-informationen visas om uppdaterad firmware finns.
3. Klicka på **Start** och följ instruktionerna på skärmen.

***Anmärkning:***
*Du kan också uppdatera firmware med Epson Device Admin. Du kan visuellt kontrollera firmware-informationen i enhetslistan. Detta är viktigt när du vill uppdatera firmware för flera enheter. Mer information finns i guiden Epson Device Admin eller hjälpavsnittet.*

### Relaterad information

➡ ”Öppna Web Config” på sidan 23
➡ ”Epson Device Admin” på sidan 55

## Uppdatera firmware med Epson Firmware Updater

Du kan hämta enhetens firmware från webbplatsen för Epson på datorn och sedan ansluta enheten och datorn med USB-kabeln för att uppdatera firmware. Prova följande om du inte kan uppdatera via nätverket.

1. Öppna webbplatsen för Epson och hämta firmware.
2. Anslut daton som innehåller hämtad firmware till enheten med USB-kabeln.
3. Dubbelklicka på den hämtade .exe-filen.

   Epson Firmware Updater startar.
4. Följ instruktionerna på skärmen.

# Säkerhetskopiera inställningar

Genom att exportera inställningsobjekten på Web Config kan du kopiera objekten till andra skannrar.

## Exportera inställningarna

Exportera varje inställning för skannern.

1. Öppna Web Config, och välj sedan **Export and Import Setting Value** > **Export**.
2. Välj de inställningar som du vill exportera.

   Välj de inställningar som du vill exportera. Om du väljer den överordnade kategorin, väljs även undergrupper. Däremot kan underkategorier som orsakar fel genom att dupliceras inom samma nätverk (såsom IP-adresser och så vidare) inte väljas.
3. Ange ett lösenord för att kryptera den exporterade filen.

   Du behöver lösenordet för att importera filen. Lämna det här fältet tomt om du inte vill kryptera filen.
4. Klicka på **Export**.

> ***Viktigt:***
>
> *Om du vill exportera skannerns nätverksinställningar som skannerns namn och IP-adress, välj **Enable to select the individual settings of device** och markera fler poster. Använd endast utvalda värden för ersättningsskanner.*

### Relaterad information

➡ ”Öppna Web Config” på sidan 23

## Importera inställningarna

Importera den exporterade Web Config-filen till skannern.

> ***Viktigt:***
>
> *Vid import av värden som inkluderar individuell information, t.ex. skannernamn eller IP-adress, kontrollera att samma IP-adress inte existerar på samma nätverk. Om IP-adressen överlappar, återspeglar inte skannern värdet.*

1. Öppna Web Config, och välj sedan **Export and Import Setting Value** > **Import**.
2. Välj den exporterade filen och ange sedan det krypterade lösenordet.
3. Klicka på **Next**.
4. Välj de inställningar som du vill importera och klicka på **Next**.
5. Klicka på **OK**.

Inställningarna aktiveras på skannern.

**Funktions- och administrationsinställningar**

### Relaterad information

➡ ”Öppna Web Config” på sidan 23

# Lösa problem

## Tips för att lösa problem

Mer information finns i följande handbok.

❏ Användarhandbok

Innehåller instruktioner om skannerns användning, underhåll och felsökning.

## Kontrollera loggen för server- och nätverksenheten

Om du har problem med nätverksanslutning, kan det vara möjligt att identifiera orsaken genom att kontrollera e-postserverns logg, LDAP-server, o.s.v., kontrollera statusen genom att använda nätverksloggen av loggar och kommandon för systemtillbehör, såsom routrar.

## Initiera nätverksinställningar

### Återställa nätverksinställningar från kontrollpanelen

Du kan återställa alla nätverksinställningar till standardinställningarna.

1. Tryck på **Inst.** på startskärmen.
2. Tryck på **Systemadministration** > **Återställ inställningarna** > **Nätverksinställningar**.
3. Kontrollera meddelandet och välj **Ja**.
4. Tryck på **Stäng** när ett meddelande om att avsluta visas.

   Skärmen stängs av automatiskt efter en viss tid om du inte trycker på **Stäng**.

## Kontrollera kommunikationen mellan enheter och datorer

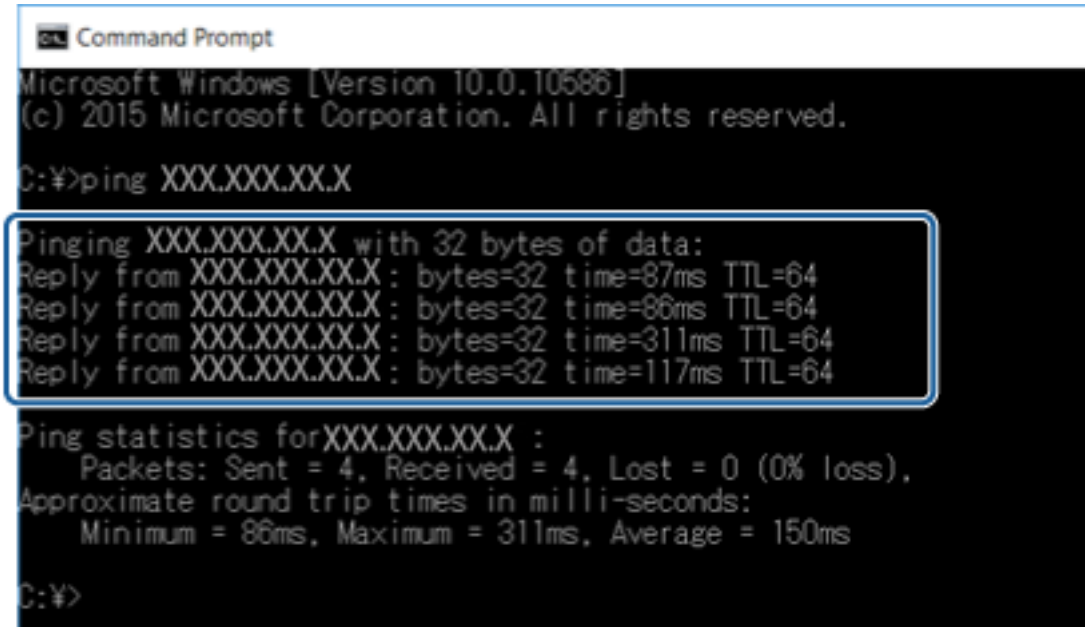
### Kontrollera anslutningen med Ping-kommandot — Windows

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

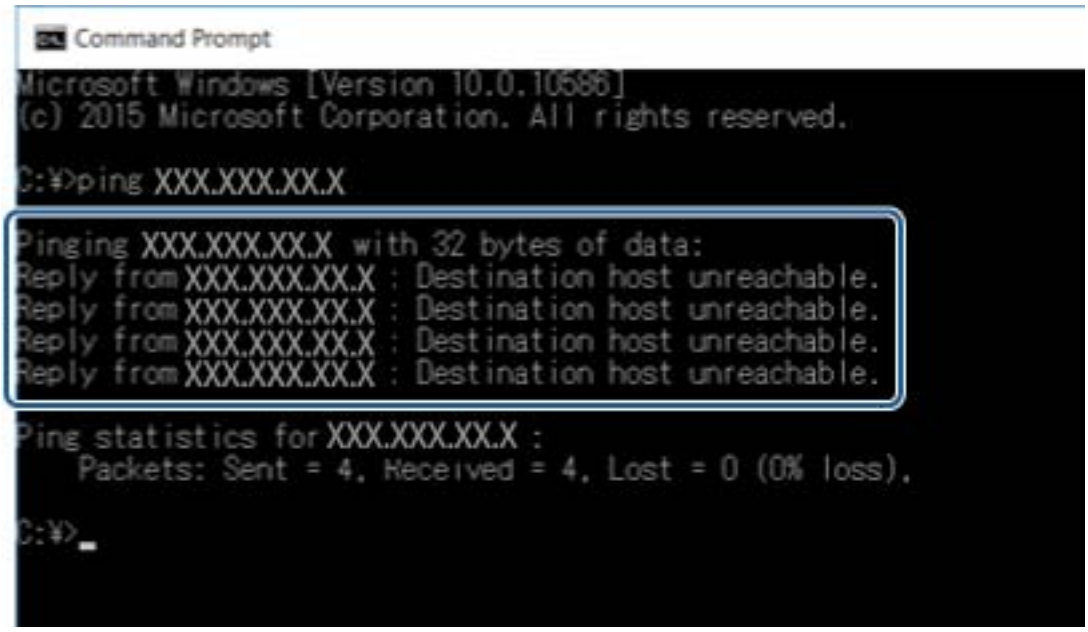
1. Kontrollera skannerns IP-adress för den anslutning som du vill kontrollera.

   Du kan kontrollera detta med Epson Scan 2.

2. Öppna skärmen med kommandotolken på datorn.
   - ❏ Windows 10
     Högerklicka på startknappen eller tryck och håll in den och välj sedan **Kommandoprompt**.
   - ❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
     Öppna programskärmen och välj **Kommandotolk**.
   - ❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 och tidigare
     Klicka på startknappen, välj **Alla program** eller **Program** > **Tillbehör** > **Kommandotolk**.
3. Skriv in ”ping xxx.xxx.xxx.xxx” och tryck på Enter.
   Ange skannerns IP-adress i stallet for xxx.xxx.xxx.xxx.
4. Kontrollera kommunikationens status.
   Följande meddelande visas om skannern och datorn kommunicerar med varandra.



Följande meddelande visas om skannern och datorn inte kommunicerar med varandra.




## Kontrollera anslutningen med Ping-kommandot — Mac OS

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

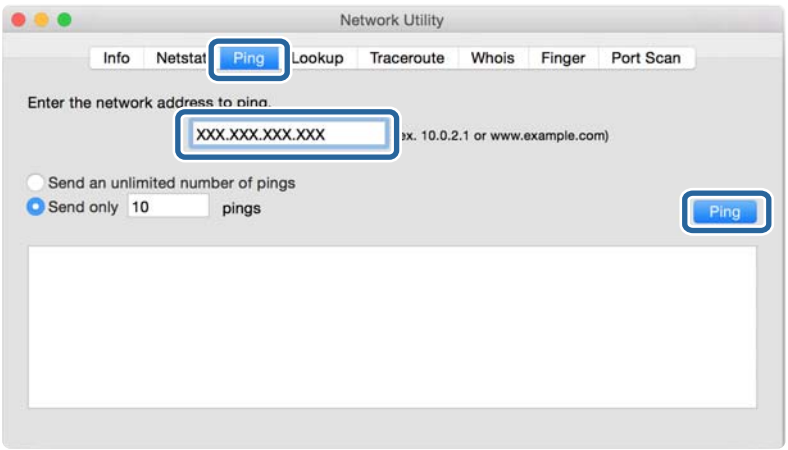
1. Kontrollera skannerns IP-adress för den anslutning som du vill kontrollera.

   Du kan kontrollera detta med Epson Scan 2.

2. Kör Network Utility.

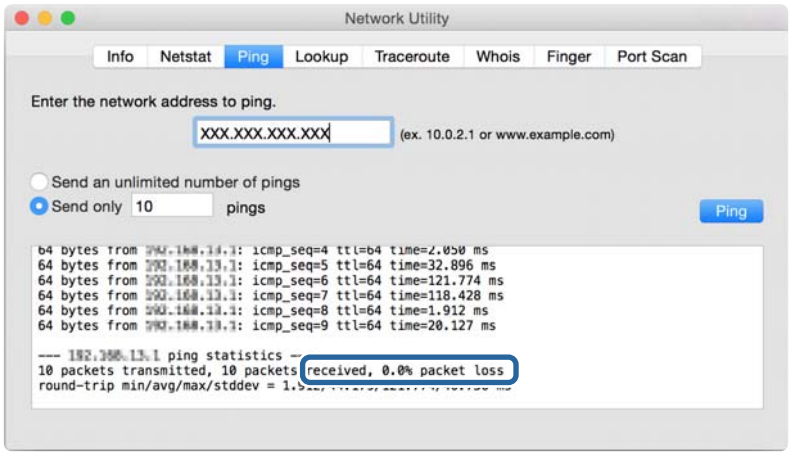
   Skriv in ”Network Utility” i **Spotlight**.

3. Klicka på fliken **Ping**, ange IP-adressen som du kontrollerade i steg 1 och klicka på **Ping**.

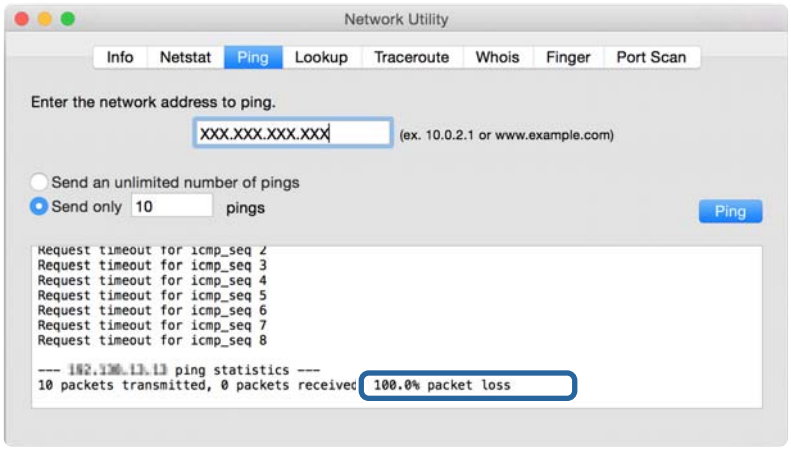


4. Kontrollera kommunikationens status.

   Följande meddelande visas om skannern och datorn kommunicerar med varandra.




   Följande meddelande visas om skannern och datorn inte kommunicerar med varandra.




# Problem att använda nätverksprogram

## Kan inte öppna webbkonfiguration

### Är skannerns IP-adress rätt konfigurerad?

Konfigurera IP-adressen med Epson Device Admin eller EpsonNet Config.

### Stöder webbläsaren bulkkrypteringar för Encryption Strength för SSL/TLS?

Bulkkrypteringarna för Encryption Strength för SSL/TLS är som följer. 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 skannerns datum är rätt konfigurerat.

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

Skannerns IP-adress som angetts för **Common Name** när du skapar ett självsignerat certifikat eller en CSR matchar inte adressen i webbläsaren. Hämta och importera ett certifikat igen eller ändra skannernamnet.

### En proxyserver används för åtkomst till skannern.

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

❏ Windows:

Välj **Kontrollpanelen** > **Nätverk och Internet** > **Internet-alternativ** > **Anslutningar** > **LAN-inställningar** > **Proxyserver** och ange att proxyservern inte ska användas för lokala adresser.

❏ Mac OS:

Välj **Systeminställningar** > **Nätverk** > **Avancerat** > **Proxyservrar** och registrera den lokala adressen i **Förbigå proxyinställningarna för dessa värdar och domäner**.

Exempel:

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

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

### Relaterad information

➡ ”Öppna Web Config” på sidan 23

➡ ”Tilldela IP-adress” på sidan 15

➡ ”Tilldela en IP-adress med EpsonNet Config” på sidan 56

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

### Valde du Blockera, Avbryt, eller Stäng av när en Windows-säkerhetsskärm eller en brandväggsskärm visades?

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

Du kan korrigera detta genom att registrera EpsonNet Config som ett undantag i Windows-brandväggen och kommersiella säkerhetsprogram. Om du använder ett antivirus- eller säkerhetsprogram ska du stänga det och sedan försöka använda EpsonNet Config.

### Är timeoutinställningen för kommunikationsfel för kort?

Kör EpsonNet Config, välj **Tools** > **Options** > **Timeout** och öka tidslängden i inställningen **Communication Error**. Observera att det kan göra att EpsonNet Config fungerar långsammare.

**Lösa problem**

### Relaterad information

➡ ”Köra EpsonNet Config — Windows” på sidan 56
➡ ”Köra EpsonNet Config — Mac OS” på sidan 56

# Bilaga

## Introduktion till nätverksmjukvara

Nedan beskrivs mjukvaran 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 supportwebbplatsen för Epson. Mer information finns i dokumentationen eller hjälpen till Epson Device Admin.

#### Köra Epson Device Admin (endast Windows)

Välj **Alla program** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**.

***Anmärkning:***
*Om en brandväggsvarning visas ska du bevilja åtkomst för Epson Device Admin.*

### EpsonNet-konfig

Med EpsonNet Config kan administratören konfigurera skannerns nätverksinställningar, t.ex. tilldela IP-adress och ändra anslutningsläget. Batch-inställningsfunktionen stöds på Windows. Mer information finns i dokumentationen eller hjälpen till EpsonNet Config.

## Köra EpsonNet Config — Windows

Välj **Alla program** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

***Anmärkning:***
*Om en brandväggsvarning visas ska du bevilja åtkomst för EpsonNet Config.*

## Köra EpsonNet Config — Mac OS

Välj **Gå** > **Applikationer** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

## EpsonNet SetupManager

EpsonNet SetupManager är en mjukvara för att skapa ett paket för enkel skannerinstallation, såsom installation och konfiguration av skannerdrivrutinen och installation av Document Capture Pro. Med programmet kan administratörer skapa unika programpaket och distribuera dem till grupper.

För mer information, besök din regionala webbplats för Epson.

# Tilldela en IP-adress med EpsonNet Config

Du kan tilldela en IP-adress till skannern med EpsonNet Config. EpsonNet Config gör det möjligt för dig att tilldela en IP-adress till en skanner som inte har tilldelats efter anslutning med en Ethernet-kabel.

## Tilldela IP-adressen med batch-inställningar

### Skapa filen för batch-inställningar

Genom att använda MAC-adressen och modellnamnet som nycklar kan du skapa en ny SYLK-fil för att konfigurera IP-adressen.

1. Öppna ett kalkylprogram (exempelvis Microsoft Excel) eller ett textredigeringsprogram.

2. Skriv in ”Info_MACAddress”, ”Info_ModelName” och ”TCPIP_IPAddress” i första raden enligt inställningsobjektnamnen.

   Ange inställningsobjekten för följande textsträngar. För att skilja mellan versaler/gemener och tecken med dubbla/enkla byte, identifieras objektet inte om något tecken varierar.

   Ange inställningsobjektnamnet enligt nedan; annars kan inte, EpsonNet Config identifiera inställningsobjekten.

| Info_MACAddress | Info_ModelName | TCPIP_IPAddress |
|---|---|---|
| | | |
| | | |

3. Ange MAC-adress, modellnamn och IP-adress för varje nätverksenhet.

| Info_MACAddress | Info_ModelName | TCPIP_IPAddress |
|---|---|---|

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

4. Ange ett namn och spara som SYLK-fil (*.slk).

## Göra Batch-inställningar med konfigurationsfilen

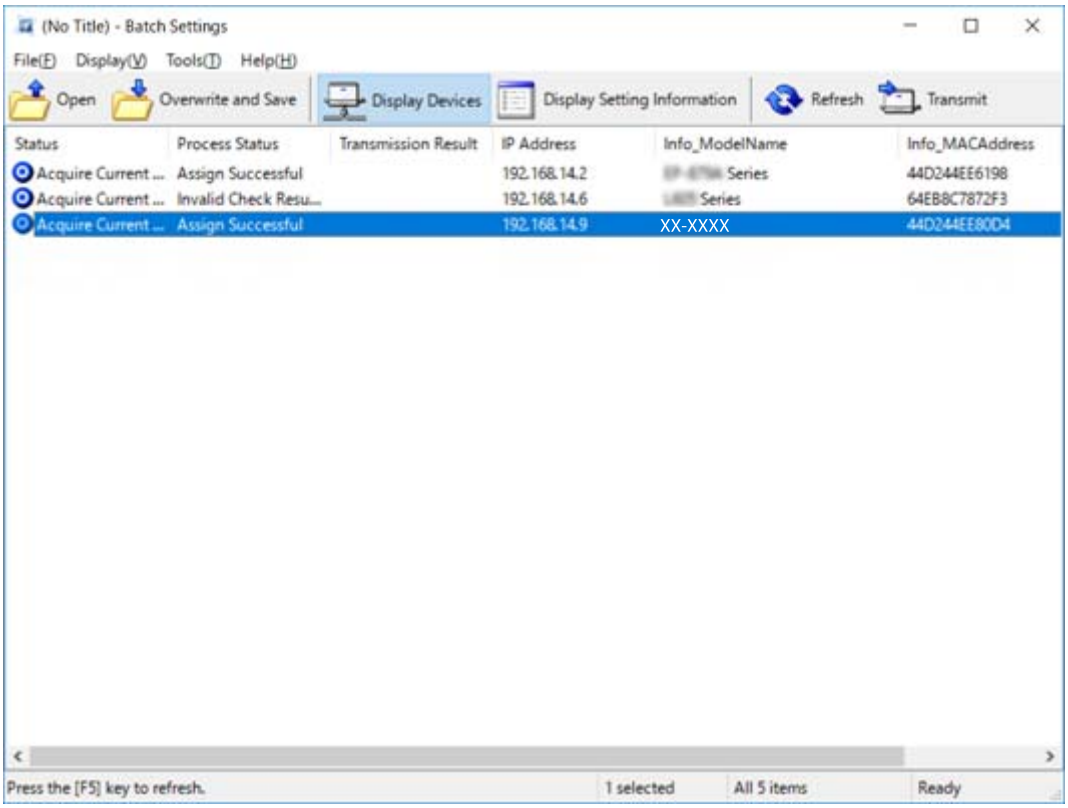
Tilldela IP-adresser i konfigurationsfilen (SYLK-fil) vid ett tillfälle. Du behöver skapa konfigurationsfilen före tilldelningen.

1. Anslut alla enheter till nätverket med Ethernet-kablar.
2. Starta skannern.
3. Starta EpsonNet Config.

   En lista över skannrarna i nätverket visas. Det kan ta en stund innan de visas.
4. Klicka på **Tools** > **Batch Settings**.
5. Klicka på **Open**.
6. På filvalsskärmen väljer du SYLK-filen (*.slk) som innehåller inställningarna och sedan klickar du på **Open**.

7. Välj enheterna för vilka du utför batch-inställningar med kolumnen **Status** som är inställd på **Unassigned**, och sedan **Process Status** konfigurerad till **Assign Successful**.

   Vid markering av flera val trycker du på Ctrl eller Shift och klickar eller drar med musen.




8. Klicka på **Transmit**.

9. När inmatningsskärmen för lösenord visas anger du lösenordet och klickar sedan på **OK**.

   Överför inställningarna.

   ***Anmärkning:***
   *Informationen överförs till nätverksgränssnittet tills förloppsindikatorn slutförts. Stäng inte av enheten eller den trådlösa adaptern och skicka inga data till enheten.*

10. På skärmen **Transmitting Settings** klickar du på **OK**.

11. Kontrollera status för enheten du har konfigurerat.

    För enheter som visar  eller  ska du kontrollera innehållet i inställningsfilen, eller att enheten har startat om normalt.

| Ikon | Status | Process Status | Förklaring |
|---|---|---|---|
|  | Setup Complete | Setup Successful | Installationen har slutförts på normalt sätt. |
|  | Setup Complete | Rebooting | När informationen har överförts behöver varje enhet startas om för att aktivera inställningarna. En kontroll utförs för att avgöra om enheten kan anslutas efter omstart eller inte. |
|  | Setup Complete | Reboot Failed | Kan inte kontrollera enheten efter överföringsinställningar. Kontrollera att enheten har slagits på, eller om den har startat om på rätt sätt. |
|  | Setup Complete | Searching | Söker efter enheten som indikeras i inställningsfilen.* |
|  | Setup Complete | Search Failed | Kan inte kontrollera enheter som redan har konfigurerats. Kontrollera att enheten har slagits på, eller om den har startat om på rätt sätt.* |

    * Endast när konfiguration av information visas.

### Relaterad information

➡ ”Köra EpsonNet Config — Windows” på sidan 56
➡ ”Köra EpsonNet Config — Mac OS” på sidan 56

## Tilldela en IP-adress till varje enhet

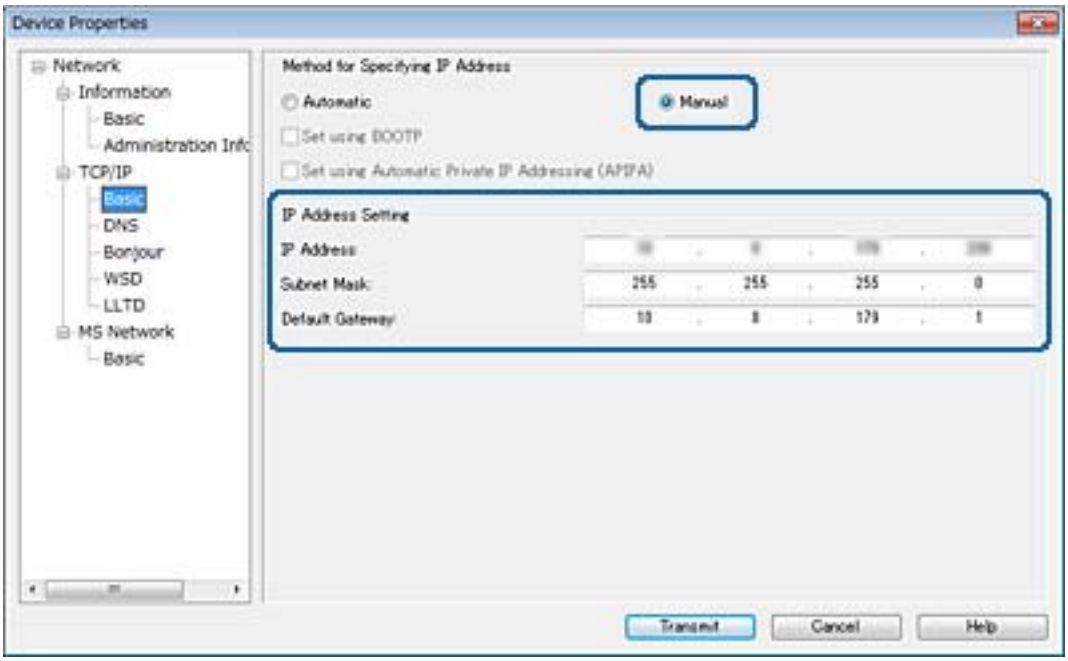
Tilldela en IP-adress till skannern med EpsonNet Config.

1. Starta skannern.
2. Anslut skannern till nätverket med en Ethernet-kabel.
3. Starta EpsonNet Config.

   En lista över skannrarna i nätverket visas. Det kan ta en stund innan de visas.
4. Dubbelklicka på skannern som du vill tilldela.

   ***Anmärkning:***
   *Om du har anslutit flera skannrar av samma modell kan du identifiera skannern med MAC-adressen.*
5. Välj **Network** > **TCP/IP** > **Basic**.

6. Ange adresser för **IP Address**, **Subnet Mask** och **Default Gateway**.




***Anmärkning:***
*Ange en fast adress när du ansluter skannern till ett säkert nätverk.*

7. Klicka på **Transmit**.

   Skärmen som bekräftar överföring av informationen visas.

8. Klicka på **OK**.

   Skärmen för slutförande av överföringen visas.

   ***Anmärkning:***
   *Informationen har överförts till enheten och meddelandet "Konfiguration slutfördes." visas. Stäng inte av enheten och skicka inga data till tjänsten.*

9. Klicka på **OK**.

### Relaterad information

➡ "Köra EpsonNet Config — Windows" på sidan 56
➡ "Köra EpsonNet Config — Mac OS" på sidan 56

# Använda port för skannern

Skannern använder följande port. Dessa portar ska göra det möjligt att bli tillgängligt efter behov för nätverksadministratören.

**Bilaga**

| Avsändare (klient) | Använd | Destination (Server) | Protokoll | Portnummer |
|---|---|---|---|---|
| Skanner | Skicka e-post (e-postavisering) | SMTP-server | SMTP (TCP) | 25 |
| | | | SMTP SSL/TLS (TCP) | 465 |
| | | | SMTP STARTTLS (TCP) | 587 |
| | POP i stället för SMTP-anslutning (e-postavisering) | POP-server | POP3 (TCP) | 110 |
| | Kontroll-WSD | Klientdator | WSD (TCP) | 5357 |
| | Sök efter en dator vid push-skanning från Document Capture Pro | Klientdator | Network Push Scan Discovery | 2968 |
| | Samla in jobbinformation vid push-skanning från Document Capture Pro | Klientdator | Network Push Scan | 2968 |
| Klientdator | Upptäck skannern från en applikation, såsom EpsonNet Config och skannerdrivrutin. | Skanner | ENPC (UDP) | 3289 |
| | Samla in och konfigurera MIB-information från en applikation, såsom EpsonNet Config och skannerdrivrutin. | Skanner | SNMP (UDP) | 161 |
| | Söker WSD-skanner | Skanner | WS-Discovery (UDP) | 3702 |
| | Vidarebefordra skanningdata från Document Capture Pro | Skanner | Nätverksskanning (TCP) | 1865 |

# Avancerade säkerhetsinställningar för företag

I det här kapitlet beskriver vi avancerade säkerhetsfunktioner.

## 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. Om du använder enheten i en miljö där du kan få åtkomst till Internet är riskerna ännu högre.

För att undvika den här risken har Epson-enheter en rad olika säkerhetstekniker.

Konfigurera enheten efter behov enligt miljövillkoren som har byggts in i kundens miljöinformation.

| Namn | Funktionstyp | Vad du kan konfigurera | Vad du kan förhindra |
|---|---|---|---|
| SSL/TLS-kommunikation | Kommunikationssökvägen för en dator och en enhet krypteras med SSL-/TLS-kommunikation. Kommunikationsinnehållet via en webbläsare skyddas. | Konfigurera ett CA-certifikat för servern som är certifikatssignerad av en CA (Certificate Authority) till enheten. | Förhindra läckage av inställningsinformation och innehåll i överförda data till skannern från datorn. Åtkomst till Epson-servern på Internet från enheten kan också skyddas med en firmware-uppdatering o.s.v. |
| IPsec-/IP-filtrering | Du kan göra inställningar för att tillåta beskärning och urklipp av data som kommer från en viss klient eller är av en viss typ. Eftersom IPsec skyddar data via IP-paketenhet (kryptering och autentisering), kan du säkert kommunicera osäkra 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. |
| 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. |
| IEEE802.1X | Gör det bara möjligt för en användare som är autentiserad för Ethernet att ansluta. Tillåter bara en behörig användare att använda enheten. | Autentiseringsinställningar för RADIUS-servern (autentiseringsserver). | Skyddar från obehörig åtkomst och användning av enheten. |

| Namn | Funktionstyp | Vad du kan konfigurera | Vad du kan förhindra |
|---|---|---|---|
| Läs ID-kort | Du kan använda enheten genom att hålla den över ett ID-kort för den autentiserade enheten som är ansluten. Du kan begränsa anskaffning av loggar för varje användare och enhet, och begränsa enheter som är tillgängliga för användning och tillgängliga funktioner för varje användare och grupp. | Anslut en autentiseringsenhet till enheten och konfigurera sedan informationen för en användare i autentiseringssystemet. | Förebygg obehörig användning och spoofing av enheten. |

**Relaterad information**

➡ ”SSL-/TLS-kommunikation med skannern” på sidan 63

➡ ”Krypterad kommunikation med IPsec/IP-filtrering” på sidan 71

➡ ”Använda SNMPv3-protokollet” på sidan 82

➡ ”Ansluta skannern till ett IEEE802.1X-nätverk” på sidan 84

## Säkerhetsfunktionsinställningar

Vid inställning av IPsec/IP-filtrering eller IEEE802.1X, rekommenderar vi att du får åtkomst till Web Config med SSL/TLS för att kommunicera inställningsinformationen och minska säkerhetsrisker, såsom klåfingerskydd och interception.

# SSL-/TLS-kommunikation med skannern

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

## 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.

❏ 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 skannern 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 64

➡ ”Radera ett CA-signerat certifikat” på sidan 67

➡ ”Uppdatera ett självsignerat certifikat” på sidan 68

# 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 nedan när du ska skapa en CSR och hämta ett CA-signerat certifikat med Web Config. CSR får formatet PEM/DER när du skapar certifikatet med Web Config.

1. Öppna Web Config, och välj sedan **Network Security Settings**. Välj sedan **SSL/TLS** > **Certificate** eller **IPsec/IP Filtering** > **Client Certificate** eller **IEEE802.1X** > **Client Certificate**.

2. Klicka **Generate** för **CSR**.

   En sida där du kan skapa en CSR öppnas.

3. Ange ett värde för varje alternativ.

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

4. Klicka på **OK**.

   Ett meddelande om slutförande visas.

5. Välj **Network Security Settings**. Välj sedan **SSL/TLS** > **Certificate**, eller **IPsec/IP Filtering** > **Client Certificate** eller **IEEE802.1X** > **Client Certificate**.

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.*

7. Skicka ett CSR till en certifikatutfärdare och skaffa ett CA-signed Certificate.

   Följ reglerna för de olika certifikatutfärdarna angående sändningsmetod och format.

8. Spara det utfärdade CA-signed Certificate på en dator som är ansluten till skannern.

   Hämtningen av det CA-signed Certificate är klar när du sparar certifikatet på en måldestination.

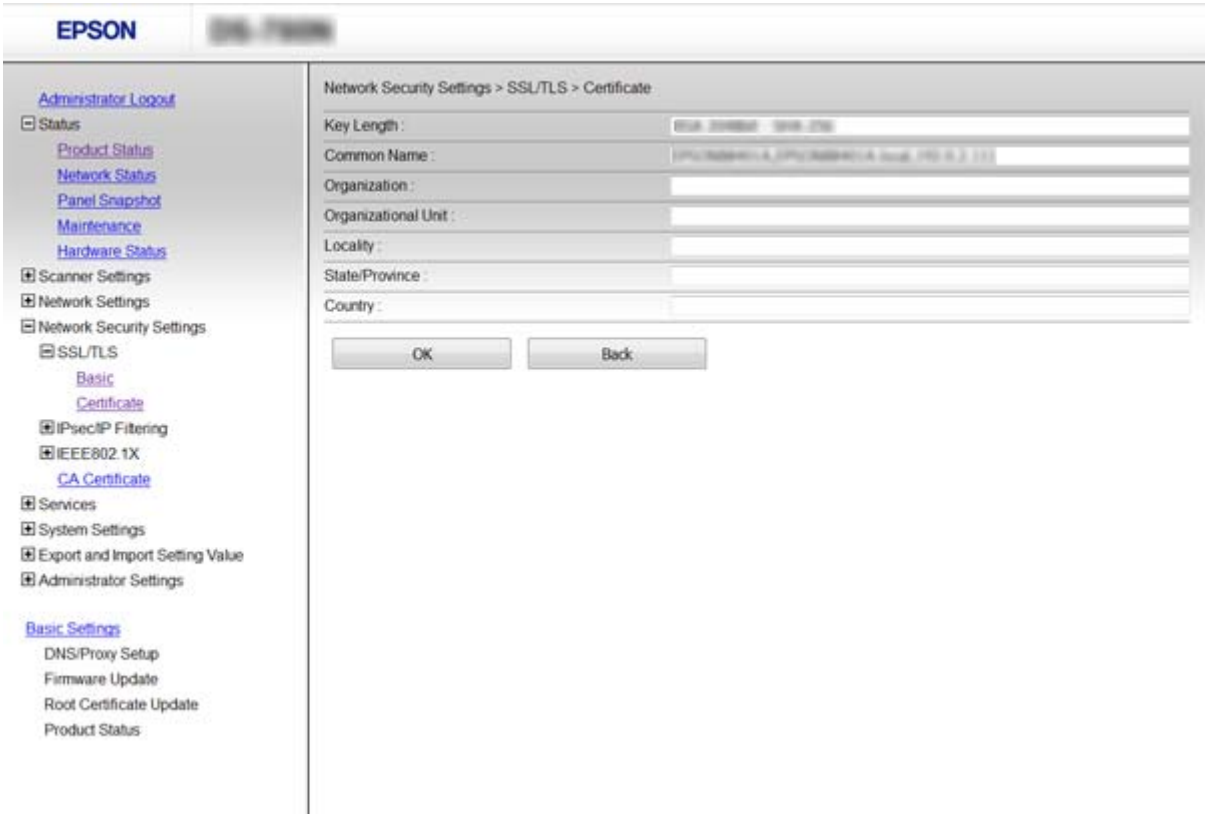
**Relaterad information**

➡ ”Öppna Web Config” på sidan 23

➡ ”Inställningsalternativ för CSR” på sidan 65

➡ ”Importera ett CA-signerat certifikat” på sidan 66

### *Inställningsalternativ för CSR*




| Alternativ | Inställningar och beskrivning |
|---|---|
| Key Length | Välj nyckellängd för CSR. |
| Common Name | Du kan uppge mellan 1 och 128 tecken. Om det är en IP-adress ska det vara en statisk IP-adress.<br>Exempel:<br>URL för åtkomst Web Config: https://10.152.12.225<br>Vanligt namn: 10.152.12.225 |
| Organization/ Organizational Unit/ Locality/ State/Province | Du kan ange mellan 0 och 64 tecken i ASCII (0x20–0x7E). Du kan skilja unika namn åt med komman. |
| Country | Skriv en landskod med ett tvåsiffrigt nummer enligt ISO-3166. |

### Relaterad information

➡ ”Hämta ett CA-signerat certifikat” på sidan 64

# Importera ett CA-signerat certifikat

***Viktigt:***

❏ *Kontrollera att rätt datum och klockslag är inställt på skannern.*

❏ *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**. Välj sedan **SSL/TLS** > **Certificate**, eller **IPsec/IP Filtering** > **Client Certificate** eller **IEEE802.1X** > **Client Certificate**.

2. Klicka på **Import**.

   En sida där du kan importera öppnas.

3. Ange ett värde för varje alternativ.

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

   ❏ Ett certifikat i formatet PEM/DER som hämtats från Web Config

   ❏ **Private Key**: Konfigureras inte eftersom skannern innehåller en privat nyckel.

   ❏ **Password**: Konfigureras inte.

   ❏ **CA Certificate 1**/**CA Certificate 2**: Valfritt

   ❏ Ett certifikat i formatet PEM/DER som hämtats från en dator

   ❏ **Private Key**: Måste anges.

   ❏ **Password**: Konfigureras inte.

   ❏ **CA Certificate 1**/**CA Certificate 2**: Valfritt

   ❏ Ett certifikat i formatet PKCS#12 som hämtats från en dator

   ❏ **Private Key**: Konfigureras inte.

   ❏ **Password**: Valfritt

   ❏ **CA Certificate 1**/**CA Certificate 2**: Konfigureras inte.

4. Klicka på **OK**.

   Ett meddelande om slutförande visas.

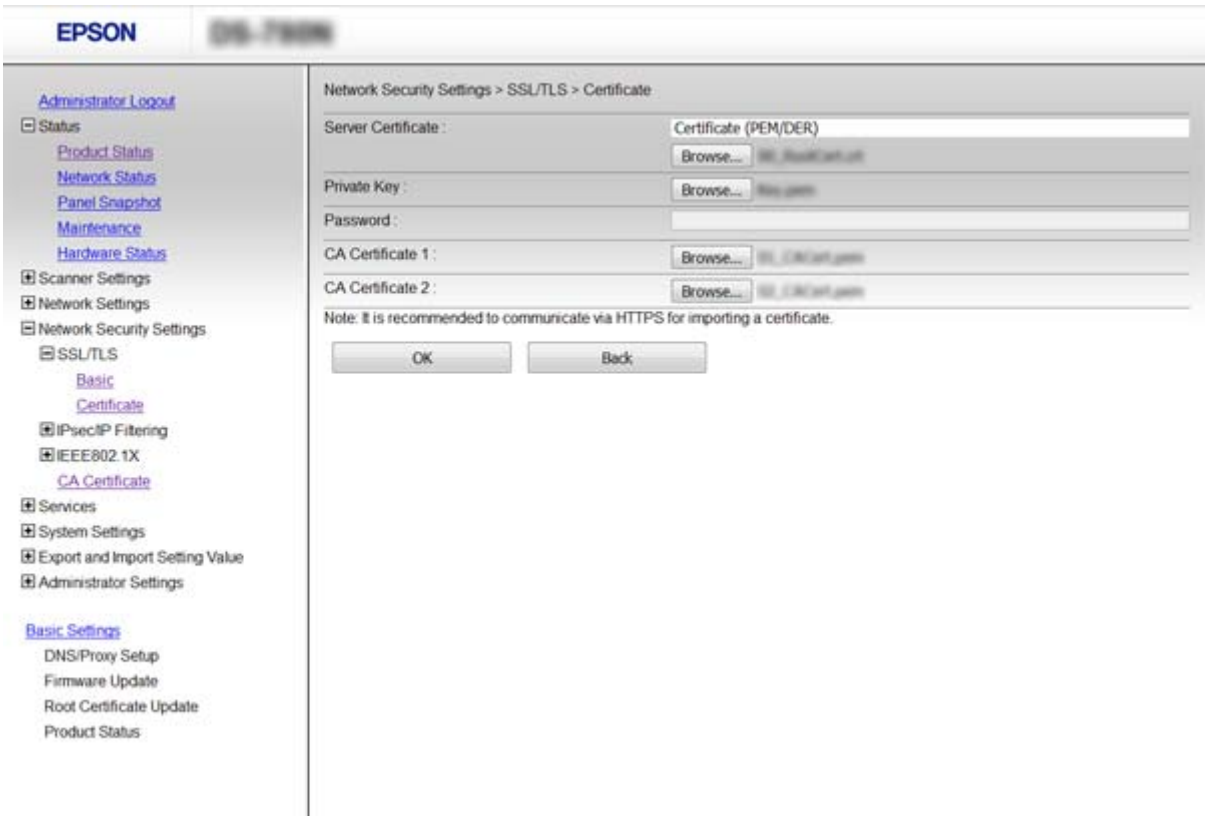
***Anmärkning:***
*Verifiera certifikatinformationen genom att klicka på* ***Confirm****.*

### Relaterad information

➡ ”Öppna Web Config” på sidan 23

➡ ”Inställningsalternativ för import av CA-signerat certifikat” på sidan 67

### *Inställningsalternativ för import av CA-signerat certifikat*




| Poster | Inställningar och förklaringar |
|---|---|
| Server Certificate eller Client Certificate | Välj ett certifikatformat. |
| Private Key | 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 | Skriv ett lösenord för kryptering av en privat nyckel. |
| CA Certificate 1 | Om certifikatets format är **Certificate (PEM/DER)** ska du importera ett certifikat från en certifikatutfärdare som utfärdar ett servercertifikat. Ange en fil om det behövs. |
| CA Certificate 2 | Om certifikatets format är **Certificate (PEM/DER)** ska du importera ett certifikat från en certifikatutfärdare som utfärdar **CA Certificate 1**. Ange en fil om det behövs. |

#### Relaterad information

➡ ”Importera ett CA-signerat certifikat” på sidan 66

## Radera ett CA-signerat certifikat

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

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

1. Öppna Web Config, och välj sedan **Network Security Settings**. Välj sedan **SSL/TLS** > **Certificate** eller **IPsec/IP Filtering** > **Client Certificate** eller **IEEE802.1X** > **Client Certificate**.
2. Klicka på **Delete**.
3. Bekräfta att du vill ta bort certifikatet i meddelandet som visas.

### Relaterad information

➡ ”Öppna Web Config” på sidan 23

## Uppdatera ett självsignerat certifikat

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

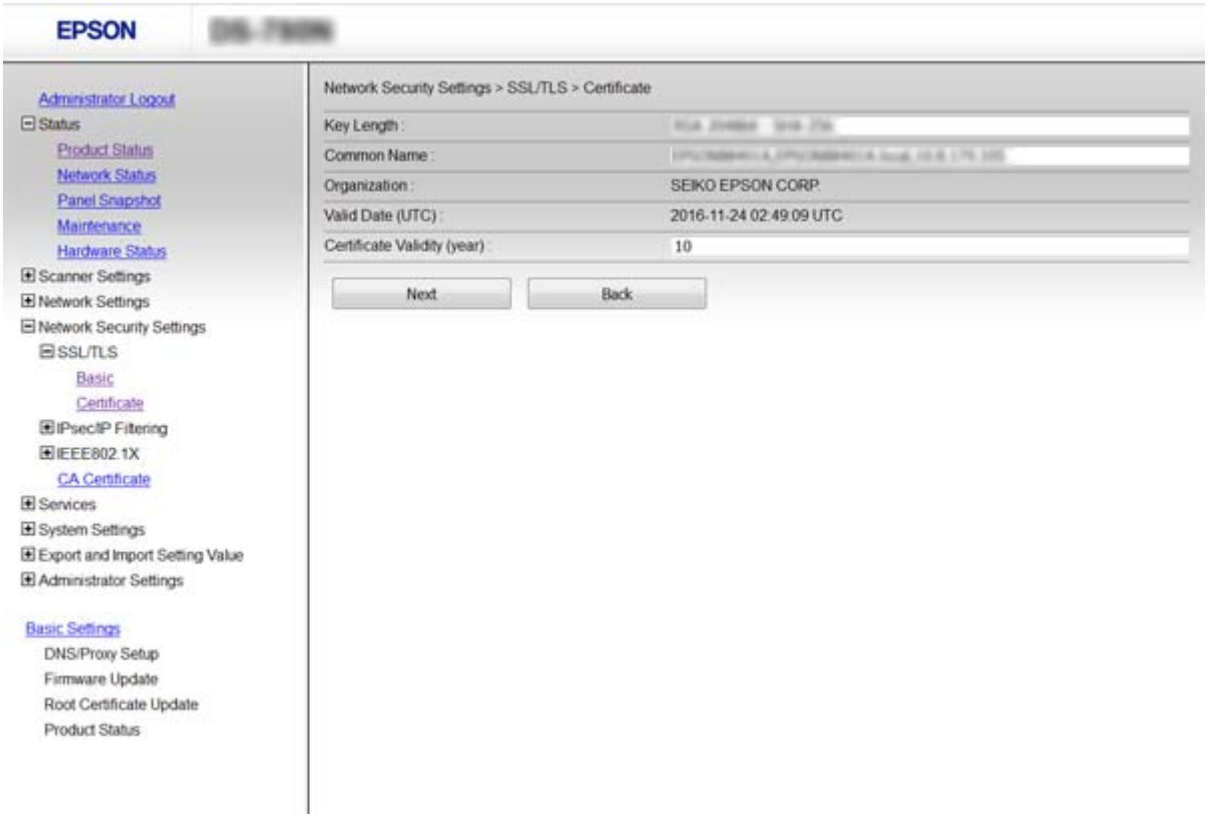
Använd ett självsignerat certifikat tills du hämtar och importerar ett CA-signerat certifikat.

1. Öppna Web Config och välj **Network Security Settings** > **SSL/TLS** > **Certificate**.
2. Klicka på **Update**.
3. Ange **Common Name**.

   Skriv en IP-adress eller en identifierare som ett FQDN-namn för skannern. Du kan uppge mellan 1 och 128 tecken.

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

4. Ange en giltighetsperiod för certifikatet.




5. Klicka på **Next**.

   Ett bekräftelsemeddelande visas.

6. Klicka på **OK**.

   Skannern uppdateras.

***Anmärkning:***
*Verifiera certifikatinformationen genom att klicka på* ***Confirm****.*

### Relaterad information

➡ ”Öppna Web Config” på sidan 23

# Konfigurera CA Certificate

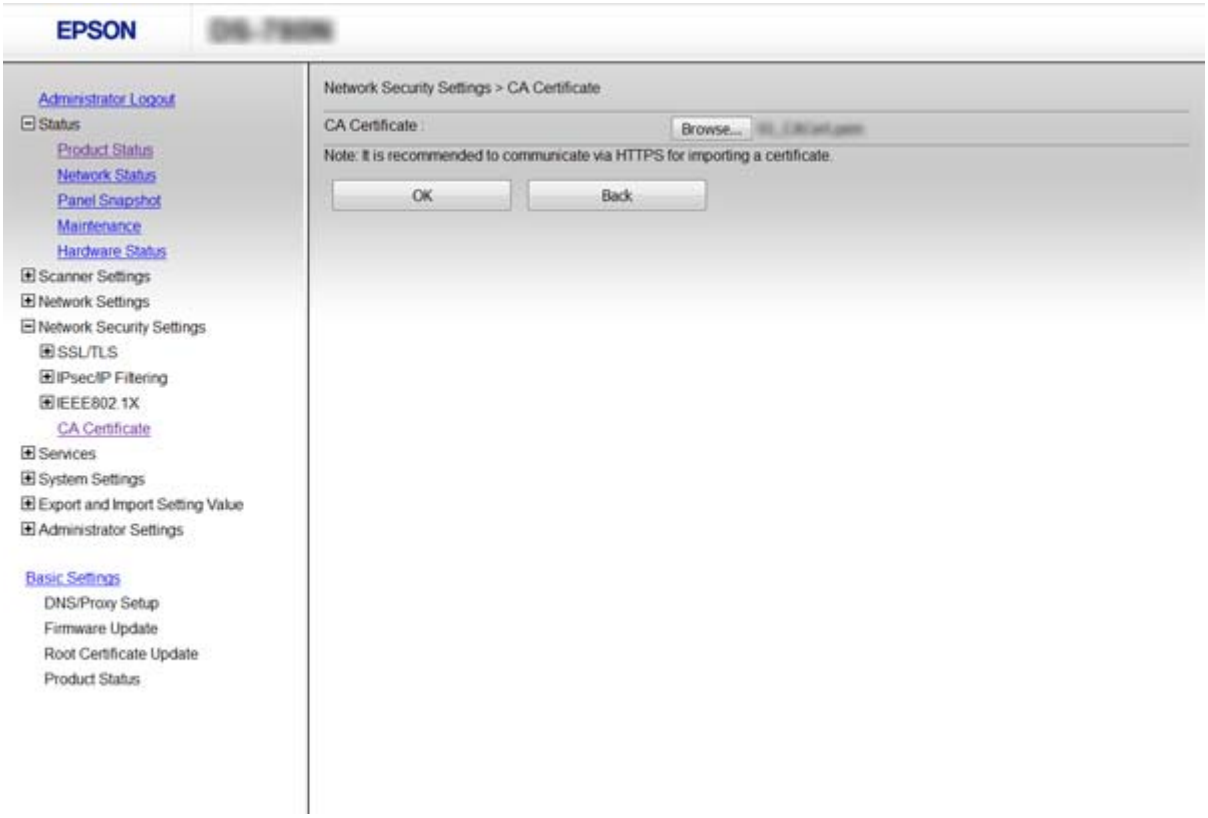
Du kan importera, visa och ta bort ett CA Certificate.

## Importera ett CA Certificate

1. Öppna Web Config, och välj sedan **Network Security Settings** > **CA Certificate**.

2. Klicka på **Import**.

3. Ange det CA Certificate du vill importera.




4. Klicka på **OK**.

När importen är klar kommer du tillbaka till skärmen **CA Certificate** och det importerade CA Certificate visas.

### Relaterad information

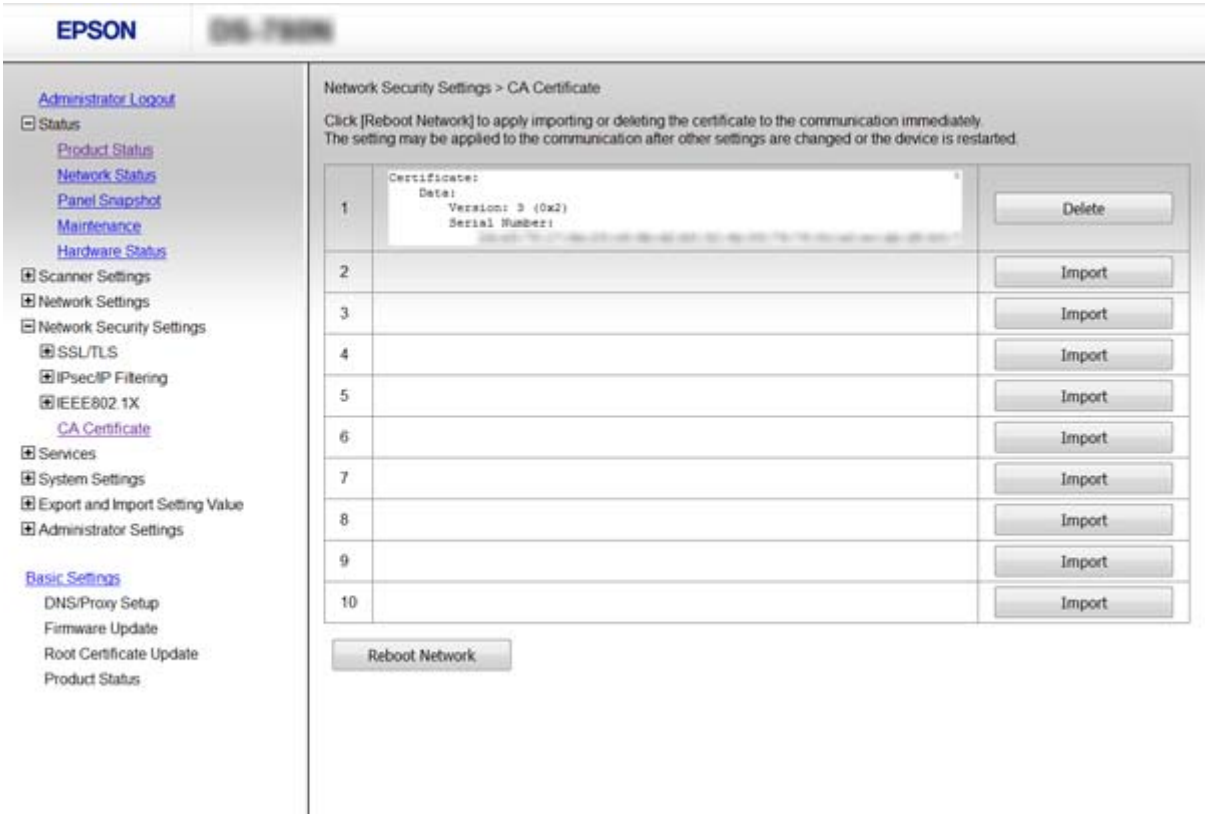
➡ ”Öppna Web Config” på sidan 23

## Ta bort ett CA Certificate

Du kan ta bort det importerade CA Certificate.

1. Öppna Web Config, och välj sedan **Network Security Settings** > **CA Certificate**.

2. Klicka på **Delete** bredvid det CA Certificate du vill ta bort.




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

### Relaterad information

➡ ”Öppna Web Config” på sidan 23

# Krypterad kommunikation med IPsec/IP-filtrering

## Om IPsec/IP Filtering

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

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

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

# Konfigurera Default Policy

1. Öppna Web Config och välj **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Ange ett värde för varje alternativ.
3. Klicka på **Next**.

   Ett bekräftelsemeddelande visas.
4. Klicka på **OK**.

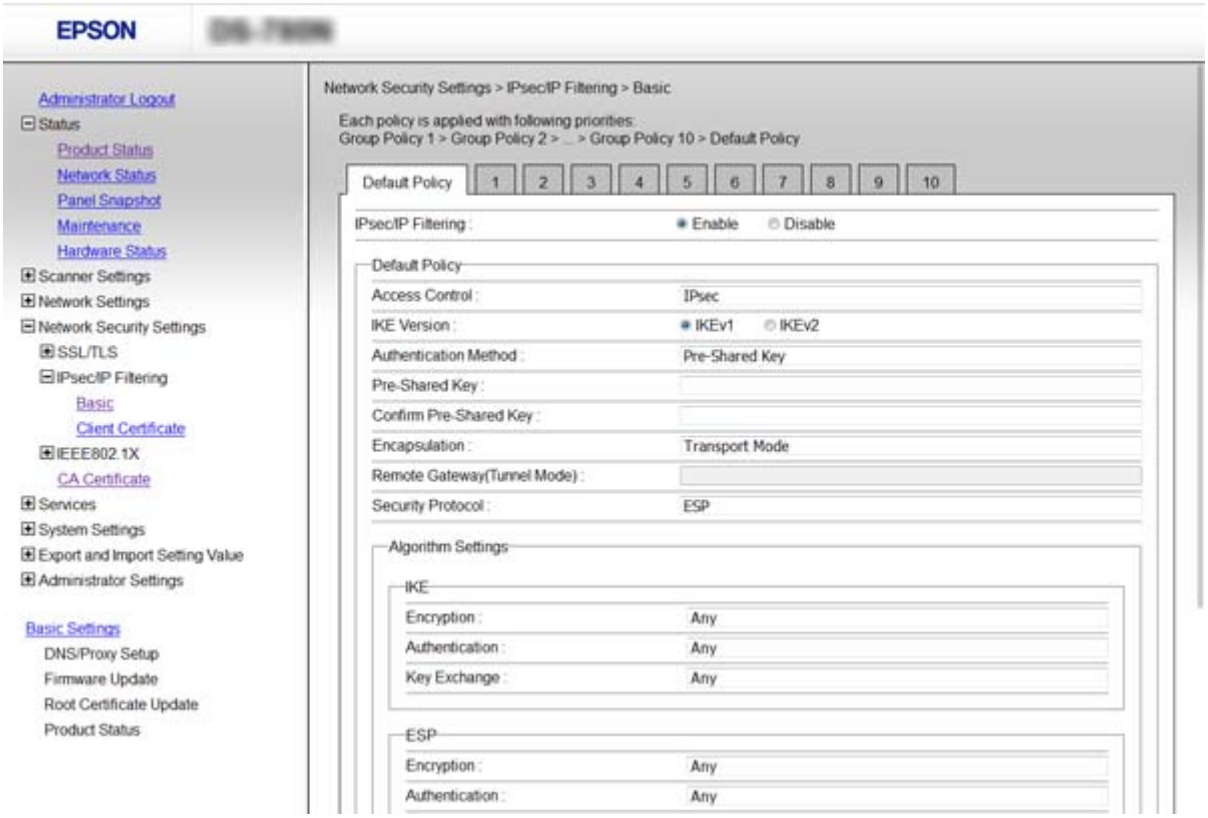
   Skannern uppdateras.

### Relaterad information

➡ ”Öppna Web Config” på sidan 23

➡ ”Inställningsalternativ för Default Policy” på sidan 72

## Inställningsalternativ för Default Policy




| Alternativ | Inställningar och beskrivning |
|---|---|
| IPsec/IP Filtering | Du kan aktivera och inaktivera funktioner för IPsec/IP-nätverk. |

## Avancerade säkerhetsinställningar för företag

| Alternativ | Inställningar och beskrivning | |
|---|---|---|
| Access Control | Konfigurera en metod för styrning av trafiken av IP-paket. | |
| | Permit Access | Välj detta när du vill att konfigurerade IP-paket ska få passera. |
| | Refuse Access | Välj detta när du inte vill att konfigurerade IP-paket ska få passera. |
| | IPsec | Välj detta när du vill att konfigurerade IPsec-paket ska få passera. |
| IKE Version | Välj IKEv1 eller IKEv2 för IKE-version.<br>Välj ett av alternativen enligt enheten som skannern är ansluten till. | |
| IKEv1 | Följande alternativ visas när du väljer **IKEv1** för **IKE Version**. | |
| | Authentication Method | Du måste hämta och importera ett CA-signerat certifikat i förväg om du väljer **Certificate**. |
| | Pre-Shared Key | Om du väljer **Pre-Shared Key** för **Authentication Method**, ska du ange en fördelad nyckel med mellan 1 och 127 tecken. |
| | Confirm Pre-Shared Key | Ange nyckeln som du konfigurerade som bekräftelse. |
| IKEv2 | Följande alternativ visas när du väljer **IKEv2** för **IKE Version**. | |
| Local | Authentication Method | Du måste hämta och importera ett CA-signerat certifikat i förväg om du väljer **Certificate**. |
| | ID Type | Välj typen av ID för skannern. |
| | ID | Ange skannerns ID som matchar typen av ID.<br>Du kan inte använda "@", "#", och "=" för första tecknet.<br>**Distinguished Name**: Ange 1 till 128 1-byte ASCII (0x20 till 0x7E) tecken. Du behöver inkludera "=".<br>**IP Address**: Ange IPv4- eller IPv6-format.<br>**FQDN**: Ange en kombination mellan 1 och 255 tecken med A–Z, a–z, 0–9, "-", och punkt (.).<br>**Email Address**: Ange 1 till 128 1-byte ASCII (0x20 till 0x7E) tecken. Du behöver inkludera "@".<br>**Key ID**: Ange 1 till 128 1-byte ASCII (0x20 till 0x7E) tecken. |
| | Pre-Shared Key | Om du väljer **Pre-Shared Key** för **Authentication Method**, ska du ange en fördelad nyckel med mellan 1 och 127 tecken. |
| | Confirm Pre-Shared Key | Ange nyckeln som du konfigurerade som bekräftelse. |

## Avancerade säkerhetsinställningar för företag

| Alternativ | Inställningar och beskrivning | |
|---|---|---|
| Remote | Authentication Method | Du måste hämta och importera ett CA-signerat certifikat i förväg om du väljer **Certificate**. |
| | ID Type | Välj typen av ID för enheten som du vill autentisera. |
| | ID | Ange skannerns ID som matchar typen av ID.<br>Du kan inte använda "@", "#", och "=" för första tecknet.<br>**Distinguished Name**: Ange 1 till 128 1-byte ASCII (0x20 till 0x7E) tecken. Du behöver inkludera "=".<br>**IP Address**: Ange IPv4- eller IPv6-format.<br>**FQDN**: Ange en kombination mellan 1 och 255 tecken med A–Z, a–z, 0–9, "-", och punkt (.).<br>**Email Address**: Ange 1 till 128 1-byte ASCII (0x20 till 0x7E) tecken. Du behöver inkludera "@".<br>**Key ID**: Ange 1 till 128 1-byte ASCII (0x20 till 0x7E) tecken. |
| | Pre-Shared Key | Om du väljer **Pre-Shared Key** för **Authentication Method**, ska du ange en fördelad nyckel med mellan 1 och 127 tecken. |
| | Confirm Pre-Shared Key | Ange nyckeln som du konfigurerade som bekräftelse. |
| Encapsulation | Om du väljer **IPsec** som **Access Control** måste du konfigurera en inkapslingsmetod. | |
| | Transport Mode | Välj detta om du bara använder skannern i samma lokala nätverk. IP-paket lager 4 eller senare krypteras. |
| | Tunnel Mode | Om du använder skannern i det Internet-förberedda nätverket, såsom IPsec-VPN, ska du markera det här alternativet. Rubriker och data i IP-paket krypteras. |
| Remote Gateway(Tunnel Mode) | Om du väljer **Tunnel Mode** för **Encapsulation**, ska du ange en gateway-adress med mellan 1 och 39 tecken. | |
| Security Protocol | **IPsec** för **Access Control**, 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. |
| Algorithm Settings | | |
| IKE | Encryption | Välj krypteringsalgoritm för IKE.<br>Objekten varierar beroende på version av IKE. |
| | Authentication | Välj autentiseringsalgoritm för IKE. |
| | Key Exchange | Välj nyckeländringsalgoritm för IKE.<br>Objekten varierar beroende på version av IKE. |

| Alternativ | Inställningar och beskrivning | |
|---|---|---|
| ESP | Encryption | Välj krypteringsalgoritm för ESP.<br>Detta är tillgängligt när **ESP** är valt för **Security Protocol**. |
| | Authentication | Välj autentiseringsalgoritm för ESP.<br>Detta är tillgängligt när **ESP** är valt för **Security Protocol**. |
| AH | Authentication | Välj krypteringsalgoritm för AH.<br>Detta är tillgängligt när **AH** är valt för **Security Protocol**. |

### Relaterad information

➡ ”Konfigurera Default Policy” på sidan 72

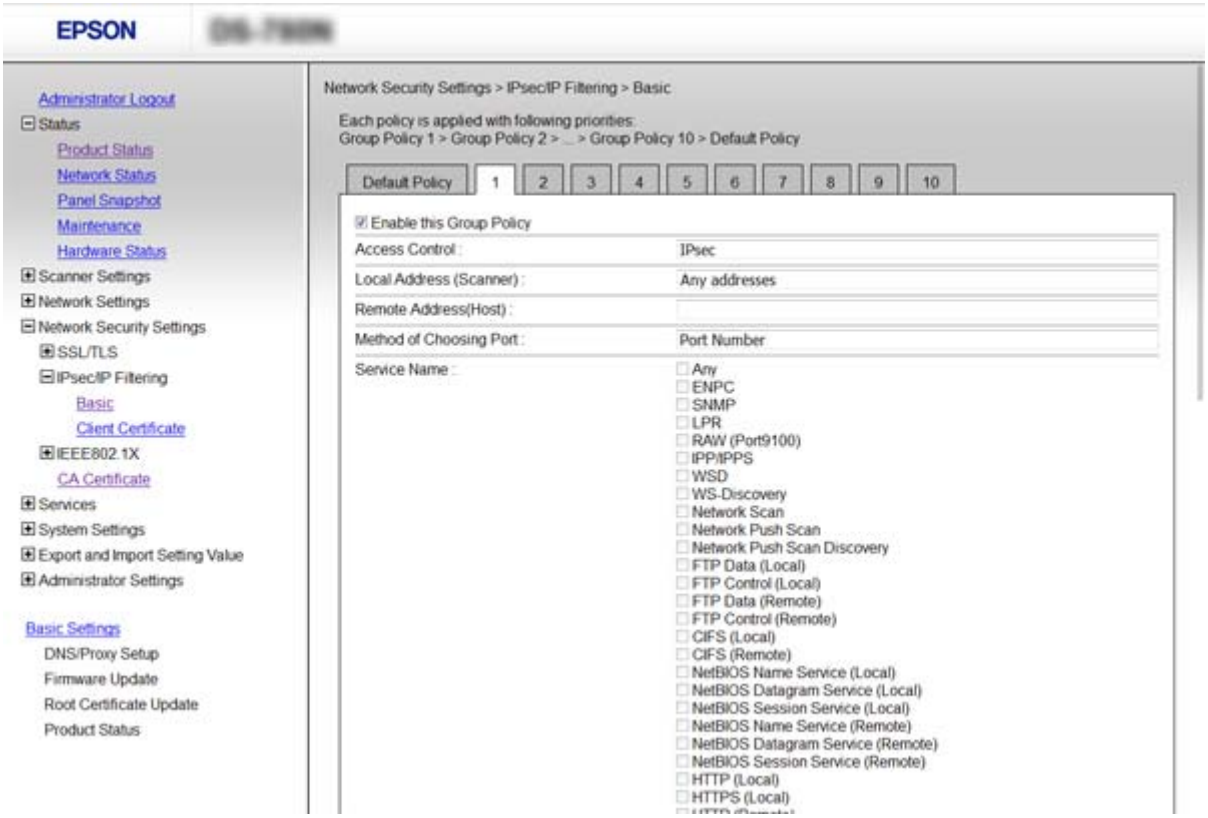
## Konfigurera Group Policy

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

### Relaterad information

➡ ”Öppna Web Config” på sidan 23
➡ ”Inställningsalternativ för Group Policy” på sidan 76

## Inställningsalternativ för Group Policy




| Alternativ | Inställningar och beskrivning | |
|---|---|---|
| Enable this Group Policy | Du kan aktivera och inaktivera en grupprincip. | |
| Access Control | Konfigurera en metod för styrning av trafiken av IP-paket. | |
| | Permit Access | Välj detta när du vill att konfigurerade IP-paket ska få passera. |
| | Refuse Access | 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 (Scanner) | 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**. | |
| Remote Address(Host) | Ange IP-adressen till en enhet för att styra åtkomsten. IP-adressen får innehålla max 43 tecken. Alla adresser styrs om du inte anger en IP-adress.<br>***Anmärkning:***<br>*Om en IP-adress tilldelas automatiskt (dvs. med DHCP) kanske anslutningen inte är tillgänglig. Konfigurera en statisk IP-adress.* | |
| Method of Choosing Port | Välj en metod för att specificera portar. | |
| Service Name | Ställ in ett alternativ om du väljer **Service Name** som **Method of Choosing Port**. | |

## Avancerade säkerhetsinställningar för företag

| Alternativ | Inställningar och beskrivning | |
|---|---|---|
| Transport Protocol | Om du väljer **Port Number** som **Method of Choosing Port** måste du konfigurera en inkapslingsmetod. | |
| | Any Protocol | 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 | Om du väljer **Port Number** för **Method of Choosing Port** och om du väljer **TCP** eller **UDP** för **Transport Protocol**, ska du ange portnummer för att styra paketmottagning och separera dem med komma. Du kan ange högst 10 portnummer.<br>Exempel: 20,80,119,5220<br>Alla portar styrs om du inte anger ett portnummer. | |
| Remote Port | Om du väljer **Port Number** för **Method of Choosing Port** och om du väljer **TCP** eller **UDP** för **Transport Protocol**, ska du ange portnummer för att styra paketsändning och separera dem med komma. Du kan ange högst 10 portnummer.<br>Exempel: 25,80,143,5220<br>Alla portar styrs om du inte anger ett portnummer. | |
| IKE Version | Välj IKEv1 eller IKEv2 för IKE-version.<br>Välj ett av alternativen enligt enheten som skannern är ansluten till. | |
| IKEv1 | Följande alternativ visas när du väljer **IKEv1** för **IKE Version**. | |
| | Authentication Method | Ställ in ett alternativ om du väljer **IPsec** som **Access Control**. Det använda certifikatet är gemensamt med standardprincipen. |
| | Pre-Shared Key | Om du väljer **Pre-Shared Key** för **Authentication Method**, ska du ange en fördelad nyckel med mellan 1 och 127 tecken. |
| | Confirm Pre-Shared Key | Ange nyckeln som du konfigurerade som bekräftelse. |
| IKEv2 | Följande alternativ visas när du väljer **IKEv2** för **IKE Version**. | |

## Avancerade säkerhetsinställningar för företag

| Alternativ | Inställningar och beskrivning | |
|---|---|---|
| Local | Authentication Method | Ställ in ett alternativ om du väljer **IPsec** som **Access Control**. Det använda certifikatet är gemensamt med standardprincipen. |
| | ID Type | Välj typen av ID för skannern. |
| | ID | Ange skannerns ID som matchar typen av ID.<br>Du kan inte använda "@", "#", och "=" för första tecknet.<br>**Distinguished Name**: Ange 1 till 128 1-byte ASCII (0x20 till 0x7E) tecken. Du behöver inkludera "=".<br>**IP Address**: Ange IPv4- eller IPv6-format.<br>**FQDN**: Ange en kombination mellan 1 och 255 tecken med A–Z, a–z, 0–9, "-", och punkt (.).<br>**Email Address**: Ange 1 till 128 1-byte ASCII (0x20 till 0x7E) tecken. Du behöver inkludera "@".<br>**Key ID**: Ange 1 till 128 1-byte ASCII (0x20 till 0x7E) tecken. |
| | Pre-Shared Key | Om du väljer **Pre-Shared Key** för **Authentication Method**, ska du ange en fördelad nyckel med mellan 1 och 127 tecken. |
| | Confirm Pre-Shared Key | Ange nyckeln som du konfigurerade som bekräftelse. |
| Remote | Authentication Method | Ställ in ett alternativ om du väljer **IPsec** som **Access Control**. Det använda certifikatet är gemensamt med standardprincipen. |
| | ID Type | Välj typen av ID för enheten som du vill autentisera. |
| | ID | Ange skannerns ID som matchar typen av ID.<br>Du kan inte använda "@", "#", och "=" för första tecknet.<br>**Distinguished Name**: Ange 1 till 128 1-byte ASCII (0x20 till 0x7E) tecken. Du behöver inkludera "=".<br>**IP Address**: Ange IPv4- eller IPv6-format.<br>**FQDN**: Ange en kombination mellan 1 och 255 tecken med A–Z, a–z, 0–9, "-", och punkt (.).<br>**Email Address**: Ange 1 till 128 1-byte ASCII (0x20 till 0x7E) tecken. Du behöver inkludera "@".<br>**Key ID**: Ange 1 till 128 1-byte ASCII (0x20 till 0x7E) tecken. |
| | Pre-Shared Key | Om du väljer **Pre-Shared Key** för **Authentication Method**, ska du ange en fördelad nyckel med mellan 1 och 127 tecken. |
| | Confirm Pre-Shared Key | Ange nyckeln som du konfigurerade som bekräftelse. |
| Encapsulation | Om du väljer **IPsec** som **Access Control** måste du konfigurera en inkapslingsmetod. | |
| | Transport Mode | Välj detta om du bara använder skannern i samma lokala nätverk. IP-paket lager 4 eller senare krypteras. |
| | Tunnel Mode | Om du använder skannern i det Internet-förberedda nätverket, såsom IPsec-VPN, ska du markera det här alternativet. Rubriker och data i IP-paket krypteras. |

**Avancerade säkerhetsinställningar för företag**

| Alternativ | Inställningar och beskrivning | |
|---|---|---|
| Remote Gateway(Tunnel Mode) | Om du väljer **Tunnel Mode** för **Encapsulation**, ska du ange en gateway-adress med mellan 1 och 39 tecken. | |
| Security Protocol | Ställ in ett alternativ om du väljer **IPsec** som **Access Control**. | |
| | 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. |
| Algorithm Settings | | |
| IKE | Encryption | Välj krypteringsalgoritm för IKE.<br>Objekten varierar beroende på version av IKE. |
| | Authentication | Välj autentiseringsalgoritm för IKE. |
| | Key Exchange | Välj nyckeländringsalgoritm för IKE.<br>Objekten varierar beroende på version av IKE. |
| ESP | Encryption | Välj krypteringsalgoritm för ESP.<br>Detta är tillgängligt när **ESP** är valt för **Security Protocol**. |
| | Authentication | Välj autentiseringsalgoritm för ESP.<br>Detta är tillgängligt när **ESP** är valt för **Security Protocol**. |
| AH | Authentication | Välj autentiseringsalgoritm för AH.<br>Detta är tillgängligt när **AH** är valt för **Security Protocol**. |

### Relaterad information


➡ ”Konfigurera Group Policy” på sidan 75

➡ ”Kombination av Local Address (Scanner) och Remote Address(Host) i Group Policy” på sidan 79

➡ ”Referenser för tjänstenamn enligt gruppolicy” på sidan 80


## Kombination av Local Address (Scanner) och Remote Address(Host) i Group Policy

| | | Inställning för Local Address (Scanner) | | |
|---|---|---|---|---|
| | | IPv4 | IPv6*2 | Any addresses*3 |
| **Inställning för Remote Address(Host)** | IPv4*1 | ✓ | – | ✓ |
| | IPv6*1, *2 | – | ✓ | ✓ |
| | Tom | ✓ | ✓ | ✓ |

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

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

*3 Förutom IPv6 länklokala adresser.

## Referenser för tjänstenamn enligt gruppolicy

***Anmärkning:***
*Otillgängliga tjänster visas, men kan inte väljas.*

| Tjänstenamn | Protokolltyp | Lokalt portnummer | Fjärrportnummer | Kontrollerade funktioner |
|---|---|---|---|---|
| Any | – | – | – | Alla tjänster |
| ENPC | UDP | 3289 | Valfri port | Söker efter en skanner från olika applikationer, såsom EpsonNet Config och en skannerdrivrutin |
| SNMP | UDP | 161 | Valfri port | Anskaffa och konfigurera MIB från applikationer, såsom EpsonNet Config och Epson skannerdrivrutin |
| WSD | TCP | Valfri port | 5357 | Kontrollera WSD |
| WS-Discovery | UDP | 3702 | Valfri port | Söka efter en skanner från WSD |
| Network Scan | TCP | 1865 | Valfri port | Vidarebefordra skanningdata från Document Capture Pro |
| Network Push Scan Discovery | UDP | 2968 | Valfri port | Söka efter en dator från skannern. |
| Network Push Scan | TCP | Valfri port | 2968 | Anskaffa jobbinformation för push-skanning från Document Capture Pro eller Document Capture |
| HTTP (Local) | TCP | 80 | Valfri port | HTTP(S)-server (vidarebefordran av data för Web Config och WSD) |
| HTTPS (Local) | TCP | 443 | Valfri port | |
| HTTP (Remote) | TCP | Valfri port | 80 | HTTP(S)-klient (kommunikation mellan firmware-uppdatering och rotcertifikatsuppdatering) |
| HTTPS (Remote) | TCP | Valfri port | 443 | |

# Exempel på konfigurering av IPsec/IP Filtering

### Endast mottagning av IPsec-paket

Det här exemplet visar hur du enbart konfigurerar en standardprincip.

**Default Policy**:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **IPsec**

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

❏ **Pre-Shared Key**: Ange högst 127 tecken.

**Group Policy**:

Konfigureras inte.

#### Godkänna skanningen med Epson Scan 2 och skannerinställningar

Det här exemplet tillåter kommunikation för skanningdata och skannerkonfiguration från specificerade tjänster.

**Default Policy**:

❏ **IPsec/IP Filtering**: **Enable**

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

**Group Policy**:

❏ **Enable this Group Policy**: Markera rutan.

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

❏ **Remote Address(Host)**: IP-adressen till en klient

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

❏ **Service Name**: Markera rutan för **ENPC**, **SNMP**, **Network Scan**, **HTTP (Local)** och **HTTPS (Local)**.

#### Endast mottagning från en angiven IP-adress fungerar

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

**Default Policy**:

❏ **IPsec/IP Filtering**: **Enable**

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

**Group Policy**:

❏ **Enable this Group Policy**: Markera rutan.

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

❏ **Remote Address(Host)**: IP-adressen till en administratörs klient

***Anmärkning:***
*Oavsett den konfigurerade principen kan klienten få tillgång till skannern och konfigurera den.*

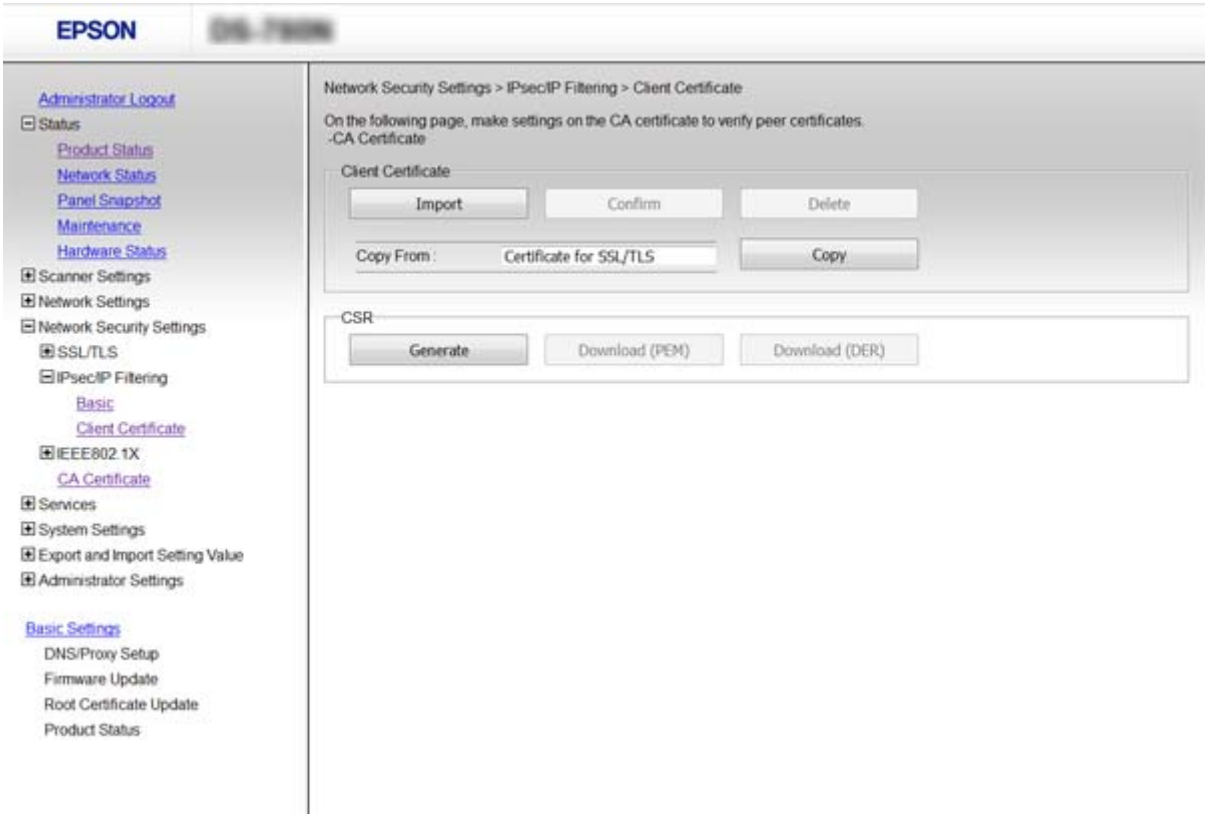
## Konfigurera ett certifikat för IPsec/IP Filtering

Konfigurera klientcertifikat för IPsec/IP-filtrering. Om du vill konfigurera certifikatutfärdare, gå till **CA Certificate**.

1. Öppna Web Config och välj **Network Security Settings** > **IPsec/IP Filtering** > **Client Certificate**.

2. Importera certifikatet i **Client Certificate**.

   Om du redan har importerat ett certifikat publicerat av en certifikatutfärdare i IEEE802.1X eller SSL/TLS, kan du kopiera certifikatet och använda den i IPsec/IP-filtrering. Om du vill kopiera, välj certifikatet från **Copy From** och klicka sedan på **Copy**.




**Relaterad information**

➡ ”Öppna Web Config” på sidan 23

➡ ”Hämta och importera ett CA-signerat certifikat” på sidan 64

# Använda SNMPv3-protokollet

## 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 skannern stöder SNMPv3-protokoll, kan du övervaka och kontrollera åtkomsten till skannern.

1. Öppna Web Config och välj **Services** > **Protocol**.
2. Ange ett värde för varje alternativ för **SNMPv3 Settings**.
3. Klicka på **Next**.

   Ett bekräftelsemeddelande visas.
4. Klicka på **OK**.

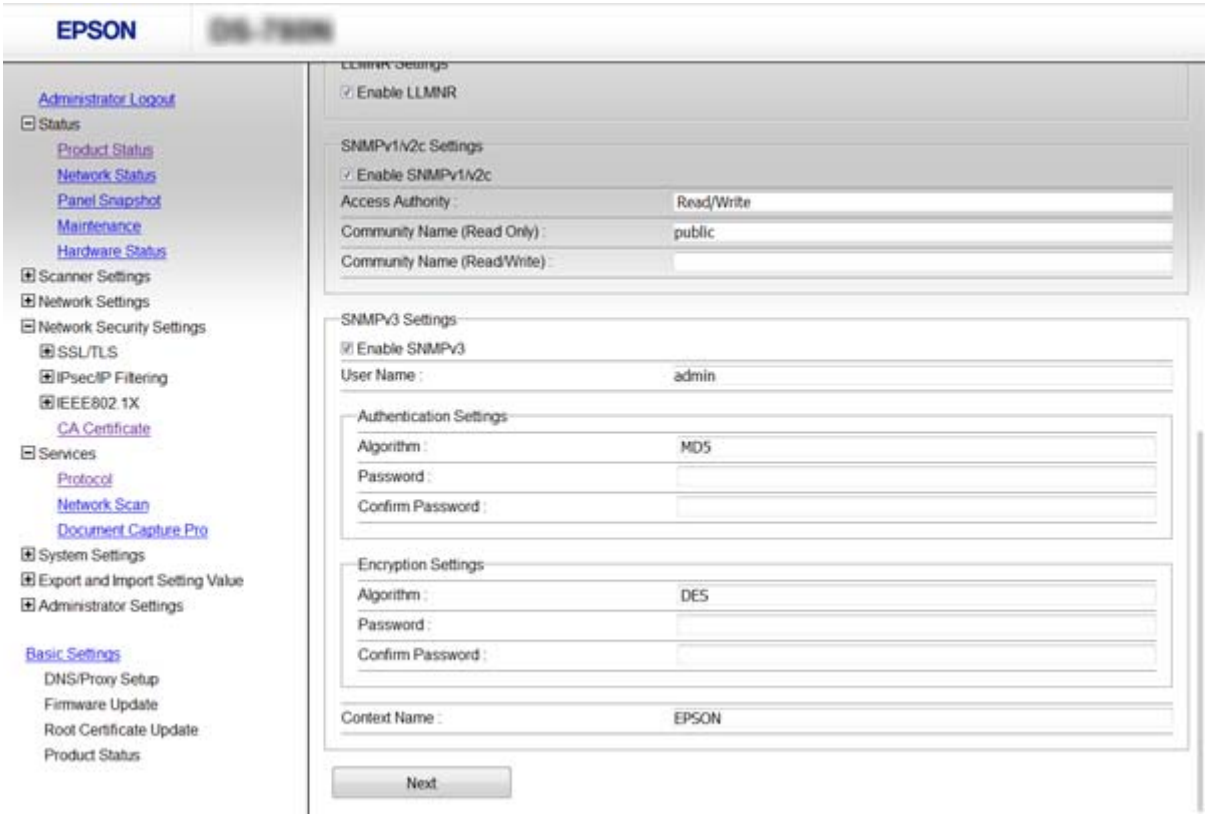
   Skannern uppdateras.

### Relaterad information

➡ ”Öppna Web Config” på sidan 23

➡ ”Alternativ för inställning av SNMPv3” på sidan 83

## Alternativ för inställning av SNMPv3




| Poster | Inställningar och förklaringar |
|---|---|
| Enable SNMPv3 | SNMPv3 aktiveras när rutan markeras. |
| User Name | Ange mellan 1 och 32 tecken med tecken om 1 byte. |
| Authentication Settings | |
| Algorithm | Välj en algoritm för autentisering. |

| Poster | Inställningar och förklaringar |
|---|---|
| Password | Ange mellan 8 och 32 tecken i ASCII (0x20-0x7E). |
| Confirm Password | Ange lösenordet som du konfigurerade för bekräftelsen. |
| Encryption Settings | |
| Algorithm | Välj en algoritm för kryptering. |
| Password | Ange mellan 8 och 32 tecken i ASCII (0x20-0x7E). |
| Confirm Password | Ange lösenordet som du konfigurerade för bekräftelsen. |
| Context Name | Ange mellan 1 och 32 tecken med tecken om 1 byte. |

### Relaterad information

➡ ”Konfigurera SNMPv3” på sidan 82

# Ansluta skannern till ett IEEE802.1X-nätverk

## Konfigurera ett IEEE802.1X-nätverk

Om skannern har stöd för IEEE802.1X kan du använda skannern i ett nätverk med autentisering som är anslutet till en RADIUS-server med ett nav som autentiserare.

1. Öppna Web Config och välj **Network Security Settings** > **IEEE802.1X** > **Basic**.
2. Ange ett värde för varje alternativ.
3. Klicka på **Next**.

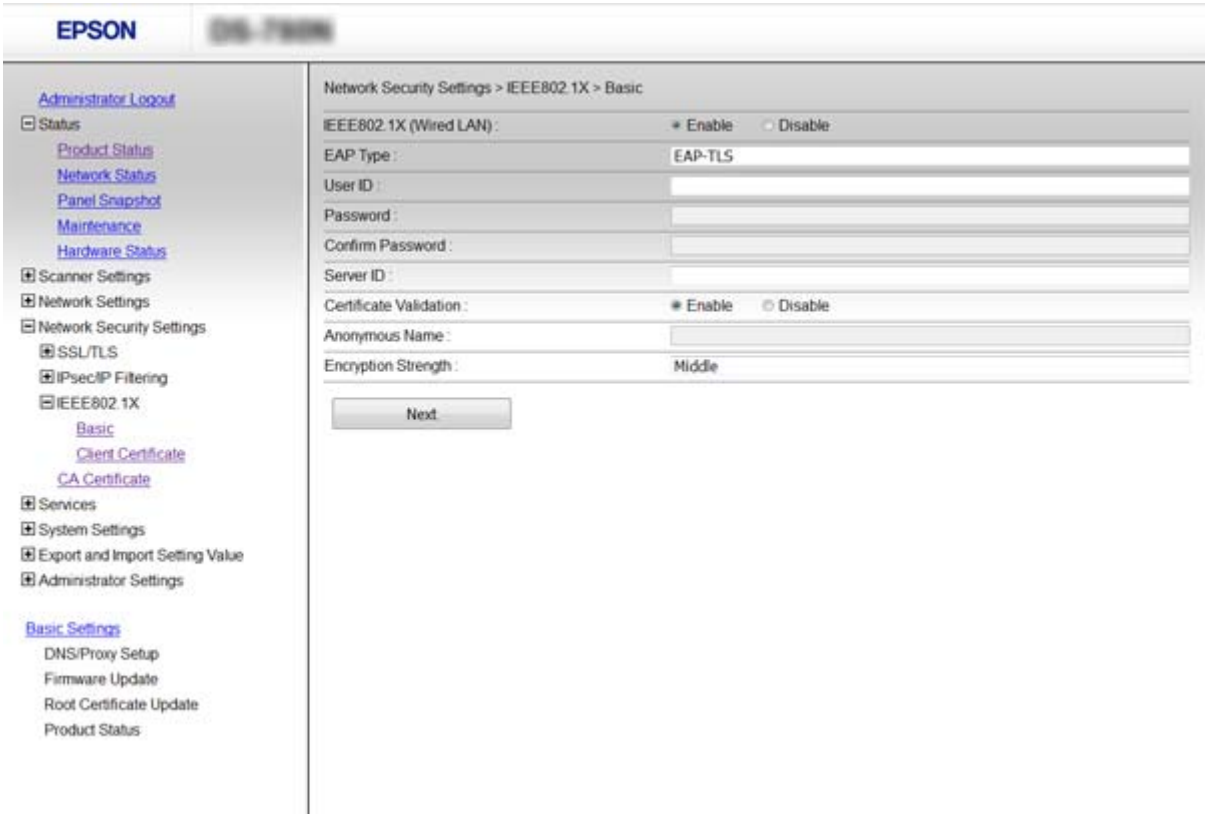
   Ett bekräftelsemeddelande visas.
4. Klicka på **OK**.

   Skannern uppdateras.

### Relaterad information

➡ ”Öppna Web Config” på sidan 23
➡ ”Inställningsalternativ för IEEE802.1X-nätverk” på sidan 85
➡ ”Kan inte öppna skrivaren eller skannern efter konfiguration av IEEE802.1X” på sidan 89

# Inställningsalternativ för IEEE802.1X-nätverk




| Alternativ | Inställningar och beskrivning | |
|---|---|---|
| IEEE802.1X (Wired LAN) | Du kan aktivera eller inaktivera inställningar på sidan (**IEEE802.1X** > **Basic**) för IEEE802.1X (trådbundet LAN). | |
| EAP Type | Välj en autentiseringsmetod mellan skannern och en RADIUS-server. | |
| | EAP-TLS | Du måste hämta och importera ett CA-signerat certifikat. |
| | PEAP-TLS | |
| | PEAP/MSCHAPv2 | Du måste konfigurera ett lösenord. |
| User ID | Konfigurera ett ID som ska användas för autentisering av en RADIUS-server.<br>Ange 1 till 128 1-byte ASCII (0x20 till 0x7E)-tecken. | |
| Password | Konfigurera ett lösenord för autentisering av skannern.<br>Ange 1 till 128 1-byte ASCII (0x20 till 0x7E)-tecken. Om du använder en Windows-server som en RADIUS-server kan du ange upp till 127 tecken. | |
| Confirm Password | Ange lösenordet som du konfigurerade som bekräftelse. | |
| Server ID | Du kan konfigurera ett server-ID för autentisering med en angiven RADIUS-server. Autentiseraren verifierar om ett server-ID anges i fältet subject/subjectAltName i ett servercertifikat som skickas från en RADIUS-server.<br>Ange 0 till 128 1-byte ASCII (0x20 till 0x7E)-tecken. | |
| Certificate Validation | Du kan ställa in certifikatvalidering oavsett autentiseringsmetod. Importera certifikatet i **CA Certificate**. | |

| Alternativ | Inställningar och beskrivning | |
|---|---|---|
| Anonymous Name | Om du väljer **PEAP-TLS** eller **PEAP/MSCHAPv2** som **Authentication Method** kan du konfigurera ett anonymt namn i stället för ett användar-ID för fas 1 i PEAP-autentisering.<br>Ange 0 till 128 1-byte ASCII (0x20 till 0x7E)-tecken. | |
| Encryption Strength | Du kan välja ett av följande. | |
| | High | AES256/3DES |
| | Middle | AES256/3DES/AES128/RC4 |

### Relaterad information

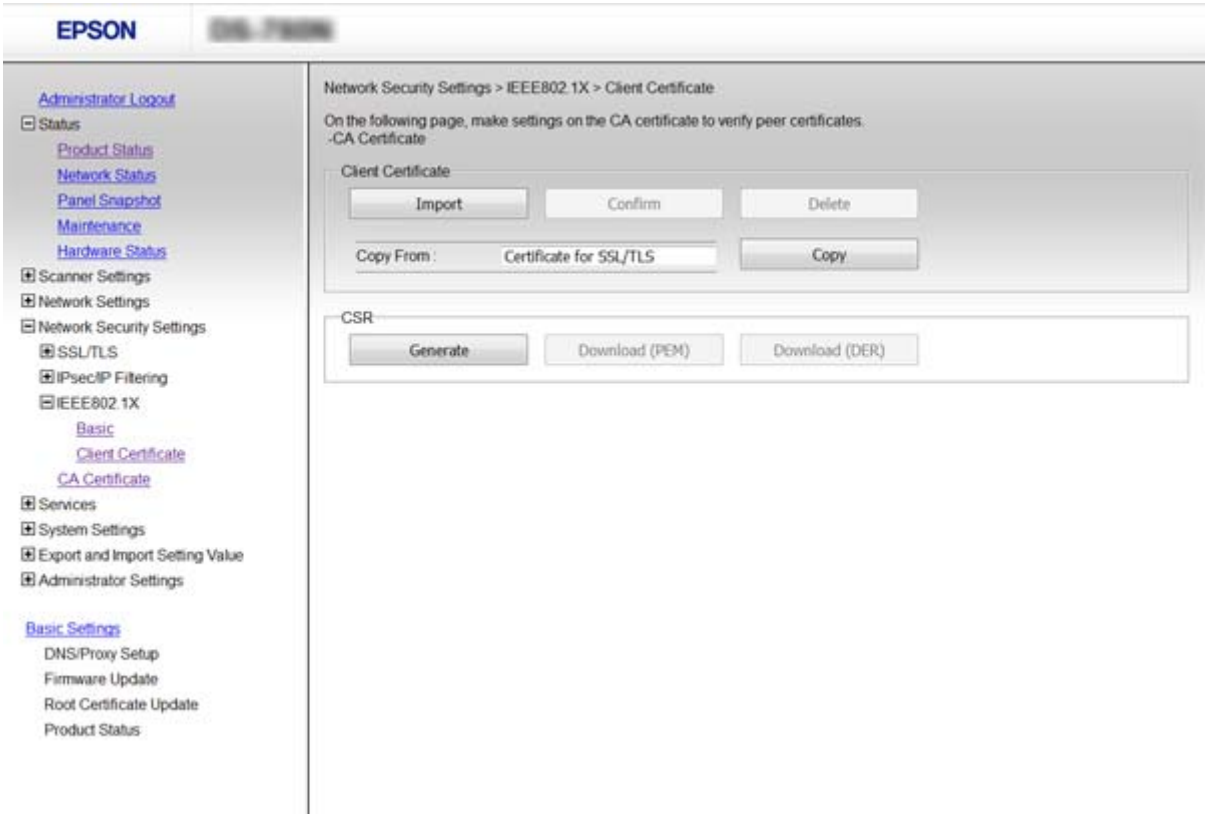
➡ ”Konfigurera ett IEEE802.1X-nätverk” på sidan 84

## Konfigurera ett certifikat för IEEE802.1X

Konfigurera klientcertifikatet för IEEE802.1X. Om du vill konfigurera certifikatutfärdare, gå till **CA Certificate**.

1. Öppna Web Config och välj **Network Security Settings** > **IEEE802.1X** > **Client Certificate**.
2. Ange ett certifikat i **Client Certificate**.

   Du kan kopiera certifikatet om det publiceras av en certifikatutfärdare. Om du vill kopiera, välj certifikatet från **Copy From** och klicka sedan på **Copy**.



**Relaterad information**

➡ ”Öppna Web Config” på sidan 23

➡ ”Hämta och importera ett CA-signerat certifikat” på sidan 64

# Lösa problem med avancerad säkerhet

## Återställa säkerhetsinställningarna

När du upprättar en mycket säker miljö, såsom IPsec-/IP-filtrering eller IEEE802.1X, kan du inte kommunicera med enheter, på grund av felaktiga inställningar eller fel i enheten eller servern. I så fall återställs säkerhetsinställningarna för att göra inställningar för enheten igen, eller för att medge tillfällig användning.

### Inaktivering av säkerhetsfunktionen med kontrollpanelen

Du kan inaktivera IPsec/IP-filtrering IEEE802.1X från skannerns kontrollpanel.

1. Tryck på **Inst.** > **Nätverksinställningar**.
2. Tryck på **Ändra inställningar**.
3. Tryck på objekt som du vill inaktivera.
   - ❏ **IPsec/IP Filtering**
   - ❏ **IEEE802.1X**
4. Tryck på **Fortsätt** när ett meddelande om att avsluta visas.

### Återställa säkerhetsfunktionen med webbkonfiguration

För IEEE802.1X, kanske enheter inte identifieras i nätverket. I det här fallet måste du inaktivera funktionen med skannerns kontrollpanel.

För IPsec/IP-filtrering kan du inaktivera funktionen om du kan få åtkomst till enheten från datorn.

#### *Inaktivera IPsec-/IP-filtrering med Web Config*

1. Öppna Web Config och välj **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Välj **Disable** för **IPsec/IP Filtering** i **Default Policy**.
3. Klicka på **Next**, och rensa sedan **Enable this Group Policy** för alla gruppolicier.
4. Klicka på **OK**.

**Relaterad information**

➡ ”Öppna Web Config” på sidan 23

# Problem att använda funktionerna för nätverkssäkerhet

## Bortglömd på förhand delad nyckel

### Konfigurera nyckeln igen med Web Config.

För att ändra nyckeln öppnar du Web Config och väljer **Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Default Policy** eller **Group Policy**.

När du ändrar den i förväg delade nyckeln, konfigurera den i förväg delade nyckeln för datorer.

### Relaterad information

➡ ”Öppna Web Config” på sidan 23

## Det går inte att kommunicera med IPsec-kommunikation

### Använder du en algoritm som saknar stöd för datorinställningarna?

Skannern har stöd för följande algoritmer.

| Säkerhetsmetoder | Algoritmer |
|---|---|
| IKE-krypteringsalgoritm | AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES |
| IKE-autentiseringsalgoritm | SHA-1, SHA-256, SHA-384, SHA-512, MD5 |
| IKE-nyckelutväxlingsalgoritm | DH-grupp 1, DH-grupp 2, DH-grupp 5, DH-grupp 14, DH-grupp 15, DH-grupp 16, DH-grupp 17, DH-grupp 18, DH-grupp 19, DH-grupp 20, DH-grupp 21, DH-grupp 22, DH-grupp 23, DH-grupp 24, DH-grupp 25, DH-grupp 26, DH-grupp 27*, DH-grupp 28*, DH-grupp 29*, DH-grupp 30* |
| ESP-krypteringsalgoritm | AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES |
| ESP-autentiseringsalgoritm | SHA-1, SHA-256, SHA-384, SHA-512, MD5 |
| AH-autentiseringsalgoritm | SHA-1, SHA-256, SHA-384, SHA-512, MD5 |

* endast tillgänglig för IKEv2

### Relaterad information

➡ ”Krypterad kommunikation med IPsec/IP-filtrering” på sidan 71

## Plötsligt går det inte att kommunicera

### Är skannerns IP-adress ogiltig eller har den ändrats?

Inaktivera IPsec med skannerns kontrollpanel.

Om DHCP är för gammal startar du om, eftersom IPv6-adressen är för gammal eller inte har hämtats, och sedan kanske den registrerade IP-adressen för skannerns Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**) inte kan hittas.

Använd en statisk IP-adress.

#### Är datorns IP-adress ogiltig eller har den ändrats?

Inaktivera IPsec med skannerns kontrollpanel.

Om DHCP är för gammal startar du om, eftersom IPv6-adressen är för gammal eller inte har hämtats, och sedan kanske den registrerade IP-adressen för skannerns Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) inte kan hittas.

Använd en statisk IP-adress.

#### Relaterad information

➡ ”Öppna Web Config” på sidan 23

➡ ”Krypterad kommunikation med IPsec/IP-filtrering” på sidan 71

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

#### Det inställda värdet kan vara felaktigt.

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

#### Relaterad information

➡ ”Krypterad kommunikation med IPsec/IP-filtrering” på sidan 71

## Kan inte öppna skrivaren eller skannern efter konfiguration av IEEE802.1X

#### Inställningarna kan vara felaktiga.

Inaktivera IEEE802.1X via skannerns kontrollpanel. Anslut skannern till datorn och konfigurera IEEE802.1X igen.

#### Relaterad information

➡ ”Konfigurera ett IEEE802.1X-nätverk” på sidan 84

# 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 skannern 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 66

## Det går inte att uppdatera ett självsignerat certifikat

### Har Common Name angetts?

Du måste ange **Common Name**.

### Används tecken som inte stöds i Common Name? Japanska stöds till exempel inte.

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

### Finns det ett komma eller mellanslag i Common Name?

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

### Relaterad information

➡ ”Uppdatera ett självsignerat certifikat” på sidan 68

## Det går inte att skapa en CSR

### Har Common Name angetts?

Du måste ange **Common Name**.

### Används tecken som inte stöds i Common Name, Organization, Organizational Unit, Locality, State/ Province? Japanska stöds till exempel inte.

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

### Finns det ett komma eller mellanslag i Common Name?

Om det finns ett komma kommer **Common Name** 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 64

## Varningar om ett digitalt certifikat visas

| Meddelanden | Orsak/åtgärd |
|---|---|
| Enter a Server Certificate. | **Orsak:**<br>Du har inte valt en fil som ska importeras.<br>**Åtgärd:**<br>Välj en fil och klicka på **Import**. |
| CA Certificate 1 is not entered. | **Orsak:**<br>CA-certifikat 1 har inte angetts, endast CA-certifikat 2 har angetts.<br>**Åtgärd:**<br>Importera CA-certifikat 1 först. |
| Invalid value below. | **Orsak:**<br>Filens sökväg och/eller lösenordet innehåller tecken som inte stöds.<br>**Åtgärd:**<br>Kontrollera att rätt tecken angetts i posten. |
| Invalid date and time. | **Orsak:**<br>Datum och klockslag har inte ställts in på skannern.<br>**Åtgärd:**<br>Ställ in datum och klockslag med Web Config eller EpsonNet Config. |
| Invalid password. | **Orsak:**<br>Lösenordet som angetts för CA-certifikatet och det angivna lösenordet matchar inte varandra.<br>**Åtgärd:**<br>Ange rätt lösenord. |

## Avancerade säkerhetsinställningar för företag

| Meddelanden | Orsak/åtgärd |
|---|---|
| Invalid file. | **Orsak:**<br>Du importerar inte en certifikatfil med X509-format.<br>**Åtgärd:**<br>Kontrollera att du väljer rätt certifikat som skickats av en betrodd certifikatutfärdare. |
| | **Orsak:**<br>Filen som du importerade är för stor. Den maximala filstorleken är 5 KB.<br>**Åtgärd:**<br>Om du valt rätt fil kan certifikatet vara skadat eller förfalskat. |
| | **Orsak:**<br>Kedjan i certifikatet är inte giltig.<br>**Åtgärd:**<br>Mer information om certifikatet finns på certifikatutfärdarens webbplats. |
| Cannot use the Server Certificates that include more than three CA certificates. | **Orsak:**<br>Certifikatfilen i PKCS#12-format innehåller mer än 3 CA-certifikat.<br>**Åtgärd:**<br>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. |
| The certificate has expired. Check if the certificate is valid, or check the date and time on the product. | **Orsak:**<br>Certifikatet har gått ut.<br>**Åtgärd:**<br>❏ Om certifikatet har gått ut ska du hämta och importera ett nytt certifikat.<br>❏ Om certifikatet inte har gått ut ska du kontrollera att rätt datum och klockslag ställts in på skannern. |
| Private key is required. | **Orsak:**<br>Det finns ingen parad privat nyckel med certifikatet.<br>**Åtgärd:**<br>❏ Om certifikatet är i PEM/DER-formatet och det hämtats med en CSR via en dator ska du ange den privata nyckelfilen.<br>❏ Om certifikatet är i PKCS#12-formatet och det hämtats med en CSR via en dator ska du skapa en fil som innehåller den privata nyckeln. |
| | **Orsak:**<br>Du har importerat ett PEM/DER-certifikat som hämtats med en CSR med Web Config på nytt.<br>**Åtgärd:**<br>Om certifikatet är i PEM/DER-formatet och det hämtats med en CSR via Web Config kan du bara importera det en gång. |

| Meddelanden | Orsak/åtgärd |
|---|---|
| Setup failed. | **Orsak:**<br>Det går inte att avsluta konfigureringen eftersom det blev fel i kommunikationen mellan skannern och datorn eller filen inte går att läsa på grund av fel.<br>**Åtgärd:**<br>Importera filen igen när du har kontrollerat den angivna filen och kommunikationen. |

### Relaterad information

➡ ”Om digital certifiering” på sidan 63

## Ett CA-signerat certifikat har raderats av misstag

### Finns det en säkerhetskopia av filen?

Importera certifikatet igen om du inte har en säkerhetskopia.

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

### Relaterad information

➡ ”Radera ett CA-signerat certifikat” på sidan 67

➡ ”Importera ett CA-signerat certifikat” på sidan 66