Pro C7100/C7100x/C7110/C7110x

Bruksanvisning

Säkerhetsguide

Läs avsnittet Säkerhetsinformation i handboken "Läs detta först" innan du använder maskinen, för säker och korrekt användning.

INNEHÅLL

1. Komma igång

2. Konfigurera användarautentisering

3. Begränsa maskinanvändning

4. Förhindra läckage av information från maskiner

5. Utökad nätverkssäkerhet

6. Förhindra spridning av dokument

7. Hantera maskinen

8. Felsökning

9. Lista över inställningsbehörigheter

1. Komma igång

I det här kapitlet beskrivs hur du vidtar nödvändiga försiktighetsåtgärder när du använder maskinens säkerhetsfunktioner och hur du konfigurerar administratörsinställningarna.

Innan du konfigurerar säkerhetsfunktionerna

Viktigt

- **Om säkerhetsfunktionerna inte konfigureras är maskinens data sårbar för attack.**
- Förhindra att maskinen blir stulen eller avsiktligt skadas genom att installera den på en säker plats.
- Den som köper denna maskin måste se till att maskinen används korrekt och i enlighet med de funktioner som bestämts av maskinadministratören och övervakaren. Om administratören eller övervakaren inte gör nödvändiga säkerhetsinställningar finns det risk att användarna äventyrar säkerheten.
- Innan maskinens säkerhetsfunktioner konfigureras, och för att säkerställa korrekt användning, måste administratörer noggrant läsa igenom hela Säkerhetsguiden, med särskild tonvikt på avsnittet "Innan du konfigurerar säkerhetsfunktionerna".
- Administratörerna informerar användarna hur de använder säkerhetsfunktionerna på rätt sätt.
- Om den här maskinen är ansluten till ett nätverk ska det skyddas av en brandvägg eller liknande säkerhetsfunktion.
- För att skydda data under kommunikationsfasen, ska maskinens säkerhetsfunktioner för kommunikation tillämpas och den ska anslutas till enheter med stöd för säkerhetsfunktioner såsom krypterad kommunikation.
- Administratörer ska regelbundet undersöka maskinens loggar med avseende på avvikande och ovanliga händelser.

Innan du använder maskinen

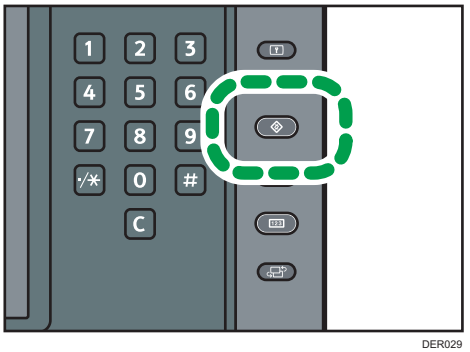
1

I det här avsnittet beskrivs hur du krypterar överförd information och konfigurerar administratörskontot. Om du vill ha hög säkerhetsnivå ska du göra följande inställning innan du använder maskinen.

1. **Slå på strömmen till maskinen.**

   För information om hur du sätter på strömmen, se handboken Komma igång.

2. **Tryck på [User Tools] (Användarverktyg)**



DER029

3. **Tryck på [Systeminställning].**
4. **Tryck på [Gränssnittsinst].**
5. **Ange Ipv4-adress.**

   För mer information om hur du anger IPv4-adressen, se Anslut maskinen/Systeminställning.

6. **Tryck på [Filöverföring] i [Systeminställning].**
7. **Tryck på [E-postadress för administratör] och ange sedan e-postadressen till maskinens administratör.**
8. **Skapa och installera enhetscertifikatet från kontrollpanelen.**

   För information om hur du installerar enhetscertifikatet, se s. 99 "Skydda kommunikationsvägar via ett enhetscertifikat".

   När du anger e-postadress för enhetscertifikatet ska du ange samma adress som du angav i steg 7.

9. **Ändra administratörens användarnamn och lösenord.**

   För mer information om hur du anger administratörers användarnamn och lösenord, se s. 14 "Registrera och ändra administratörer".

10. **Anslut maskinen till den allmänna nätverksmiljön.**

Obs

- För att aktivera högre säkerhet, se s. 202 "Mer information om utökad säkerhet".

Administratörer och användare

I detta avsnitt beskrivs begreppen "administratör", "övervakare", "användare" och "ägare" som de används i den här handboken.

Administratör

Maskinen använder 4 typer av administratörer: användaradministratör, maskinadministratör, nätverksadministratör och filadministratör.

Deras främsta uppgift är att ange maskinens inställningar. Deras behörighet beror på administratörstypen. Administratörer kan inte utföra normala funktioner, som att skriva ut dokument.

Övervakare

Det finns bara en övervakare. Övervakaren kan ange varje administratörs lösenord. För normal drift krävs ingen övervakare eftersom administratörer anger sina egna lösenord.

Användare

Användarna är personer som använder maskinen för normala funktioner, som att skriva ut dokument.

Ägare

En användare som har registrerat lagrade utskriftsfiler i maskinen kallas för en ägare.

Administratörer

Administratörer hanterar användarnas åtkomst till maskinen och diverse andra viktiga funktioner och inställningar.

När en administratör ska kontrollera begränsad åtkomst och inställningar måste du börja med att välja maskinens administratör och aktivera autentiseringsfunktionen innan maskinen används. När autentiseringsfunktionen aktiveras krävs inloggning med användarnamn och lösenord för att man ska kunna använda maskinen. Administratörsrollen för denna maskin är uppdelad i 4 olika kategorier utifrån funktion: användaradministratör, maskinadministratör, nätverksadministratör och filadministratör. Delade administratörsuppgifter underlättar varje administratörs uppgifter samtidigt som det förhindrar obehöriga administratörsfunktioner. Flera administratörsroller kan tilldelas en administratör och en roll kan delas av fler än en administratör. Man kan även utse en övervakare med behörighet att ändra administratörers lösenord.

Administratörer kan inte använda funktioner som är tillgängliga för användare, till exempel skriva ut dokument. För att utföra sådana funktioner måste administratören också vara autentiserad som användare.

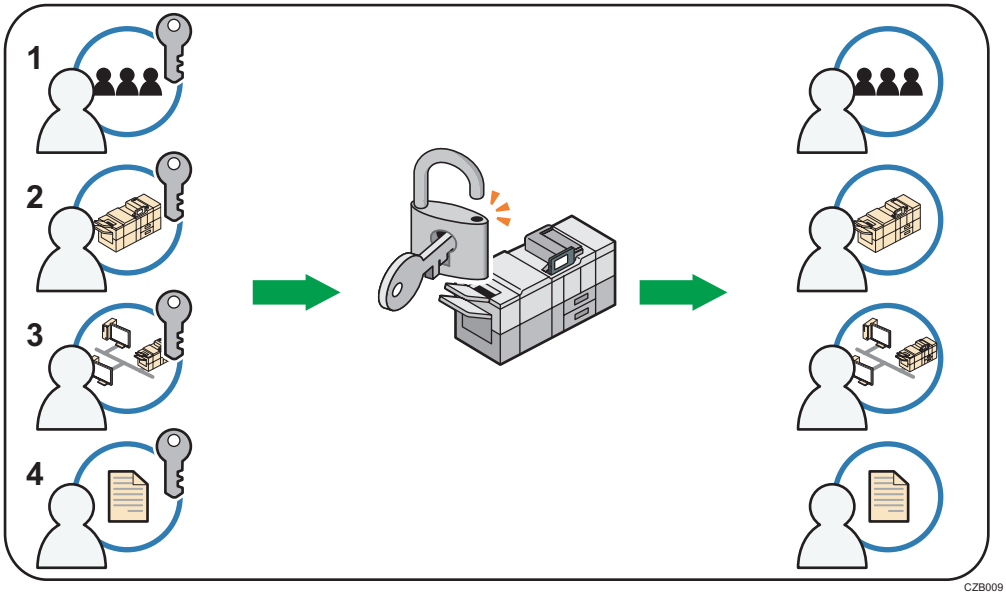
För anvisningar om hur man registrerar administratörer, se s. 14 "Registrera och ändra administratörer", för anvisningar om hur man ändrar adminstratörens lösenord, se s. 21 "Övervakare". För information om användare, se s. 25 "Användare".

Konfigurera administratörsautentisering

Administratörsautentisering kräver användarnamn och lösenord för att verifiera administratörer som försöker ange maskininställningar eller få åtkomst till dem via ett nätverk. När du registrerar en administratör kan du inte använda ett användarnamn som redan finns i adressboken. Administratörer hanteras på ett annat sätt än användarna registrerade i adressboken. Windows-autentisering och LDAP-autentisering utförs inte för en administratör, varför en administratör kan logga in även om servern inte kan nås på grund av ett nätverksproblem. Varje administratör identifieras av ett användarnamn. En person kan fungera som mer än en sorts administratör om ett och samma användarnamn får flera administratörsrättigheter. För instruktioner om hur man registrerar administratören, se s. 14 "Registrera och ändra administratörer".

Du kan specificera användarnamn och lösenord samt krypteringslösen för respektive administratör. Lösenordet för kryptering används för kryptering av data överförd via SNMPv3. Det används också av program som t.ex. Device Manager NX som använder SNMPv3. Administratörer kan endast hantera maskininställningar och kontrollera användaråtkomst, Administratörer kan endast hantera maskininställningar och kontrollera användaråtkomst. De kan inte använda funktioner som utskrift. För att använda denna funktion måste administratören registrera sig som en användare i adressboken, och sedan bli autentiserad. Ange administratörsautentisering och ange sedan användarautentisering. För information om hur man anger autentisering, se s. 27 "Konfigurera Konfigurera användarautentisering".

Roller för varje administratör



1. **Användaradministratör**

   Hanterar personuppgifter i adressboken.

En användaradministratör kan registrera/radera användare i adressboken eller ändra användares personliga information.

Användare registrerade i adressboken kan också ändra och radera sin egen information.

Om en användare glömmer sitt lösenord kan användaradministratören radera det och skapa ett nytt som ger användaren åtkomst till maskinen igen.

2. **Maskinadministratör**

   Hanterar främst maskinens standardinställningar. Du kan ställa in maskinen så att standarden för varje funktion bara kan anges av maskinadministratören. Med den inställningen kan du hindra obehöriga användare från att ändra inställningarna och låta maskinen användas säkert av dess användare.

3. **Nätverksadministratör**

   Hanterar nätverksinställningar. Du kan ställa in maskinen så att endast nätverksadministratören kan ange IP-adress och inställningar för att skicka och ta emot e-post.

   Genom att göra denna inställning kan du förhindra obehöriga användare från att ändra inställningarna och avaktivera skrivaren, och därmed säkra korrekt användning av nätverket.

4. **Filadministratör**

   Hanterar åtkomst till lagrade filer. Du kan ange och radera lösenord för låsta utskriftsfiler och andra filer. Genom denna inställning kan du förhindra dataläckage och manipulering som beror på att obehöriga användare granskar och använder registrerad data.

Obs

- Administratörsautentisering kan också anges via Web Image Monitor. För mer information, se hjälpen till Web Image Monitor.
- Du kan ange autentisering av användarkod utan att ange administratörsautentisering.

Ange administratörsprivilegier

När du anger administratörsautentisering ställer du "Hantering av administratörsautentisering" på [På]. Om inställningen är aktiverad kan administratörer endast konfigurera de inställningar som tilldelats dem.

För att logga in som administratör ska du använda standardanvändarnamn och lösenord.

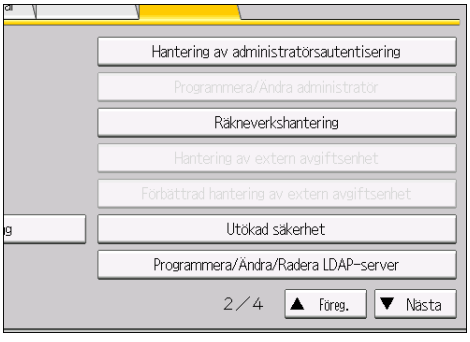
För mer information om in- och utloggning med administratörsautentisering, se s. 18 "Inloggningsmetod administratör " och s. 20 "Utloggningsmetod administratör".

Viktigt

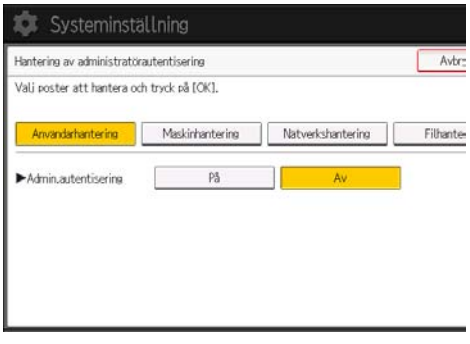
- **Om du har aktiverat "Hantering av administratörsautentisering", ska du se till att inte glömma administratörens användarnamn och lösenord för inloggning. Om du glömmer en administratörs användarnamn eller lösenord måste du ange ett nytt lösenord med hjälp av övervakarprivilegier. För mer information om övervakarprivilegier, se s. 21 "Övervakare".**

1. **Tryck på [User Tools] (Användarverktyg)**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**

4. **Tryck på [▼Nästa].**
5. **Tryck på [Hantering av administratörsautentisering].**



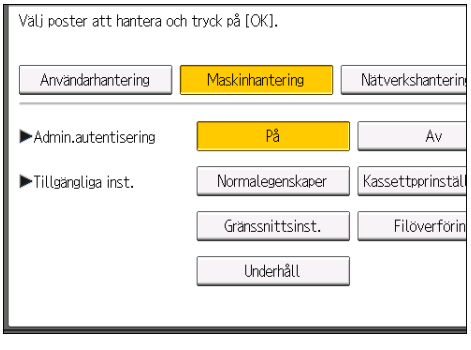
6. **Tryck på [Användarhantering], [Maskinhantering], [Nätverkshantering] eller [Filhantering] för att välja vilka inställningar som ska hanteras.**



7. **Ställ in "Admin.autentisering" på [På].**

   "Tillgängliga inst." visas.

8. **Välj de inställningar som ska hanteras i "Tillgängliga inst.".**



   De valda inställningarna är inte tillgängliga för användare.

   De tillgängliga inställningarna beror på administratörstyp.

   Upprepa steg 6-8 för att ange administratörsautentisering för mer än en kategori.

9. **Tryck på [OK].**

10. **Tryck på [User Tools] (Användarverktyg)**

Registrera och ändra administratörer

Om administratörsautentisering är angivet rekommenderar vi att en person tar varje administratörsroll.

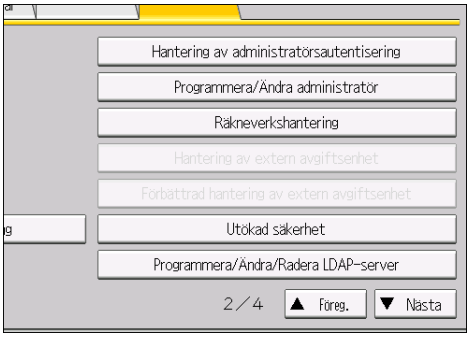
Delade administratörsuppgifter underlättar varje administratörs uppgifter och det förhindrar obehöriga administratörsfunktioner. Du kan registrera upp till 4 användarnamn (Administratör 1 till 4) till vilka olika behörigheter kan tilldelas.

En administratörs rättigheter kan endast ändras av en administratör med lämpliga rättigheter.

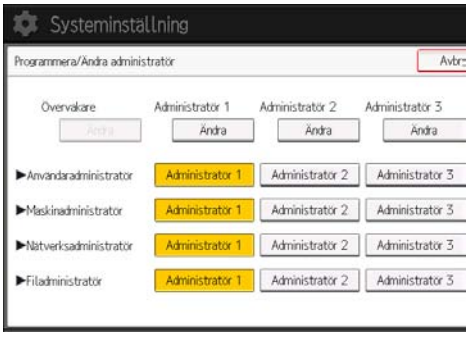
Se till att tilldela alla administratörsrättigheter så att var och en av rättigheterna är sammankopplade med åtminstone en administratör.

För mer information om in- och utloggning med administratörsautentisering, se s. 18 "Inloggningsmetod administratör " och s. 20 "Utloggningsmetod administratör".

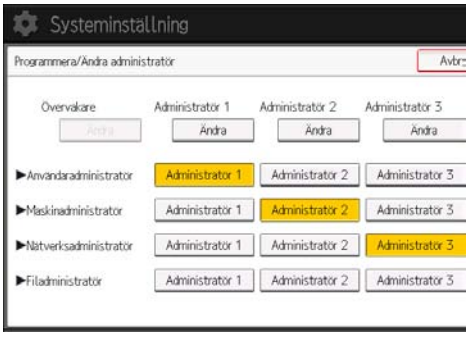
1. **Logga in som en administratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa].**
5. **Tryck på [Programmera/Ändra administratör].**



6. **I raden för den administratör vars privilegier du vill ange, tryck på [Administratör 1], [Administratör 2], [Administratör 3] eller [Administratör 4] följt av [Ändra].**



Välj en administratör för varje kategori som visas nedan när administratörers privilegier fördelas till olika personer.



För att kombinera flera administratörsprivilegier kan flera administratörsprivilegier tilldelas en enskild administratör.

För att exempelvis tilldela maskinadministratörs- och användaradministratörsprivilegier till [Administratör 1], tryck på [Administratör 1] i fälten för maskin- och användaradministratör.

7. **Tryck på [Ändra] för "Användarnamn".**
8. **Ange användarnamnet och tryck på [OK].**
9. **Tryck på [Ändra] för "Lösenord".**
10. **Ange lösenordet och tryck på [OK].**

    Följ lösenordsprincipen för att stärka lösenordet.

    För mer information om lösenordsprinciper och hur de anges, se s. 193 "Ange Utökade säkerhetsfunktioner".
11. **Ange lösenordet på nytt för att bekräfta och tryck sedan på [OK].**
12. **Tryck på [Ändra] för "Krypteringslösen".**
13. **Ange krypteringslösen och tryck på [OK].**
14. **Ange krypteringslösenordet på nytt för att bekräfta och tryck sedan på [OK].**

15. **Tryck på [OK] två gånger.**

    Du kommer att loggas ut automatiskt.

Obs

- För info om vilka tecken som kan användas för användarnamn och lösenord, se s. 16 "Tecken som kan användas för användarnamn och lösenord".

Tecken som kan användas för användarnamn och lösenord

Följande tecken kan användas för användarnamn och lösenord. Namn och lösenord är skiftlägeskänsliga.

- Versaler: A till Z (26 tecken)
- Gemener: a till z (26 tecken)
- Siffror: 0 till 9 (10 tecken)
- Symboler: (mellanrum) ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ (33 tecken)

Användarnamn

- Får inte innehålla mellanslag, kolon eller citationstecken.
- Kan inte lämnas tomt.
- Kan vara max 32 tecken långt.
- En administratörs användarnamn innehåller 8 eller färre tecken måste annat än numeriska tecken (siffror) användas. Om användarnamnet bara består av siffror måste det vara minst 9 tecken långt.

Lösenord

- Lösenordets längd för adminstratörer och övervakare får vara högst 32 tecken, och för användare högst 128 tecken.
- Det finns inga begränsningar för vilka typer av tecken som kan användas för ett lösenord. Av säkerhetsskäl rekommenderas du att skapa ett lösenord som består av versaler och gemener, siffror och symboler. Ett lösenord som består av ett stort antal tecken är mindre lätt att gissa av andra.
- I [Lösenordspolicy] i [Utökad säkerhet] kan du ange ett lösenord som består av stora eller små bokstäver (versaler och gemener), siffror och symboler samt det minsta antalet tecken som ska ingå i lösenordet. För mer information om lösenordspolicy, se s. 193 "Ange Utökade säkerhetsfunktioner".

Använda Web Image Monitor för att konfigurera administratörsautentisering

När du använder Web Image Monitor kan du logga in på maskinen och ändra administratörsinställningarna. För mer information om in- och utloggning med

administratörsautentisering, se s. 18 "Inloggningsmetod administratör " och s. 20 "Utloggningsmetod administratör".

1. **Logga in som adminstratör på Web Image Monitor.**
2. **Peka på [Enhetshantering] och klicka sedan på [Konfiguration].**
3. **Klicka på [Hantering av administratörsautentisering] eller [Programmera/Ändra administratör] under "Enhetsinställningar".**
4. **Ändra inställningarna enligt önskemål.**
5. **Logga ut.**

Obs

- Mer information om Web Image Monitor finns i Web Image Monitor-hjälpen.

1

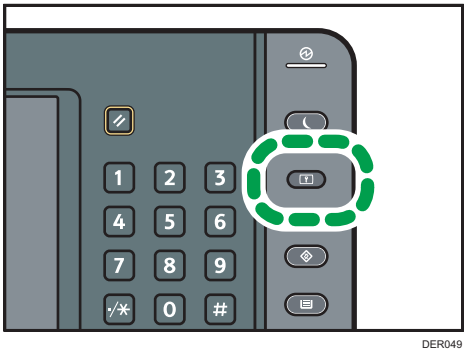
Inloggningsmetod administratör

Om administratörsautentisering är angivet ska du logga in med administratörens användarnamn och lösenord. Övervakare loggar in på samma sätt.

För mer information om administratörens och övervakarens användarnamn och lösenord, fråga administratören.

Inloggning via kontrollpanelen

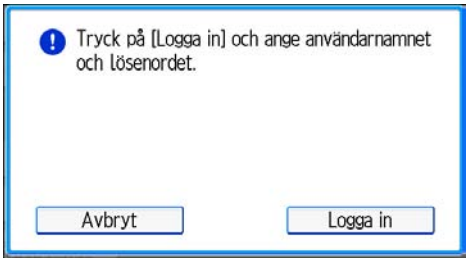
1. **Tryck på [User Tools] (Användarverktyg)**
2. **Tryck på tangenten [Logga in/Logga ut].**



Inloggningsskärmen visas.

Inloggningsskärmen visas också om du trycker på [Logga in] i menyn Användarverktyg.

3. **Tryck på [Logga in].**



4. **Ange användarnamnet och tryck på [OK].**
5. **Ange lösenordet och tryck på [OK].**

"Autentiserar. . . Vänta. " visas, följt av skärmen för initialinställningar.

Obs

- Om administratörsautentisering har angivits öppnas skärmen för autentisering. För att logga in som administratör, ange administratörens användarnamn och lösenord.

- Om du loggar in med administratörsprivilegier så visas namnet på den administratör som loggar in. När du loggar in med ett användarnamn som har flera administratörsbehörigheter visas en av de behörigheter som är tilldelade det namnet.
- Om du försöker logga in från en operativ skärmbild visas "Du har inte rättigheter att använda den här funktionen. Du kan endast ändra inställningar om du är administratör." Tryck på tangenten [Användarverktyg] för att visa skärmen för initialinställningar.

Inloggning med Web Image Monitor

1. **Öppna en webbläsare.**
2. **Ange "http://(maskinens IP-adress eller värdnamn)/" i adressfältet.**

   När du anger en IPv4-adress, börja inte segmentet med nollor. Om adressen är t.ex. "192.168.001.010", måste du skriva in den som "192.168.1.10" för att ansluta till maskinen.

   Ange IPv6-adressen med hakparentes före och efter, så här: [2001:db8::9abc].

   Du ställer in "Tillåt kommunikation via SSL/TLS" på [Endast chiffertext], skriver in "http://(maskinens IP-adress eller värdnamn)/" i webbläsaren för tillgång till maskinen.
3. **Klicka på [Logga in] längst upp till höger i fönstret.**
4. **Skriv in användarnamn och lösenord för en administratör och klicka på [Logga in].**

Obs

- Webbläsaren kan konfigureras så att den automatiskt kompletterar dialogrutorna för inloggning genom att komma ihåg användarnamn och lösenord. Den funktionen minskar säkerheten. För att förhindra att webbläsaren kommer ihåg användarnamn och lösenord kan du inaktivera funktionen Komplettera automatiskt.

Utloggningsmetod administratör

Om administratörsautentisering är angivet, se till att logga ut när inställningsändringar har slutförts. Övervakare loggar ut på samma sätt.

Utloggning via kontrollpanelen

1. **Tryck på [Logga in/Logga ut] och tryck sedan på [Ja].**

Obs

- Du kan även logga ut på följande sätt:
  - Tryck på [Energibesparing].

Utloggning med Web Image Monitor

1. **Klicka på [Logga ut] längst upp till höger i fönstret.**

Obs

- Töm cacheminnet i Web Image Monitor när du har loggat ut.

Övervakare

Övervakaren kan radera en administratörs lösenord och ange ett nytt.

Om en administratör glömmer bort eller ändrar sitt lösenord kan övervakaren tilldela ett nytt till administratören. Om du loggar in med övervakarens användarnamn och lösenord kan du inte använda de normala funktionerna eller ange systeminställningar. In- och utloggningsmetoder är desamma som för administratörer. Se s. 18 "Inloggningsmetod administratör " och s. 20 "Utloggningsmetod administratör".

Viktigt

- **Se till att inte glömma bort övervakarens användarnamn och lösenord. Om du glömmer bort dessa måste en servicerepresentant återställa maskinen till standardinställningarna. Det resulterar i att data för maskininställningar, räkneverk, loggar och andra uppgifter förloras. Servicebesöket kan eventuellt medföra extra kostnader.**

Obs

- För info om vilka tecken som kan användas för användarnamn och lösenord, se s. 16 "Tecken som kan användas för användarnamn och lösenord".
- Du kan inte specificera samma inloggningsnamn för övervakaren och administratörerna.
- Med Web Image Monitor kan du logga in som övervakare och radera en administratörs lösenord eller ange ett nytt.

Återställa administratörens lösenord

1. **Logga in som övervakare via kontrollpanelen.**

   För mer information om hur man loggar in, se s. 18 "Inloggningsmetod administratör ".
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa].**
5. **Tryck på [Programmera/Ändra administratör].**

6. **Tryck på [Ändra] för den administratör som du vill återställa.**

7. **Tryck på [Ändra] för "Lösenord".**
8. **Ange lösenordet och tryck på [OK].**
9. **Ange lösenordet på nytt för att bekräfta och tryck sedan på [OK].**
10. **Tryck på [OK] två gånger.**

    Du kommer att loggas ut automatiskt.

Obs

- Övervakaren kan ändra administratörnas lösenord, men inte deras användarnamn.

Ändra övervakare

Detta avsnitt beskriver hur man ändrar övervakarens användarnamn och lösenord.

För att göra detta måste du aktivera användaradministratörens behörighet i inställningarna under "Hantering av administratörsautentisering". För mer information, se s. 12 "Ange administratörsprivilegier".

1. **Logga in som övervakare via kontrollpanelen.**

   För mer information om hur man loggar in, se s. 18 "Inloggningsmetod administratör ".
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa].**
5. **Tryck på [Programmera/Ändra administratör].**
6. **Under "Övervakare", trycker du på [Ändra].**
7. **Tryck på [Ändra] för "Användarnamn".**
8. **Ange användarnamnet och tryck på [OK].**
9. **Tryck på [Ändra] för "Lösenord".**
10. **Ange lösenordet och tryck på [OK].**

11. **Ange lösenordet på nytt för att bekräfta och tryck sedan på [OK].**
12. **Tryck på [OK] två gånger.**

    Du kommer att loggas ut automatiskt.

2. Konfigurera användarautentisering

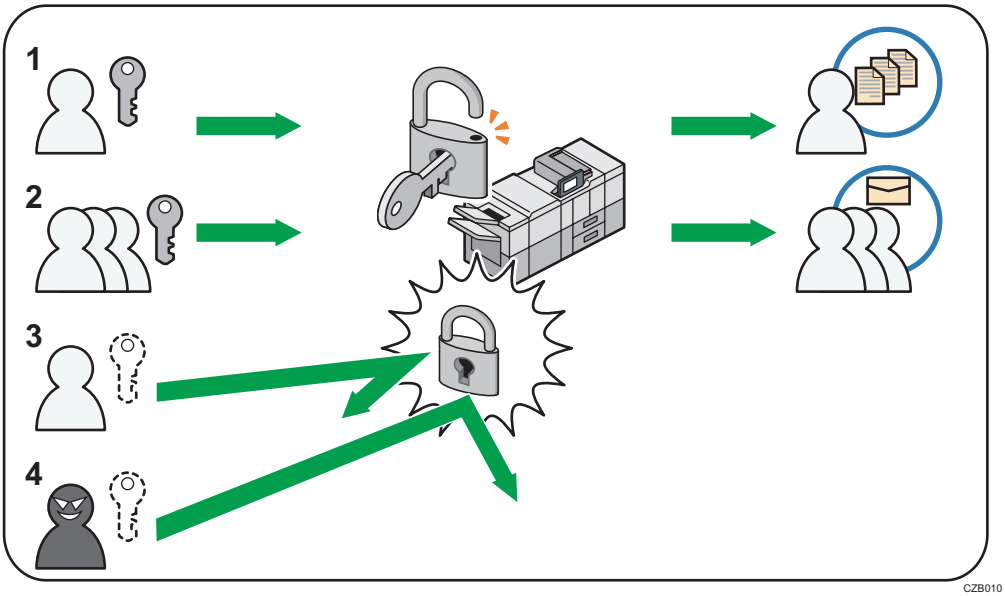
I det här kapitlet beskrivs dels hur du anger användarautentisering, dels de funktioner som aktiveras via användarautentisering.

Användare

En användare utför vanliga uppgifter med maskinen, t.ex. utskrift. Användare hanteras via informationen i maskinens adressbok och de kan endast utföra de funktioner som de får tillgång till av administratören. Genom att aktivera användarautentisering kan du ge endast personer registrerade i adressboken möjlighet att använda maskinen. Användarna kan hanteras i adressboken av användaradministratören. För mer information om administratörer, se s. 10 "Administratörer". För mer information om användarregistrering i adressboken, se Anslut maskinen/Systeminställning eller Web Image Monitors hjälp.

Om användarautentisering

Användarautentisering är ett system som kräver att användarnamn och lösenord anges för att verifiera användare som använder maskinen eller har åtkomst till maskinen över nätverket.



1. **Användare**

   En användare utför vanliga uppgifter med maskinen, t.ex. utskrift.

2. **Grupp**

   En grupp utför vanliga uppgifter med maskinen, t.ex. utskrift.

3. **Obehörig användare**

4. **Obehörig åtkomst**

Konfigurera Konfigurera användarautentisering

Det finns 4 olika autentiseringsmetoder: autentisering via användarkod, grundläggande autentisering, Windows-autentisering och LDAP-autentisering. För att använda användarautentisering ska du först välja en autentiseringsmetod på kontrollpanelen och sedan göra de inställningar som krävs för autentisering. Inställningarna beror på vilken autentiseringsmetod du väljer. Ange administratörsautentisering och ange sedan användarautentisering.

Viktigt

- **Om användarautentisering inte kan aktiveras på grund av hårddisks- eller nätverksproblem kan du få åtkomst till maskinen genom att använda administratörsautentisering och inaktivera användarautentisering. Gör så här om du har bråttom och snabbt behöver använda maskinen.**
- **Du kan inte använda mer än en autentiseringsmetod samtidigt.**

Konfigurationsflöde för användarautentisering

Konfigurationsprocess	Detaljer
Konfigurera administratörsautentisering	s. 12 "Ange administratörsprivilegier" s. 14 "Registrera och ändra administratörer"
Konfigurera användarautentisering	Ange användarautentisering. 4 typer av användarautentisering finns tillgängliga: • s. 29 "Användarkodsautentisering" • s. 31 "Grundläggande autentisering" • s. 34 "Windows-autentisering" • s. 43 "LDAP-autentisering"

Användares autentiseringsmetoder

Typ	Detaljer
Användarkodautentisering	Autentisering utförs med hjälp av åttasiffriga användarkoder. Autentisering tillämpas på varje användarkod, inte på varje användare. Du måste registrera användarkoden i maskinens adressbok i förväg.

Typ	Detaljer
Grundläggande autentisering	Autentisering utförs med hjälp av maskinens adressbok. Du måste registrera användare i maskinens adressbok i förväg. Autentisering kan tillämpas på varje användare.
Windows-autentisering	Autentisering utförs med hjälp av domänkontrollanten i Windows-servern på samma nätverk som maskinen. Autentisering kan tillämpas på varje användare.
LDAP-autentisering	Autentisering utförs med hjälp av LDAP-servern på samma nätverk som maskinen. Autentisering kan tillämpas på varje användare.

Om användarens autentiseringsmetod ändras halvvägs

- Ett användarkodskonto som inte har fler än 8 siffror och som används för autentisering av användarkod kan överföras och användas som ett användarnamn även efter att autentiseringsmetoden har ändrats från autentisering av användarkod till grundläggande autentisering, Windows-autentisering eller LDAP-autentisering. I detta fall är lösenordet tomt eftersom autentisering av användarkonto inte har något angivet lösenord.
- Om autentiseringen ändras till en extern autentiseringsmetod (Windows-autentisering eller LDAP-autentisering) kan autentisering inte aktiveras om den externa autentiseringsenheten inte har det överförda användarkodkontot registrerat sedan tidigare. Användarkodskontot kommer dock att lagras i maskinens adressbok även om autentiseringen misslyckas.
- Vid ändring från autentisering av användarkod till en annan autentiseringsmetod rekommenderar vi att du ur säkerhetssynpunkt raderar konton som du inte använder eller anger ett lösenord. För mer information om borttagning av konton, se Anslut maskinen/ Systeminställning. För mer information om hur du ändrar lösenord, se s. 33 "Ange användarnamn och lösenord.".

Obs

- Efter att huvudströmmen har slagits på visas eventuellt inte utökade funktioner i listan över poster för användarautentisering i menyn Hantering av användarautentisering. Vänta en stund om detta inträffar, och öppna sedan menyn Hantering av användarautentisering igen.
- Användarautentisering kan även anges via Web Image Monitor. För mer information, se hjälpen till Web Image Monitor.

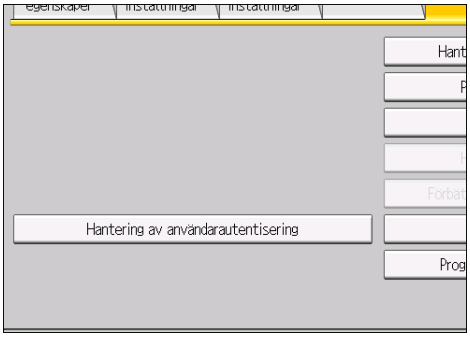
Användarkodsautentisering

Detta är en autentiseringsmetod för att begränsa åtkomst till funktioner enligt en användarkod. Samma användarkod kan användas av flera användare.

För mer information om hur man anger användarkoder, se handboken Anslut maskinen/ Systeminställningar.

För mer information om hur man anger användarkod i skrivardrivrutinen, se drivrutinens hjälp.

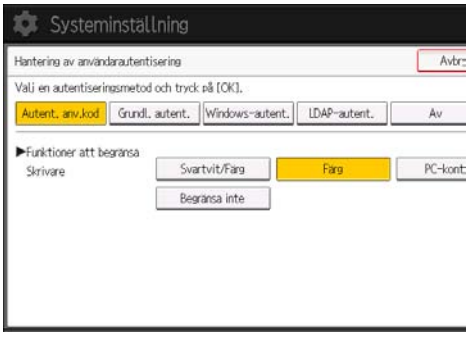
1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa].**
5. **Tryck på [Hantering av användarautentisering].**



6. **Välj [Autent. anv.kod].**

   Om du inte vill aktivera användarautentisering väljer du [Av].

7. **I "Funktioner att begränsa" väljer du de funktioner som ska begränsas.**



   De valda funktionerna omfattas av användarkodautentisering. Användarkodautentisering tillämpas inte på de funktioner som inte valts.

   För mer information om hur man begränsar tillgängliga funktioner för användare och grupper, se s. 59 "Begränsa Tillgängliga funktioner".

8. **För att ange jobbautentisering för skrivaren ska du välja en annan post än [PC-kontroll] för "Skrivare" under "Funktioner att begränsa".**

   Om objekten inte visas, tryck på tangenten [▼Nästa].

   Om du inte vill ange utskriftsautentisering går du vidare till steg 14.

9. **Tryck på [▼Nästa].**

10. **Välj nivå för "Utskriftsjobbsautent.".**

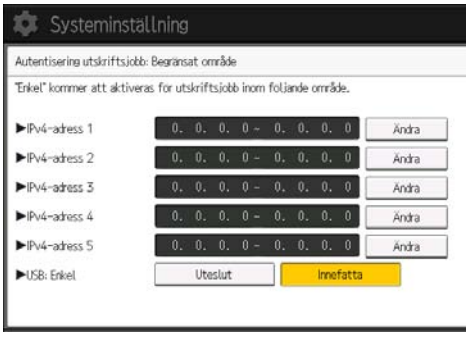
    För en beskrivning av autentiseringsnivåer för utskriftsjobb, se s. 48 "Autentisering av utskriftsjobb".

    Om du väljer [Hela] eller [Enkel (Alla)] så fortsätter du till steg 14.

    Om du väljer [Enkel (Begränsning)] så fortsätter du till steg 11.

11. **Tryck på [Ändra] vid "Begränsat område".**

12. **Ange inom vilket intervall [Enkel (Begränsning)] ska tillämpas för "Utskriftsjobbsautent.".**



    Du kan ange ett intervall av IPv4-adresser som denna inställning ska gälla för.

13. **Tryck på [Avsluta].**

14. **Tryck på [OK].**

15. **Tryck på tangenten [Logga in/Logga ut].**

    Ett bekräftelsemeddelande visas. Om du trycker på [Ja] loggas du automatiskt ut.

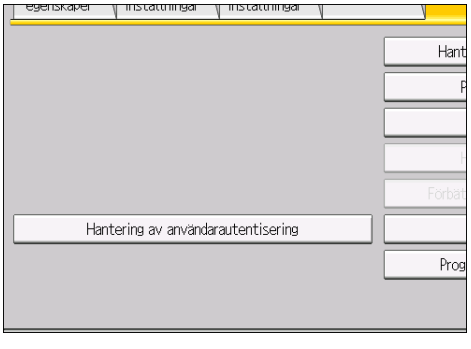
Grundläggande autentisering

Ange denna autentiseringsmetod när du använder maskinens adressbok för att autentisera varje användare. Med grundläggande autentisering kan du både hantera maskinens tillgängliga inställningar samt begränsa åtkomst till lagrade filer och adressboken. Under grundläggande autentisering måste administratören ange de funktioner som är tillgängliga för varje registrerad användare i adressboken. För mer information om hur du begränsar funktioner, se s. 32 "Autentiseringsinformation lagrad i adressboken".

Ange grundläggande autentisering

Innan du konfigurerar maskinen ska du kontrollera att administratörsautentiseringen är korrekt konfigurerad under "Hantering av administratörsautentisering".

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa].**
5. **Tryck på [Hantering av användarautentisering].**



6. **Välj [Grundl. autent.].**

   Om du inte vill aktivera användarautentisering väljer du [Av].

7. **I "Tillgängliga funktioner" väljer du vilka maskinfunktioner du vill tillåta.**

   De funktioner du väljer här blir standardinställningarna för basautentisering som tilldelas till alla nya användare av adressboken.

   För mer information om hur man anger tillgängliga funktioner för användare eller grupper, se s. 59 "Begränsa Tillgängliga funktioner".

8. **Tryck på [▼Nästa].**

9. **Välj nivå för "Utskriftsjobbsautent.".**

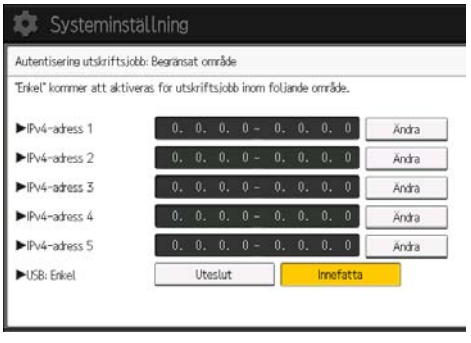
   För en beskrivning av autentiseringsnivåer för utskriftsjobb, se s. 48 "Autentisering av utskriftsjobb".

   Om du väljer [Hela] eller [Enkel (hela)] så fortsätter du till steg 13.

   Om du väljer [Enkel (begränsning)] så fortsätter du till steg 10.

10. **Tryck på [Ändra] vid "Begränsat område".**

11. **Ange inom vilket intervall [Enkel (Begränsning)] ska tillämpas för "Utskriftsjobbsautent.".**



   Du kan ange ett intervall av IPv4-adresser som denna inställning ska gälla för.

12. **Tryck på [Avsluta].**

13. **Tryck på [OK].**

14. **Tryck på tangenten [Logga in/Logga ut].**

    Ett bekräftelsemeddelande visas. Om du trycker på [Ja] loggas du automatiskt ut.

Autentiseringsinformation lagrad i adressboken

Om du har aktiverat användarautentisering kan du ange åtkomstgränser och användningsgränsen för maskinens funktioner för varje användare eller grupp av användare. Ange de inställningar som krävs i Adressboken för varje användare. För mer information om funktionerna som kan begränsas, se s. 59 "Begränsa Tillgängliga funktioner".

Användare måste ha ett registrerat konto i adressboken för att kunna använda maskinen när användarautentisering har angivits. För mer information om användarregistrering i adressboken, se handboken Anslut maskinen/Systeminställningar.

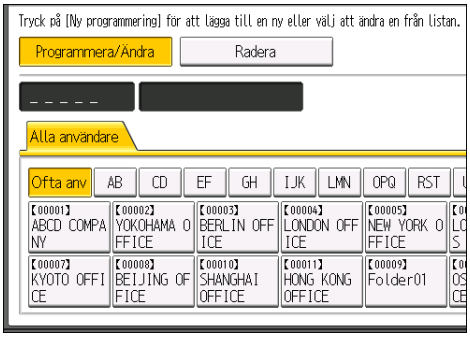
Användarautentisering kan även anges via Web Image Monitor. För mer information, se hjälpen till Web Image Monitor.

Ange användarnamn och lösenord.

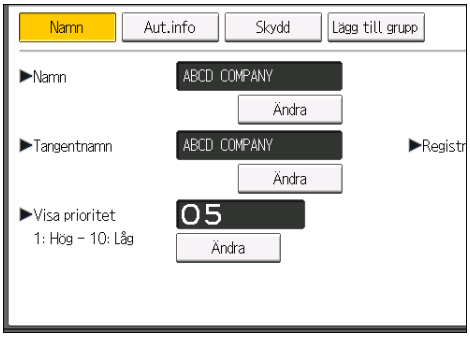
I "Hantera adressboken" anger du det användarnamn och lösenord som ska användas för "Hantering av användarautentisering".

För info om vilka tecken som kan användas för användarnamn och lösenord, se s. 16 "Tecken som kan användas för användarnamn och lösenord".

1. **Logga in som användaradministratör via kontrollpanelen.**
2. **Tryck på [Hantera adressboken].**
3. **Välj användare.**



4. **Tryck på [Aut.info].**



5. **Tryck på [Ändra] för "Användarnamn".**
6. **Ange ett användarnamn för inloggning och tryck sedan på [OK].**
7. **Tryck på [Ändra] för "Lösenord".**
8. **Ange ett lösenord och tryck sedan på [OK].**
9. **Ange lösenordet på nytt för att bekräfta och tryck på [OK].**
10. **Tryck på [OK].**
11. **Tryck på [Avsluta].**
12. **Logga ut.**

Windows-autentisering

Ange den här autentiseringstypen när du använder Windows domänkontrollant för att autentisera användare som har sina konton på katalogservern. Användare kan inte autentiseras om de inte har konton på katalogservern. Med Windows-autentisering kan du ange åtkomstbegränsning för varje grupp som finns registrerad på katalogservern. Adressboken som är lagrad på katalogservern kan registreras på maskinen så att du kan autentisera användare utan att först använda maskinen till att registrera enskilda inställningar i adressboken.

Första gången du får tillgång till maskinen kan du använda de funktioner som finns tillgängliga för din grupp. Om du inte har registrerats i en grupp, kan du använda de funktioner som finns tillgängliga under "*Standardgrupp". För att begränsa funktioner som endast är tillgängliga för vissa användare ska du först göra inställningar i adressboken.

För att automatiskt registrera användarinformation under Windows-autentisering rekommenderas att kommunikationen mellan maskinen och domänövervakaren krypteras med SSL. För att göra det måste du skapa ett servercertifikat för domänkontrollanten. För mer information om hur du skapar ett servercertifikat, se s. 41 "Skapa servercertifikat.".

Viktigt

- **Om du använder Windows-autentisering registreras användarinformationen som finns registrerad i katalogservern automatiskt i maskinens adressbok. Även om användarinformationen som registreras automatiskt i maskinens adressbok redigeras i maskinen, så skrivs den över av informationen från katalogservern när autentiseringen utförs.**
- **Användare som hanteras i andra domäner kan autentiseras men de kan inte erhålla poster som användarnamn.**
- **Om du skapade en ny användare i domänkontrollanten och vid lösenordskonfigurationen valde "Användare måste byta lösenord vid nästa inloggning" ska du först logga in på datorn och sedan ändra lösenordet.**
- **Om den autentiserande servern bara stöder NTLM när Kerberos-autentisering har valts på maskinen, kommer autentiseringsmetoden att automatiskt skifta till NTLM.**
- **Användarnamnet för inloggning är skiftlägeskänsligt när Windows-autentisering används. Ett felaktigt angivet användarnamn kommer att läggas till i adressboken. Ta bort den tillagda användaren om detta sker.**
- **Om gästkontot på Windows-servern är aktiverat kan även användare som inte är registrerade i domänkontrollanten bli autentiserade. När detta konto är aktiverat, registreras användare i adressboken som kan använda de tillgängliga funktionerna under "*Standardgrupp".**

Windows-autentisering kan utföras med en av två autentiseringsmetoder: NTLM- eller Kerberos-autentisering. Användarkraven för båda metoderna listas nedan:

Driftskrav för NTLM-autentisering

För att ange NTLM-autentisering ska följande krav uppfyllas:

- Den här maskinen har stöd för NTLMv1-autentisering och NTLMv2-autentisering.
- Upprätta en domänkontrollant för den domän som du vill använda.
- Funktionen stöds av de operativsystem som listas nedan. Använd LDAP för att erhålla användarinformation när Active Directory körs. Om du använder LDAP rekommenderar vi att ni använder SSL för att kryptera kommunikation mellan maskinen och LDAP-servern. SSL-kryptering är bara möjligt om LDAP-servern har stöd för TLSv1 eller SSLv3.
  - Windows Server 2003/2003 R2
  - Windows Server 2008/2008 R2
  - Windows Server 2012/2012 R2

Driftskrav för Kerberos-autentisering

För att ange Kerberos-autentisering ska följande krav uppfyllas:

- Upprätta en domänkontrollant för den domän som du vill använda.
- Operativsystemet måste stödja KDC (Key Distribution Center). Använd LDAP för att erhålla användarinformation när Active Directory körs. Om du använder LDAP rekommenderar vi att ni använder SSL för att kryptera kommunikation mellan maskinen och LDAP-servern. SSL-kryptering är bara möjligt om LDAP-servern har stöd för TLSv1 eller SSLv3. Kompatibla operativsystem återfinns nedan:
  - Windows Server 2003/2003 R2
  - Windows Server 2008/2008 R2
  - Windows Server 2012/2012 R2

  För att använda Kerberos-autentisering under Windows Server 2008 måste Service Pack 2 eller senare installeras.
- Överföring av data mellan maskinen och KDC-servern är krypterad om Kerberos-autentisering är aktiverad. Information om hur du anger krypterad överföring finns i s. 135 "Krypteringsinställningar för Kerberos-autentisering".

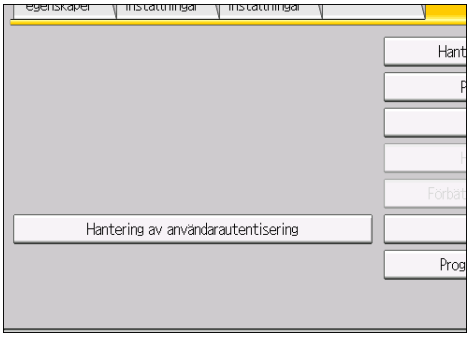
Obs

- För info om vilka tecken som kan användas för användarnamn och lösenord, se s. 16 "Tecken som kan användas för användarnamn och lösenord".
- När du sedan använder skrivaren kan du använda alla funktioner som är tillgängliga för din grupp och för dig som individuell användare.
- Användare som är registrerade i flera grupper kan använda alla funktioner som finns tillgängliga för dessa grupper.
- Med Windows-autentisering behöver du inte skapa ett servercertifikat om du inte vill att användarinformation som användarnamn ska registreras automatiskt med SSL.

Ange Windows-autentisering

Innan du konfigurerar maskinen ska du kontrollera att administratörsautentiseringen är korrekt konfigurerad under "Hantering av administratörsautentisering".

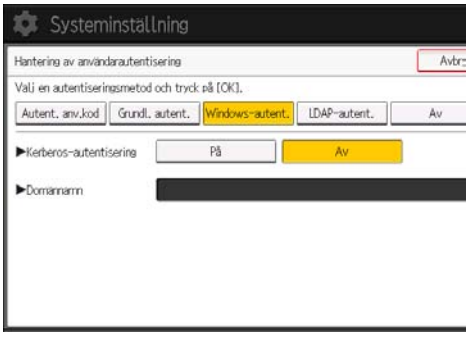
1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa].**
5. **Tryck på [Hantering av användarautentisering].**



6. **Välj [Windows-autent.].**

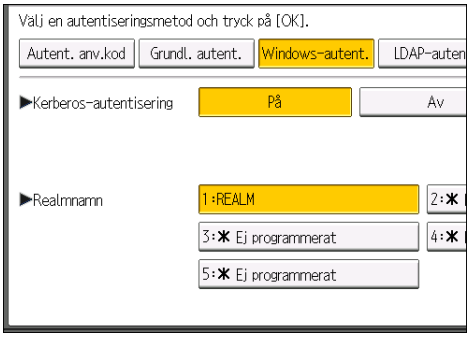
   Om du inte vill aktivera användarautentisering väljer du [Av].

7. **Om du vill använda Kerberos-autentisering, tryck på [På].**



   Om du vill använda NTLM-autentisering, tryck på [Av] och fortsätt till steg 9.

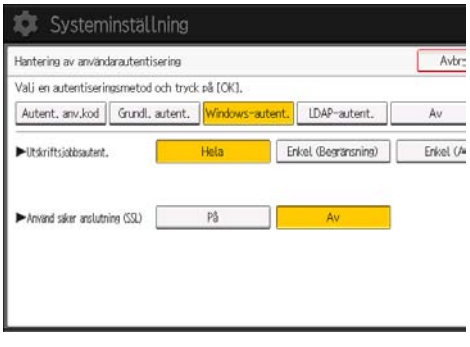
8. **Välj realmen för Kerberos-autentisering och fortsätt till steg 10.**



För att aktivera Kerberos-autentisering måste en realm först registreras. Ett realmnamn måste registreras med versaler. För mer information om hur du registrerar en realm, se Anslut maskinen/ Systeminställningar.

Upp till 5 realmer kan registreras

9. **Tryck på [Ändra] för "Domännamn", skriv in namnet på domänövervakaren som ska autentiseras och tryck sedan på [OK].**
10. **Tryck på [▼Nästa].**
11. **Välj nivån "Utskriftsjobbsautent.".**

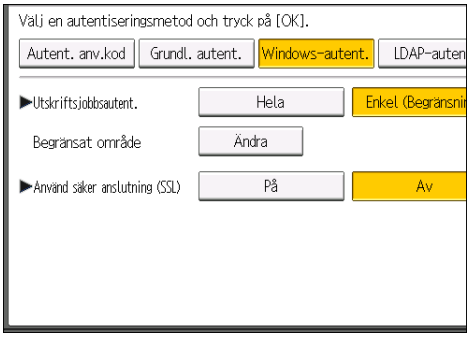


För en beskrivning av autentiseringsnivåerna för utskriftsjobb, se s. 48 "Autentisering av utskriftsjobb".

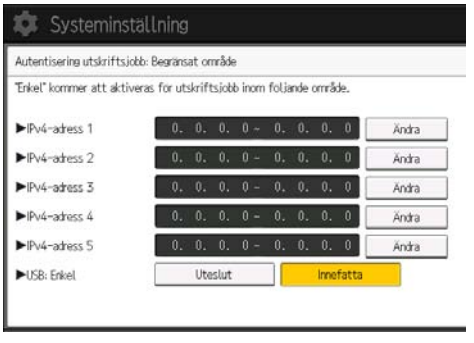
Om du väljer [Hela] eller [Enkel (hela)] så fortsätter du till steg 15.

Om du väljer [Enkel (begränsning)] så fortsätter du till steg 12.

12. **Tryck på [Ändra].**



13. **Ange inom vilket intervall [Enkel (Begränsning)] ska tillämpas för "Utskriftsjobbsautent.".**



Du kan ange ett intervall av IPv4-adresser som denna inställning ska gälla för.

14. **Tryck på [Avsluta].**

15. **Tryck på [På] för "Använd säker anslutning (SSL)".**

Om du inte använder SSL för autentisering, tryck på [Av].

Om du inte har registrerat en global grupp fortsätter du till steg 22.

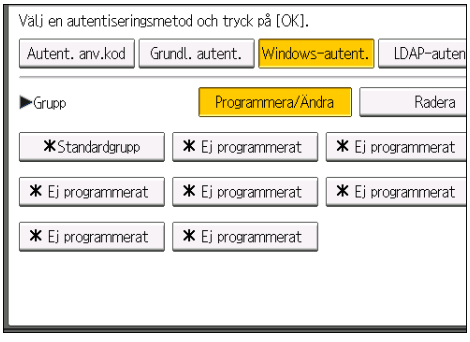
Om du har registrerat en global grupp fortsätter du till steg 16.

Om globala grupper har registrerats i Windows-servern kan du begränsa användningen av funktionerna för varje global grupp.

Du måste skapa globala grupper i Windows-servern i förväg och registrera användarna som ska autentiseras i respektive grupp. Du måste även registrera de tillgängliga funktionerna för globala gruppmedlemmar i maskinen. Skapa globala grupper på maskinen genom att föra in namnen på de globala grupperna som registrerats på Windowsservern. (Tänk på att gruppnamn är skiftlägeskänsliga.) Ange sedan vilka maskinfunktioner som ska vara tillgängliga för varje grupp.

Om globala grupper inte har angivits kan användare använda de funktioner som har angivits i [*Standardgrupp]. Om globala grupper har angivits kan användare som inte registrerats i en global grupp använda de funktioner som har angivits i [*Standardgrupp]. Med standardinställningen är alla funktioner tillgängliga för medlemmar av *Standardgrupp. Specificera begränsningarna för de tillgängliga funktionerna efter användarnas behov.

16. **Tryck på [▼Nästa].**
17. **Under "Grupp" trycker du på [Programmera/Ändra] och sedan på [* Ej programmerat].**



18. **Tryck på [Ändra] för "Gruppnamn" och ange sedan gruppnamnet.**
19. **Tryck på [OK].**
20. **I "Tillgängliga funktioner" väljer du vilka maskinfunktioner du vill tillåta.**

    Windows-autentisering tillämpas på de valda funktionerna.

    Användare kan endast använda de valda funktionerna.

    För mer information om hur man anger tillgängliga funktioner för användare eller grupper, se s. 59 "Begränsa Tillgängliga funktioner".
21. **Tryck på [OK].**
22. **Tryck på [OK].**
23. **Tryck på tangenten [Logga in/Logga ut].**

    Ett bekräftelsemeddelande visas. Om du trycker på [Ja] loggas du automatiskt ut.

Installera Internet Information Services (IIS) och Certificate Services

Ange denna inställning om du vill att maskinen automatiskt ska ta emot användarinformation som registrerats i Active Directory.

Vi rekommenderar att du installerar IIS (Internet Information Services) och Certificate Services som Windows-komponenter.

Installera komponenterna och skapa servercertifikatet.

Om de inte har installerats ska du installera dem så här.

Installation under Windows Server 2008 R2

1. **På [Start]-menyn pekar du på [Administrationsverktyg] och klicka sedan på [Serverhanteraren].**

2. **Klicka på [Roller] i den vänstra kolumnen, klicka på [Lägg till roller] från [Åtgärd]-menyn.**
3. **Klicka på [Nästa >].**
4. **Markera kryssrutorna "Web Server (IIS)" och "Active Directory Certificate Services" och klicka sedan på [Nästa>].**

   Om ett bekräftelsemeddelande visas, klicka på [Lägg till funktioner].
5. **Läs innehållet och klicka sedan på [Nästa >].**
6. **Kontrollera att [Certifikatutfärdare] är vald och klicka sedan på [Nästa >].**
7. **Välj [Företag] och klicka sedan på [Nästa >].**
8. **Välj [Rot CA] och klicka sedan på [Nästa >].**
9. **Välj [Skapa en ny privat nyckel] och klicka sedan på [Nästa >].**
10. **Välj en kryptografileverantör, nyckellängd och hashalgoritm för att skapa en ny privat nyckel och klicka sedan på [Nästa >].**
11. **I "Namn för denna CA:", anger du certifikatutfärdarens namn och klickar på [Nästa>].**
12. **Välj giltigthetsperiod och klicka på [Nästa >].**
13. **Ställ in standardinställningarna för "Plats för certifikatdatabas:" och "Plats för certifikatdatabaslogg:" och klicka sedan på [Nästa >].**
14. **Kontrollera platsen och klicka sedan på [Nästa >].**
15. **Välj den roll du vill använda och klicka sedan på [Nästa >].**
16. **Klicka på [Installera].**
17. **När installationen är färdig trycker du på [Stäng].**
18. **Stäng [Server Manager].**

Installation under Windows Server 2012

1. **Klicka på [Serverhanteraren] på startskärmen.**
2. **I menyn [Hantera] klickar du på [Lägg till roller och funktioner].**
3. **Klicka på [Nästa >].**
4. **Välj [Rollbaserad eller funktionsbaserad installation] och klicka sedan på [Nästa>].**
5. **Välj en server och klicka sedan på [Nästa>].**
6. **Markera kryssrutorna "Active Directory Certificate Services" och "Web Server (IIS)" och klicka sedan på [Nästa>].**

   Om ett bekräftelsemeddelande visas, klicka på [Lägg till funktioner].
7. **Markera de funktioner du vill installera och klicka sedan på [Nästa>].**
8. **Läs innehållet och klicka sedan på [Nästa >].**

9. **Se till att [Certifikatutfärdare] är markerat i området [Rolltjänster] i [Active Directory-certifikattjänster] och klicka sedan på [Nästa>].**
10. **Läs innehållet och klicka sedan på [Nästa >].**
11. **Markera de rolltjänster som du vill installera under [Webbserver (IIS)] och klicka sedan på [Nästa>].**
12. **Klicka på [Installera].**
13. **När du har slutfört installationen ska du klicka på Serverhanterarens meddelandeikon och sedan klicka på [Konfigurera Active Directory-certifikattjänster på målservern].**
14. **Klicka på [Nästa >].**
15. **Klicka på [Certifikatutfärdare] i området [Rolltjänster] och klicka sedan på [Nästa>].**
16. **Välj [Företag CA] och klicka sedan på [Nästa>].**
17. **Välj [Rot CA] och klicka sedan på [Nästa >].**
18. **Välj [Skapa en ny privat nyckel] och klicka sedan på [Nästa >].**
19. **Välj en kryptografileverantör, nyckellängd och hashalgoritm för att skapa en ny privat nyckel och klicka sedan på [Nästa>].**
20. **I "Namn för denna CA:", anger du certifikatutfärdarens namn och klickar på [Nästa>].**
21. **Välj giltigthetsperiod och klicka på [Nästa >].**
22. **Ställ in standardinställningarna för "Plats för certifikatdatabas:" och "Plats för certifikatdatabaslogg:" och klicka sedan på [Nästa >].**
23. **Klicka på [Konfigurera].**
24. **Om meddelandet "Konfiguration slutförd" visas, klicka på [Stäng].**

Skapa servercertifikat.

När du har installerat IIS, certifikatservice och Windows-komponenter skapar du servercertifikatet så här:

Windows Server 2008 R2 används för att visa processen.

1. **På [Start]-menyn pekar du på [Administrationsverktyg] och klicka sedan på [IIS-hanteraren (Internet Information Services)].**

   Klicka på [IIS-hanteraren (Internet Information Services)] på startskärmen under Windows Server 2012.

   När bekräftelsemeddelandet visas klickar du på [Ja].
2. **I den vänstra kolumnen klickar du på servernamnet och dubbelklickar sedan på [Servercertifikat].**
3. **I den högra kolumnen klickar du på [Skapa certifikatansökan...].**

4. Ange all information som krävs, och klicka sedan på [Nästa].
5. I "Kryptografileverantör:", väljer du en leverantör och klickar på [Nästa].
6. Klicka på [...] och ange sedan ett filnamn för certifikatansökan.
7. Ange en plats där filen ska lagras och klicka sedan på [Öppna].
8. Stäng [Internet Information Services (IIS) Manager] genom att klicka på [Slutför].

LDAP-autentisering

Ange den här autentiseringsmetoden när du använder LDAP-servern för att autentisera användare som har sina konton på LDAP-servern. Användare kan inte autentiseras om de inte har sina konton på LDAP-servern. Adressboken som finns lagrad på LDAP-servern kan registreras på maskinen, så att man kan autentisera användare utan att först använda maskinen för att registrera individuella inställningar i adressboken. När LDAP-autentisering används rekommenderas att man använder SSL för att kryptera kommunikationen mellan maskinen och LDAP-servern, för att på så sätt förhindra att lösenordsinformationen skickas okrypterad över nätverket. Du kan ange på LDAP-servern om du vill eller inte vill aktivera SSL. För att göra det måste du skapa ett servercertfikat för LDAP-servern. För mer information om hur du skapar ett servercertifikat, se s. 41 "Skapa servercertifikat.". SSL-inställningar kan anges i LDAP-serverinställningarna.

Genom att använda Web Image Monitor kan du aktivera en funktion som kontrollerar att SSL-servern är betrodd. För mer om hur du ställer in LDAP-autentisering med Web Image Monitor, se hjälp för Web Image Monitor.

När du väljer okrypterad autentisering aktiveras förenklad LDAP-autentisering. Förenklad autentisering kan utföras med ett användarattribut (som t.ex. cn eller uid) i stället för DN.

För att aktivera Kerberos för LDAP-autentisering måste en realm först registreras. En realm måste konfigureras med versaler. För mer information om hur du registrerar en realm, se Anslut maskinen/ Systeminställningar.

Viktigt

- **Om du använder LDAP-autentisering registreras användarinformationen som finns registrerad i LDAP-servern automatiskt i maskinens adressbok. Även om användarinformationen som registreras automatiskt i maskinens adressbok redigeras i maskinen, så skrivs den över av informationen från LDAP-servern när autentiseringen utförs.**
- **Vid LDAP-autentisering kan du inte ange åtkomstbegränsning för grupper som har registrerats i katalogservern.**
- **Undvik dubbelbytetecken som japanska, kinesiska (traditionella och förenklade) och hangultecken vid inloggning eller som lösenord. Om du använder dubbelbytetecken kan du inte autentisera med Web Image Monitor.**
- **Om du använder Active Directory i LDAP-autentisering när Kerberos-autentisering och SSL är inställda samtidigt, kan inte användarinformation erhållas.**
- **Om "Anonym autentisering" i inställningarna för LDAP-servern under LDAP-autentisering inte är inställd på Förbjud, kan användare som inte har ett LDAP-serverkonto få åtkomst till servern.**
- **Om LDAP-servern är konfigurerad med Windows Active Directory kan det hända att "Anonym autentisering" är tillgänglig. Om Windows-autentisering är tillgängligt rekommenderar vi att du använder den.**

Driftskrav för LDAP-autentisering

För att ange LDAP-autentisering ska följande krav uppfyllas:

- Konfigurera nätverket så att maskinen kan upptäcka LDAP-servern.
- När SSL används kan TLSv1 eller SSLv3 köras på LDAP-servern.
- Registrera LDAP-servern till maskinen.
- För att registrera LDAP-servern anger du följande inställningar:
  - Servernamn
  - Sökbas
  - Portnummer
  - SSL-kommunikation
  - Autentisering

    Välj antingen Kerberos, DIGEST eller okrypterad autentisering (klartext).
  - Användarnamn

    Du behöver inte ange användarnamn om LDAP-servern stöder "Anonym autentisering".
  - Lösenord

    Du behöver inte ange lösenord om LDAP-servern stöder "Anonym autentisering".

För mer information om hur du registrerar en LDAP-server, se Anslut maskinen/Systeminställningar.

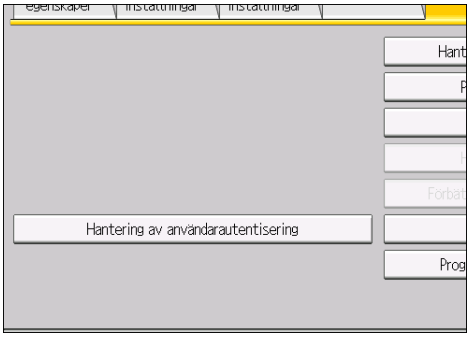
Obs

- För info om vilka tecken som kan användas för användarnamn och lösenord, se s. 16 "Tecken som kan användas för användarnamn och lösenord".
- I enkelt LDAP-autentiseringsläge misslyckas autentiseringen om lösenordet är tomt. För att använda tomma lösenord, kontakta din servicerepresentant.
- Första gången som en oregistrerad användare får åtkomst till maskinen efter att LDAP-autentisering har angivits registreras denna användare på maskinen och får åtkomst till de funktioner som finns under "Tillgängliga funktioner" under LDAP-autentisering. Om du vill begränsa tillgängliga funktioner för olika användare kan du registrera varje användare och motsvarande inställning för "Tillgängliga funktioner" i adressboken eller ange "Tillgängliga funktioner" för varje registrerad användare. Inställningen "Tillgängliga funktioner" aktiveras så snart användaren loggar in på maskinen.
- Överföring av data mellan maskinen och KDC-servern är krypterad om Kerberos-autentisering är aktiverad. Information om hur du anger krypterad överföring finns i s. 135 "Krypteringsinställningar för Kerberos-autentisering".

Innan du konfigurerar maskinen ska du kontrollera att administratörsautentiseringen är korrekt konfigurerad under "Hantering av administratörsautentisering".

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**

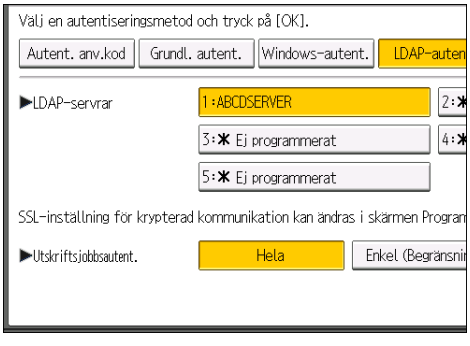
4. **Tryck på [▼Nästa].**
5. **Tryck på [Hantering av användarautentisering].**



6. **Välj [LDAP-autent.].**

   Om du inte vill aktivera användarautentisering väljer du [Av].

7. **Välj LDAP-servern som ska användas för LDAP-autentisering.**



8. **Välj nivån "Utskriftsjobbsautent.".**

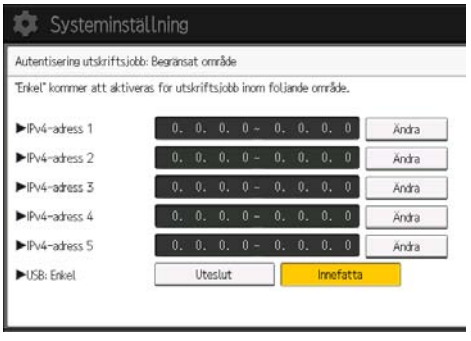
   För en beskrivning av autentiseringsnivåer för utskriftsjobb, se s. 48 "Autentisering av utskriftsjobb".

   Om du väljer [Hela] eller [Enkel (hela)] så fortsätter du till steg 12.

   Om du väljer [Enkel (begränsning)] så fortsätter du till steg 9.

9. **Tryck på [Ändra] vid "Begränsat område".**

10. **Ange inom vilket intervall [Enkel (Begränsning)] ska tillämpas för "Utskriftsjobbsautent.".**



Du kan ange ett intervall av IPv4-adresser som denna inställning ska gälla för.

11. **Tryck på [Avsluta].**
12. **Tryck på [▼Nästa].**
13. **I "Tillgängliga funktioner" väljer du vilka maskinfunktioner du vill tillåta.**

    LDAP-autentisering tillämpas på de valda funktionerna.

    Användare kan endast använda de valda funktionerna.

    För mer information om hur man anger tillgängliga funktioner för användare eller grupper, se s. 59 "Begränsa Tillgängliga funktioner".
14. **Tryck på [▼Nästa].**
15. **Tryck på [Ändra] för "Attr. f. inloggningsnamn".**
16. **Ange användarnamnets attribut och tryck sedan på [OK].**

    Använd inloggningsnamnattributet som ett sökvillkor för att få information om en autentiserad användare. Du kan skapa ett sökfilter baserat på attribut för inloggningsnamn, välja en användare och sedan hämta användarinformationen från LDAP-servern så att den överförs till maskinens adressbok.

    För att ange flera inloggningsattribut, sätt ett komma (,) mellan dem. Sökningen visar träffar för ett eller båda attributen.

    Om du placerar ett likhetstecken (=) mellan två inloggningsattribut (t.ex. cn=abcde, uid=xyz) ger sökningen bara träffar som matchar attributen. Denna sökfunktion kan även tillämpas när okrypterad autentisering anges.

    Vid autentisering med DN-format, behöver inte inloggningsattribut registreras.

    Metoden för hur du väljer användarnamn beror på servermiljön. Kolla upp servermiljön och ange sedan användarnamnet på rätt sätt.
17. **Tryck på [Ändra] för "Unikt attribut".**

18. **Ange unikt attribut och tryck sedan på [OK].**

    Ange unikt attribut på maskinen om du vill matcha användarinformationen i LDAP-servern med den i maskinen. Om det unika attributet för en användare registrerad i LDAP-servern matchar det för en användare registrerad i maskinen, betraktas de två attributen som samma användare.

    Du kan ange ett attribut som "serienummer" eller "uid". Dessutom kan du ange "cn" eller "anställnNummer", förutsatt att det är unikt. Om du inte anger det unika attributet, skapas ett konto med samma användarinformation men med ett annat användarnamn för inloggning på maskinen.

19. **Tryck på [OK].**

20. **Tryck på tangenten [Logga in/Logga ut].**

    Ett bekräftelsemeddelande visas. Om du trycker på [Ja] loggas du automatiskt ut.

Autentisering av utskriftsjobb

Autentisering av utskriftsjobb är en funktion för tillämpning av användarautentisering för utskriftsjobb.

Både PCL- och PostScript3-drivrutiner stöder användarautentisering. Drivrutinen PostScript3 stöder endast autentisering av användarkod.

Autentiseringsnivåer för utskriftsjobb

Säkerhetsnivån för "Hela" är den högsta, följt av "Enkel (Begränsning)" och lägst "Enkel (Alla)".

- Hela

  Välj denna för att autentisera alla utskriftsjobb samt fjärrinställningar.

  Maskinen autentiserar alla utskriftsjobb och fjärrinställningar och avbryter jobb och inställningar som inte kan autentiseras.

  För att skriva ut i en miljö som inte stödjer autentiseringen, välj [Enkel (alla)] eller [Enkel (begränsning)].

- Enkel (begränsning)

  Välj detta för att begränsa intervallet för [Enkel (alla)].

  Det angivna intervallet kan skrivas ut oberoende av autentisering. Autentisering kommer att tillämpas för adresser utanför detta intervall.

  Du kan ange om du vill tillämpa [Enkel (Alla)] för användarens IPv4-adress. Programintervallet för IPv6-adresser kan konfigureras från Web Image Monitor.

- Enkel (alla)

  Välj denna inställning om du vill skriva ut med en skrivardrivrutin eller enhet som inte kan identifieras av maskinen, eller om autentisering inte behövs för utskrifter.

  Utskriftsjobb och inställningar utan autentiseringsinformation utförs utan att de autentiseras.

  Maskinen autentiserar utskriftsjobb och fjärrinställningar som har autentiseringsinformation och avbryter jobb och inställningar som inte kan autentiseras.

  Obehöriga användare kan eventuellt använda maskinen eftersom utskrift är tillåten utan användarautentisering.

Typer av utskriftsjobb

Beroende på kombinationen av nivån av autentisering av utskriftsjobb och typ av utskriftsjobb, kan det hända att skrivaren inte fungerar riktigt. Ställ in en lämplig kombination för den miljö du arbetar i.

När användarautentisering har inaktiverats kan alla jobbtyper skrivas ut.

Jobbtyper: Ett utskriftsjobb anges när:

1. [Användarautentisering] är markerad i PCL-skrivardrivrutinen eller i PCL universell drivrutin.
2. [Användarautentisering] och [Med kryptering] är markerade i PCL-mini-drivrutinen*.
   * Autentiseringsfunktionen kan inte användas med IA-64-operativsystem.
3. [Användarautentisering] är markerad i PCL-mini-drivrutinen.
4. [Användarautentisering] är inte markerad i PCL-skrivardrivrutinen eller i PCL-mini-drivrutinen*.
   * Autentiseringsfunktionen kan inte användas med IA-64-operativsystem.
5. Användarkoden anges med hjälp av PostScript3-skrivardrivrutin eller PS3 universell drivrutin.

   Detta gäller även återskapade/parallellutskrifter med en PCL-drivrutin som inte stöder autentisering.
6. Användarkoden anges inte med hjälp av PostScript3-skrivardrivrutin eller PS3 universell drivrutin. Detta gäller även återskapade/parallellutskrifter med en PCL-drivrutin som inte stöder autentisering.
7. Ett utskriftsjobb eller en PDF-fil skickas från en värddator som inte har en skrivardrivrutin och skrivs ut via LPR.
8. En PDF-fil skrivs ut via ftp. Personlig autentisering utförs med hjälp av det användar-ID och lösenord som används för inloggning via ftp. Användar-ID och lösenord krypteras inte.

Autentiseringsnivåer och typer av utskriftsjobb

Utskriftsjobbsautent.: Krypteringskod f drivrutin:Krypteringsgrad	Enkel (Alla): Enkel kryptering	Enkel (alla): DES	Enkel (alla): AES	Hela: Enkel kryptering	Hela: DES	Hela: AES
Utskriftsjobb typ 1	C*1	C*1	C*1	C*1	C*1	C*1
Utskriftsjobb typ 2	C*1	C*1	X*1	C*1	C*1	X*1
Utskriftsjobb typ 3	B	X*1	X*1	B	X*1	X*1
Utskriftsjobb typ 4	X	X	X	X	X	X
Utskriftsjobb typ 5	A	A	A	B	B	B
Utskriftsjobb typ 6	A	A	A	X	X	X
Utskriftsjobb typ 7	A	A	A	X	X	X
Utskriftsjobb typ 8	B	B	B	B	B	B

*1 Utskrift med användarkodsautentisering klassificeras som B.

A: Utskrift kan göras oavsett användarautentisering.

B: Utskrift kan göras om användarautentisering lyckas. Om användarautentiseringen inte lyckas nollställs utskriftsjobbet.

C: Utskrift är möjlig om användarautentiseringen lyckas och "Krypteringskod för drivrutin" till skrivardrivrutinen och maskinen stämmer överens.

X: Utskrift kan inte göras oavsett användarautentisering, utskriftsjobbet nollställs.

Obs

- För mer information om "Krypteringskod f drivrutin: Krypteringsgrad", se s. 193 "Ange Utökade säkerhetsfunktioner".

"authfree"-kommandot

Om [Enkel(Begränsning)] har valts under autentisering av utskriftsjobb, kan kommandot telnet authfree användas för att ange undantag för autentiseringen av utskriftsjobben.

För mer information om användarnamn och lösenord för att logga in på telnet, fråga administratören. För mer information om hur man loggar in och använda telnet, se handboken Anslut maskinen/ Systeminställningar.

Visa inställningar

```
msh> authfree
```

Om uteslutning av utskriftsjobbautentisering inte är inställt, visas inte kontrollen av autentiseringsuteslutning.

IPv4-adressinställningar

```
msh> authfree "ID" range "start-address" "end-address"
```

IPv6-adressinställningar

```
msh> authfree "ID" range6 "start-address" "end-address"
```

Inställningar för IPv6-adressmask

```
msh> authfree "ID" mask6 "base-address" "masklen"
```

Initialisering av autentiseringens exkluderingskontroll

```
msh> authfree flush
```

Obs

- För IPv4- och IPv6-omgivningarna kan upp till 5 åtkomstområden registreras och väljas.

Automatisk registrering i adressboken

Personuppgifter för användare som loggar in via Windows- eller LDAP-autentisering registreras automatiskt i adressboken.

Poster som har registrerats automatiskt i adressboken

- Användarnamn
- Lösenord
- Registreringsnr
- Namn*1
- Tangentnamn*1

*1 När informationen inte kan erhållas registreras användarnamnet i det här fältet.

Obs

- Du kan automatiskt ta bort gamla användarkonton när du utför automatisk registrering om mängden data som registrerats i adressboken har nått gränsen. För mer information, se s. 192 "Hantera adressboken".

Funktion för utelåsning av användare

Om ett felaktigt lösenord anges flera gånger förhindrar utelåsningsfunktionen ytterligare inloggningsförsök under samma användarnamn. Även om den utelåsta användaren anger rätt lösenord senare, kommer autentiseringen att misslyckas och maskinen kan inte användas förrän utelåsningsperioden löper ut eller en administratör eller övervakare avaktiverar utelåsningen.

För att använda utelåsningsfunktionen för användarautentisering måste autentiseringsmetoden vara inställd på grundläggande autentisering. Under andra autentiseringsmetoder skyddar utelåsningsfunktionen endast övervakares och administratörers konton, inte vanliga användarkonton.

Inställningsposter för utelåsning

Inställningar för utelåsningsfunktionen kan göras med Web Image Monitor.

Inställningsposter	Beskrivning	Inställningsvärden	Standardinställning
Utelåsning	Ange om du ska aktivera utelåsningsfunktionen eller inte.	• Aktivt • Ej aktivt	Ej aktivt
Antal försök innan Utelåsning sker	Ange antalet autentiseringsförsök som ska tillåtas innan utelåsning sker.	1-10	5
Timer för när utelåsningen ska upphöra	Ange om du vill avbryta utelåsningen efter att en angiven period har löpt ut eller inte.	• Aktivt • Ej aktivt	Ej aktivt
Lås användare ute i	Ange efter hur många minuter utelåsningen ska avbrytas.	1-9999 min.	60 min.

Behörighet att häva utelåsning

Administratörer med behörighet att låsa upp är följande:

Utelåst användare	Administratör som låser upp
Allmän användare	Användaradministratör

Utelåst användare	Administratör som låser upp
Användaradministratör, nätverksadministratör, filadministratör, maskinadministratör	Övervakare
Övervakare	Maskinadministratör

Ange funktionen utelåsning av användare

1. **Logga in som maskinadministratör från Web Image Monitor.**
2. **Peka på [Enhetshantering] och klicka sedan på [Konfiguration].**
3. **Klicka på [User Lockout Policy] under "Säkerhet".**
4. **Ställ in "Utelåsning" på [Aktivt].**
5. **I rullgardinsmenyn väljer du antalet inloggningsförsök som du vill tillåta innan utelåsningen aktiveras.**
6. **Om du blivit utelåst och vill upphäva utelåsningen efter en angiven tid ställer du "Lockout Release Timer" på [Aktivt].**
7. **I fältet "Lås användare ute i" anger du antal minuter innan utelåsningen upphävs.**
8. **Klicka på [OK].**

   Princip om utelåsning av användare ställs in.
9. **Logga ut.**

Upphäva lösenordsutelåsning

1. **Logga in som användaradministratör från Web Image Monitor.**
2. **Peka på [Enhetshantering] och klicka sedan på [Adressbok].**
3. **Markera den utelåsta användarens konto.**
4. **Klicka på [Detaljerad inmatning] och klicka sedan på [Ändra].**
5. **Ställ in "Utelåsning" på [Ej aktivt] under "Autentiseringsinformation".**
6. **Klicka på [OK].**
7. **Logga ut.**

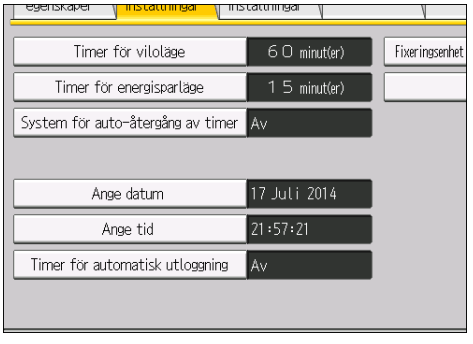
Obs

- Du kan avbryta utelåsning av administratörs- och övervakarlösenord genom att slå av och på huvudströmmen eller genom att avbryta inställningen i [Programmera/Ändra administratör] under [Konfiguration] i Web Image Monitor.

Automatisk utloggning

När du har loggat in loggar maskinen automatiskt ut dig om du inte använder kontrollpanelen inom en given tid. Funktionen kallas "Automatisk utloggning". Ange hur länge skrivaren ska vänta med automatisk utloggning.

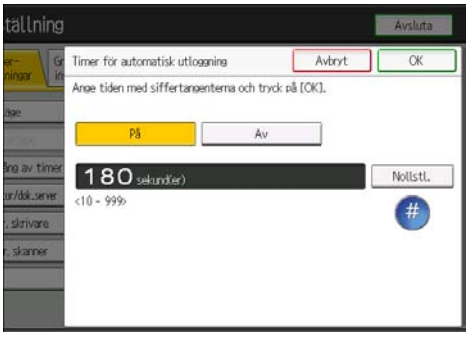
1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Timerinställningar].**
4. **Tryck på [Timer för automatisk utloggning].**



5. **Välj [På].**

   Om du inte vill ange en [Timer för automatisk utloggning], välj [Av].

6. **Ange "10" till "999" (sekunder) med siffertangenterna och tryck sedan på [#].**



   Om du gör ett misstag, tryck på [Nollstl.].

7. **Tryck på [OK].**
8. **Tryck på tangenten [Logga in/Logga ut].**

   Ett bekräftelsemeddelande visas. Om du trycker på [Ja] loggas du automatiskt ut.

Obs

- Du kan ange inställningar för Automatisk utloggning med Web Image Monitor via [Webbsida]. För mer information, se hjälpen för Web Image Monitor.

Autentisering med extern enhet

För att utföra autentisering genom en extern enhet, se enhetens handboken.

Mer information kan du få av din säljare.

3. Begränsa maskinanvändning

I detta kapitel beskrivs hur du begränsar användarens användning av maskinen.

Förhindra att administratörsinställningar ändras

Begränsa de inställningar som kan ändras av varje administratör

Inställningarna som kan göras för den här maskinen varierar beroende på administratörstyp samt definierar de olika åtgärder som kan delas mellan olika administratörer.

Följande administratörer är definierade för denna maskin:

- Användaradministratör
- Maskinadministratör
- Nätverksadministratör
- Filadministratör

För mer information om de inställningar som de olika administratörerna kan göra, se s. 221 "Lista över inställningsbehörigheter".

Registrera administratörerna innan du använder maskinen. För instruktioner om hur man registrerar administratörer, se s. 14 "Registrera och ändra administratörer".

Förhindra att användare kan ändra inställningar

Det är möjligt att förhindra användare från att ändra administratörsinställningar.

Välj objektet under "Tillgängliga inst." in "Hantering av administratörsautentisering" för att förhindra ändringar.

Mer information om vilka poster som kan väljas finns i "Tillgängliga inst.", se s. 11 "Konfigurera administratörsautentisering".

Specificera Menyskydd

Via Menyskydd kan du begränsa användarens åtkomst till inställningarna i menyn Användarverktyg med undantag av Systeminställningar. Denna inställning kan användas oavsett användarautentisering. För att använda inställningen Menyskydd aktiveras administratörsautentisering för maskinadministratören i förväg. För mer information om hur du ställer in administratörsautentisering, se s. 11 "Konfigurera administratörsautentisering". För en lista över de inställningar som användare kan ange enligt nivån på Skydda meny, se s. 221 "Lista över inställningsbehörigheter".

Om du vill aktivera "Menyskydd" ställer du in det på [Nivå 1] eller [Nivå 2]. Välj [Nivå 2] för att införa striktare restriktioner på användarnas åtkomstbehörighet till maskininställningarna.

Om du vill inaktivera "Menyskydd" ställer du det på [Av].

Skrivarfunktion

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Skrivaregenskaper].**
3. **Tryck på [Datahantering].**
4. **Tryck på [Menyskydd].**
5. **Välj nivå för menyskydd och tryck sedan på [OK].**
6. **Logga ut.**

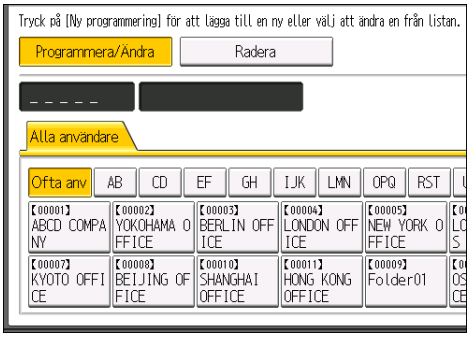
Begränsa Tillgängliga funktioner

För att förhindra obehörig användning kan du ange vem som kan få åtkomst till maskinens olika funktioner.

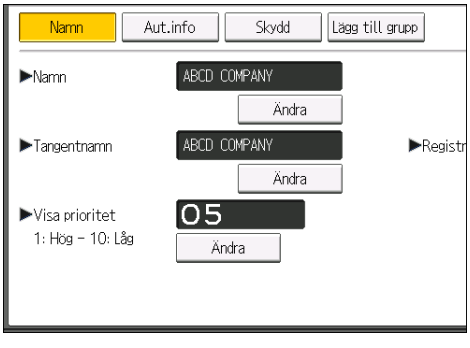
Ange vilka funktioner som är tillgängliga för registrerade användare. Genom att konfigurera denna inställning kan du begränsa funktionerna som är tillgängliga för användare.

Du kan begränsa användningen av skrivaren och utökade funktioner.

1. **Logga in som användaradministratör via kontrollpanelen.**
2. **Tryck på [Hantera adressboken].**
3. **Välj användare.**



4. **Tryck på [Aut.info].**



5. **Tryck på [▼Nästa] två gånger.**
6. **Under "Tillgängliga funktioner" väljer du de funktioner som ska anges.**

   Om den funktion du vill välja inte visas, tryck på [▼Nästa].
7. **Tryck på [OK].**
8. **Logga ut.**

Begränsa åtkomst till medieanslutning

Ange på kontrollpanelen om användare ska tillåtas använda medieanslutning eller inte. Med den här inställningen kan du begränsa utskrift av filer som lagrats på en flyttbar minnesenhet.

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa].**
5. **Tryck på [Använd Mediaanslutning].**
6. **För att begränsa utskrift av filer lagrade på en flyttbar minnesenhet, tryck på [Förhindra] under "Skriv ut från minnesenhet".**
7. **Tryck på [OK].**
8. **Logga ut.**

Obs

- Om du väljer [Förbjud] under "Skriv ut från minnesenhet" visas inte knappen [Skriv ut från minnesenhet] på skrivarfunktionens startskärm.

Hantera utskriftsvolym per användare

Denna funktion anger begränsad utskriftsvolym för varje användare. Om antalet utskrifter som en användare kan ange når max tillåten volym kommer utskriftsjobben att avbrytas och ett meddelande som indikerar att utskriftvolymen har nått den maximala nivån visas.

Utskriftsvolym

Utskriftsvolymen räknas ut genom att multiplicera antalet utskrivna sidor med en enhetsräkning.

Enhetsräkningen kan anges enligt utskriftsförhållandena. Exempel: om enhetsräkningen är 10 för 1 sida som skrivs ut, blir utskriftsvolymen 10.

Utskriftsvolymen spåras för varje användare.

Ställa in poster

Post	Förklaring	Inställning
Maskinåtgärd när begränsning är nådd	Ange om utskriftsvolymen ska begränsas samt vilken metod som ska användas för att begränsa utskrift. • Avbryt jobb När den maximala tillåtna utskriftsvolymen har nåtts, avbryts både aktuella och väntande jobb. • Slutför jobb & begr forts anv När max tillåtna utskriftsvolym har nåtts, slutförs det aktuella jobbet men väntande jobb avbryts. • Tillåt fortsatt användning Anger att inga begränsningar av utskriftsvolym finns.	• Avbryt jobb • Slutför jobb & begr forts anv • **Tillåt fortsatt användning** (standardinställning)
Begränsad utskriftsvolym: räkneverksinställning	Du kan ange begränsad utskriftsvolym per användare enligt följande 4 villkor. • Skrivare: Färg: A3/DLT • Skrivare: Svartvitt: A3/DLT • Skrivare: Färg: Övriga • Skrivare: Svartvitt: Övriga	0 till 200 (Antal enheter per sida är som standard 1 för varje utskriftsvillkor.)

Observera för begränsad utskriftsvolym

Utskrift är inte möjligt om följande inträffar:

- Registrerat användarnamn eller användarkod ändras i adressboken under tiden som användaren är inloggad och autentiserad.

Om följande inträffar kan inte hanteringen av utskriftsvolym fungera korrekt:

- Vid Windows eller LDAP-autentisering loggar en användare in till samma användarkonto via flera användarnamn och dessa användarnamn är registrerade i adressboken som separata användare.

Begränsad utskriftsvolym tillämpas inte vid följande åtgärder:

- Skriva ut från ett operativsystem som inte stödjer aktuell autentiseringsmetod

Ange begränsad utskriftsvolym

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa].**
5. **Tryck på [Maskinåtgärd när begränsning är nådd].**
6. **Välj [Avbryt jobb] eller [Slutför jobb & begr forts anv] och tryck sedan på [OK].**

   Om du inte vill begränsa utskriftsvolymen väljer du [Tillåt fortsatt användning].
7. **Tryck på [Begränsad utskriftsvolym: räkneverksinställning].**
8. **För varje utskriftsvillkor, använd siffertangenterna och ange antal enheter per sida mellan "0" och "200" och tryck sedan på [#].**

   Om du anger "0" som utskriftsvillkor tillämpas ingen begränsad utskriftsvolym för jobb som matchar detta villkor.
9. **Tryck på [OK].**
10. **Logga ut.**

Obs

- Begränsningar av utskriftsvolym kan även anges i [Begränsad utskriftsvolym] under "Konfiguration" i Web Image Monitor.

Begränsningar när Autentisering av användarkod är aktiverad

När autentisering av användarkod är aktiverad gäller följande för begränsad utskriftsvolym:

- Om [PC-kontroll] har valts som skrivarfunktion kanske värdena som angivits för utskriftsvolymen inte gäller för användarens utskriftsräkneverk. Välj inte [PC-kontroll] om du vill ange begränsad utskriftsvolym när autentisering av användarkod är aktiverad.

- Under grund-, Windows- samt LDAP-autentisering indikerar de siffror som visas längst ner till vänster i kontrollpanelen den totala utskriftsvolymen som administratören anger för användaren. Under autentisering av användarkod kan användarna själva inte kontrollera den totala utskriftsvolym de använt via kontrollpanelen eller via Web Image Monitor. Användare måste fråga administratörer om den totala utskriftsvolymen.
- Loggdata om använd utskriftsvolym registreras inte i jobb- eller åtkomstloggen.
- Beroende på vilka inställningar som konfigurerats för autentisering av användarkod kan det vara möjligt för användare att skriva ut innan de loggar in, oavsett vilka begränsningar av utskriftsvolym som angivits av administratören. Begränsa alla funktioner via "Funktioner att begränsa" i [Autent. anv.kod.] i [Hantering av användarautentisering].

Ange standardvärdet för begränsad utskriftsvolym

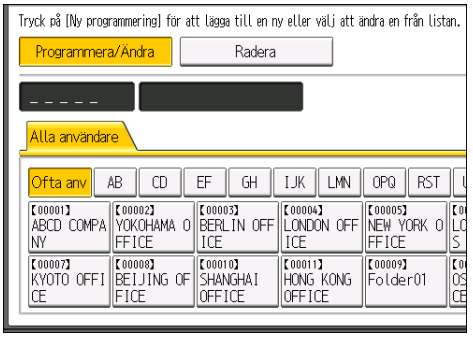
1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa].**
5. **Tryck på [Begränsad utskriftsvolym: standardvärde].**

   [Begränsad utskriftsvolym: standardvärde] visas inte om du har valt [Tillåt fortsatt användning] i "Maskinåtgärd när begränsning är nådd".
6. **Använd siffertangenterna för att ange ett värde mellan "0" och "999 999" som högsta värde för utskriftsvolym och tryck sedan på [#].**
7. **Tryck på [OK].**
8. **Logga ut.**

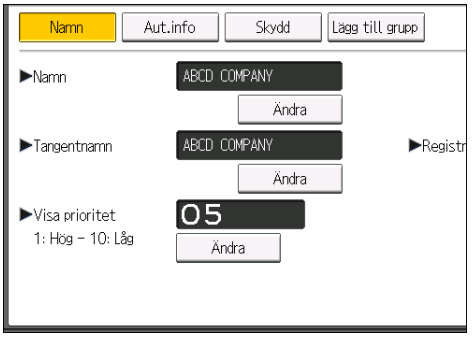
Ange maximal användning per användare

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Hantera adressboken].**

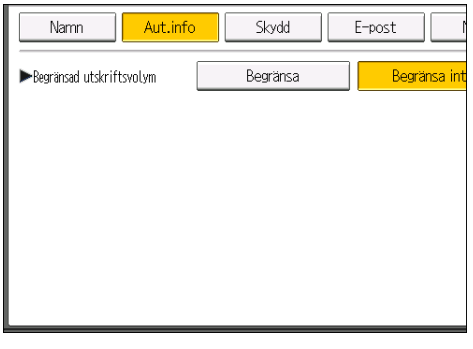
3. **Välj den användare vars utskriftsvolym du vill begränsa.**



4. **Tryck på [Aut.info].**



5. **Tryck på [▼Nästa] två gånger.**
6. **Tryck på [Begränsa] i "Begränsad utskriftsvolym".**



"Begränsad utskriftsvolym" visas inte om du har valt [Tillåt fortsatt användning] i "Maskinåtgärd när begränsning är nådd".

Om du inte vill ange någon begränsad utskriftsvolym, tryck på [Begränsa inte].

7. **Tryck på [Ändra] och använd siffertangenterna för att ange ett värde mellan "0" och "999 999" som högsta värde för utskriftsvolym och tryck sedan på [#].**

En användares maximala utskriftsvolym är inställd på "0" kan endast skriva ut jobb vars utskriftsvillkor matchar de med ett enhetsvärde av "0".

8. **Tryck på [OK].**
9. **Logga ut.**

Obs

- Den maximala utskriftsvolymen för varje användare kan även anges i [Adressbok]en i Web Image Monitor.

Kontrollera utskriftsvolym per användare

Den här metoden kan hanteras av vilken administratör som helst.

1. **Logga in som administratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [Visa/Rensa/Skriv ut räkneverk per användare].**

5. **Tryck på [Utskriftsvolym].**

   Begränsad utskriftsvolym samt total utskriftsvolym visas för varje användare.
6. **När du har bekräftat inställningarna loggar du ut.**

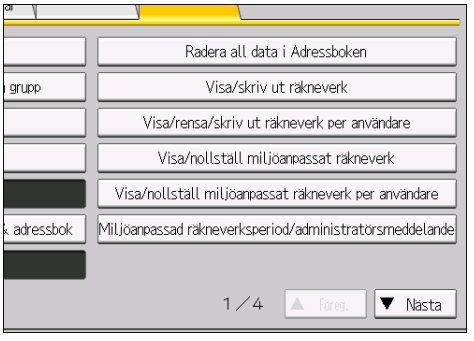
Obs

- Auktoriserade användare och användaradministratörer kan även använda [Adressbok] i Web Image Monitor för att kontrollera räkneverken för utskriftsvolym för varje användare.

Skriva ut en lista över användarräkneverkens utskriftsvolym

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**

4. **Tryck på [Visa/Rensa/Skriv ut räkneverk per användare].**



5. **Tryck på [Utskriftsvolym].**

   En lista över användarräkneverkens utskriftsvolym visas.

   För att välja alla användare som visas på sidan, tryck på [Välj allt på sidan].

6. **För att skriva ut en lista över användarräkneverkens utskriftsvolym trycker du på [Skriv räknv.lista] under "Alla användare". För att skriva ut en lista över användarräkneverkens utskriftsvolym med endast valda användare, väljer du vilka användares räkneverk du vill skriva ut och trycker sedan på [Skriv räknv.lista] under "Per användare".**
7. **Välj vilket räkneverk du vill skriva ut ifrån listan och tryck på [Utskrift].**
8. **Logga ut.**

Obs

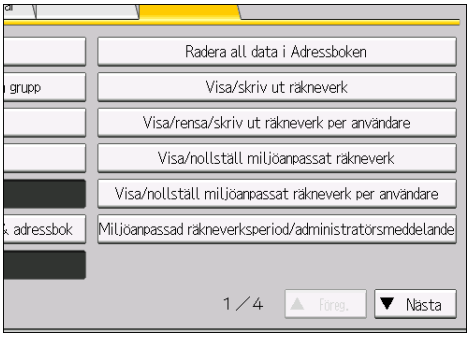
- Listor över användarräkneverk för utskriftsvolym kan endast skrivas ut om följande pappersformat är laddat i papperskassetten: A4, 8 $^{1}/_{2}$ × 11 tum, B4, 8 $^{1}/_{2}$ × 14 tum, A3, eller 11 × 17 tum.

Återställa användarräkneverk för utskriftsvolym

När användarräkneverken för utskriftsvolym återställs eller när begränsad utskriftsvolym höjs kan användaren skriva ut mer än hans eller hennes tillåtna utskriftsvolym.

1. **Logga in som användaradministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**

4. **Tryck på [Visa/Rensa/Skriv ut räkneverk per användare].**



5. **Tryck på [Utskriftsvolym].**

   En lista över användarräkneverkens utskriftsvolym visas.

6. **För att återställa användarräkneverken för utskriftsvolym trycker du på [Nollstl.] under "Alla användare". För att återställa räkneverken för utskriftsvolym för valda användare, väljer du de användare vars räkneverk du vill återställa och trycker sedan på [Nollstl.] under "Per användare".**

   För att välja alla användare som visas på sidan, tryck på [Välj allt på sidan].

7. **Välj [Utskriftsvolym] och tryck sedan på [OK].**

8. **Logga ut.**

Obs

- Du kan också använda [Adressbok] i Web Image Monitor för att återställa räkneverken för utskriftsvolym. Använd kontrollpanelen om du vill återställa alla användares räkneverk för utskriftsvolym samtidigt.

Konfigurera automatisk återställning

Räkneverket för utskriftsvolym kan återställas vid en angiven tidpunkt.

Tillval	Detaljer
Varje månad	Återställer utskriftsvolymen på angivet klockslag/datum varje månad.
Ange datum	Återställer utskriftsvolymen (endast en gång) på angivet klockslag/datum.
Ange cykel	Återställs efter ett angivet intervall enligt ett referensdatum och återställs sedan vid samma intervall.

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**

3. **Tryck på [Admin.verktyg].**
4. **Tryck 3 gånger på [▼Nästa].**
5. **Tryck på[Räkneverk f utskr.volym: Schemalagd/ang återställn.inst.].**
6. **Välj [Varje månad], [Ange datum] eller [Ange cykel].**
7. **Konfigurera villkoren.**
8. **Tryck på [OK].**
9. **Logga ut.**

Obs

- Om maskinen är avstängd vid angiven tidpunkt på den angivna dagen, återställs utskriftsvolymen när strömmen slås på.
- Om du väljer ett datum i [Varje månad], exempelvis den 31 varje månad - ett datum som finns vissa månader men inte andra - kommer utskriftsvolymen att återställas klockan 24:00 den 1a dagen i månaden som följer den månad som inte har 31 dagar.

4. Förhindra läckage av information från maskiner

I det här kapitlet beskrivs hur du skyddar information som har lagrats i maskinens minne eller på hårddisken.

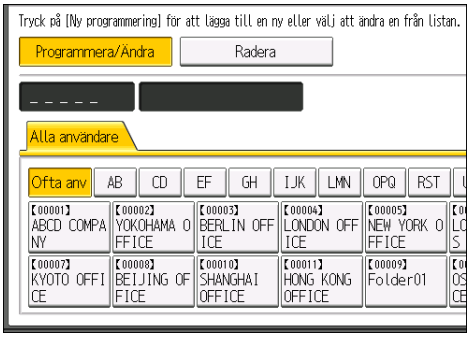
Skydda adressboken

Du kan ange vilka personer som ska ha åtkomst till datan i adressboken. För att skydda data från obehöriga användare kan du även kryptera uppgifterna i adressboken.

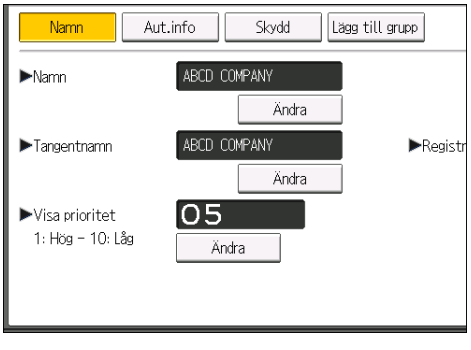
Ange åtkomstbehörighet till adressboken

Åtkomstbehörigheter kan anges av användare som är registrerade i adressboken, användare med full behörighet samt användaradministratören.

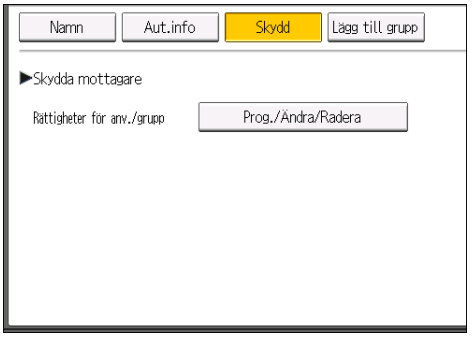
1. **Logga in som användaradministratör via kontrollpanelen.**
2. **Tryck på [Hantera adressboken].**
3. **Välj den användare vars åtkomstbehörighet du vill ändra.**



4. **Tryck på [Skydd].**



5. **Tryck på [Prog./Ändra/Radera] för "Rättigheter för användare/grupper", under "Skydda mottagare".**



6. **Tryck på [Ny progr.].**

7. **Välj de användare eller grupper som ska tilldelas åtkomstbehörighet.**

   Du kan välja flera användare.

   Genom att trycka på [Alla användare] kan du välja alla användare.

8. **Tryck på [Avsluta].**
9. **Välj den användare som du vill tilldela åtkomstbehörigheter och ange sedan vilken behörighet.**

   Ange en av följande: [Skrivskyddad], [Redigera], [Redigera/Ta bort] eller [Fulla rättigheter].

10. **Tryck på [Avsluta].**
11. **Tryck på [OK].**
12. **Logga ut.**

Obs

- Åtkomstbehörigheterna "Redigera", "Redigera/Ta bort" och "Fulla rättigheter" gör det möjligt för användare att utföra åtgärder som kan innebära att känslig information ändras eller går förlorad. Vi rekommenderar att du endast ger behörigheten "Skrivskyddad" till vanliga användare.

Kryptera data i adressboken

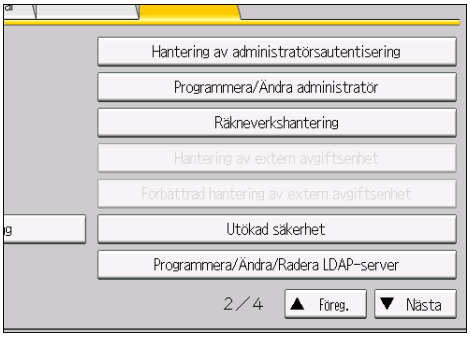
Viktigt

- **Maskinen kan inte användas under krypteringen.**

Hur länge det tar att kryptera data i adressboken beror på antalet registrerade användare.

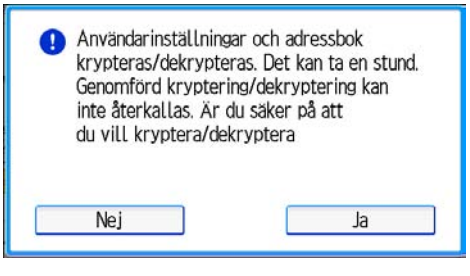
Kryptering av uppgifter i adressboken kan ta längre tid.

1. **Logga in som användaradministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa].**
5. **Tryck på [Utökad säkerhet].**



6. **Tryck [På] för "Kryptera användarinställningar & adressbok".**
7. **Tryck på [Ändra] för "Krypteringskod".**
8. **Ange krypteringskod och tryck på [OK].**

   Ange krypteringskod med upp till 32 alfanumeriska tecken.
9. **Tryck på [Kryptera/Dekryptera].**
10. **Tryck på [Ja].**



Stäng inte av strömmen till maskinen medan kryptering pågår eftersom data då kan skadas.

Om du trycker på [Stopp] under kryptering, avbryts kryptering av all data.

Om du trycker på [Stopp] under dekryptering så avbryts dekryptering av all data.

Vanligtvis, när krypteringen är slutförd, visas "Kryptering/dekryptering slutförd. Tryck på [Avsluta]."

11. **Tryck på [Avsluta].**
12. **Tryck på [OK].**
13. **Logga ut.**

Obs

- Om du registrerar ytterligare användare efter att du krypterat data i adressboken så krypteras även deras uppgifter.
- Säkerhetskopian av adressboksinformationen som lagrats på SD-kortet är krypterad. För mer information om hur man säkerhetskopierar och återställer adressboken med hjälp av ett SD-kort, se handboken Connecting the Machine/System Settings (Anslut maskinen/Systeminställningar).

Kryptera data på maskinen

⚠FÖRSIKTIGT

- Se till att SD-kort och USB-minnen hålls utom räckhåll för barn. Kontakta läkare omdelbart om ett barn råkar svälja ett SD-kort eller USB-minne.

Även om minnesenheten eller hårddisken blir stulen kan dataläckage förhindras genom kryptering av all data på maskinen som adressbok, autentiseringsdata och filer.

När du aktiverat kryptering kommer all data som sedan lagras på maskinen att krypteras.

Du kan också välja att kryptera eller radera de data som lagras på maskinen för tillfället.

Krypteringsalgoritmen är AES-256.

Data som är krypterad

Den här funktionen krypterar data som lagras i maskinens NVRAM (minne som finns kvar även efter att maskinen har stängts av) och på hårddisken.

Följande data krypteras:

NVRAM

- Information om systeminställningar
- Information om inställningar för nätverk I/F
- Information om användarkod
- Räkneverksinformation

Hårddisk

- Adressbok
- Programmet Embedded Software Architectures program/loggar
- Loggar (jobblogg/åtkomstlogg/miljöanpassad logg)
- Skickad/mottagen e-post
- Registrerade fonter
- Spooljobb
- Lagrade dokument

Typ av kryptering

Ange om du vill kryptera befintlig data och ha den kvar på hårddisken eller radera (formatera) den. Krypteringen tar lång tid om du ska ha kvar stora mängder data. NVRAM-data kommer inte raderas (initialiseras).

Inställning	Data som sparas.	Data som ska initieras	Tidsåtgång
Endast filsystems data	• Adressbok • Programmet Embedded Software Architectures program/loggar • Loggar (jobblogg/ åtkomstlogg/ miljöanpassad logg) • Skickad/mottagen e-post • Registrerade fonter • Spooljobb	• Lagrade dokument (Säker utskrift/ Provutskrift/Lagrad utskrift/Utskriftskö)	Cirka 2 timme och 45 minuter
All data	All data: Både data som ska sparas och som inte ska sparas när [Endast filsystemsdata] anges	Inget	Cirka 8 timmar
Formatera all data	Inget	All data: Både data som ska sparas och som inte ska sparas när [Endast filsystemsdata] anges	Flera minuter

Anvisningar för att aktivera krypteringsinställningar

- Om du använder programmet Embedded Software Architecture eller App2Me ska du vara noga med at ange [Endast filsystems data] eller [All data].
- Observera att maskinens inställningar inte initieras till systemstandard även om [Formatera all data], [Endast filsystems data] eller [All data] anges.

Återställa data

- Återställ krypterad data för att överföra data till en ny maskin. För mer information, kontakta en servicetekniker.
- Krypteringsnyckeln som används vid datakrypteringen krävs för att återställa data.
- Du kan välja mellan att skriva ut krypteringsnyckeln eller att lagra den på ett SD-kort.
- Du kan ändra krypteringsnyckeln senare.

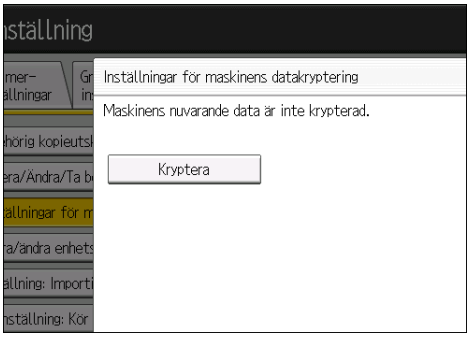
Aktivera krypteringsinställningar

Viktigt

- Maskinen kan inte användas när data krypteras.
- När krypteringsprocessen har startat kan den inte avbrytas. Se till att maskinens strömförsörjning inte bryts under krypteringsprocessen. Om maskinens ström slås av under krypteringsprocessen kommer hårddisken att förstöras och all data kommer att bli oanvändbar.
- Krypteringsnyckel krävs för att återställa data om det är fel på maskinen. Se till att förvara krypteringskoden säkert för att återfå säkerhetskopierad data.
- Krypteringen startas efter att du har slutfört kontrollpanelsprocessen och startat om maskinen genom att slå av och sedan på strömbrytaren. Om både funktionen för Radera allt minnesamt funktionen för kryptering har angivits börjar krypteringen när den data som lagrats på hårddisken har skrivits över och maskinen har startats om genom att strömbrytaren slås av och på.
- Om du använder Radera allt minnet och kryptering samtidigt, och väljer att skriva över 3 gånger med "Slumpvisa siffror" tar processen upp till 13 timmar och 15 minuter. Att göra en ny kryptering när data redan krypterats tar ungefär lika lång tid.
- Funktionen "Radera allt minne" raderar även maskinens säkerhetsinställningar, så att varken maskin- eller användaradministration är möjligt. Säkerställ att användarna inte sparar data på maskinen när Radera allt minne har slutförts.
- Omstarten går snabbare om det inte finns data som ska överföras till hårddisken och om kryptering är inställd på [Formatera all data], även om all data på hårddisken är formaterad. Innan du utför kryptering rekommenderar vi att du säkerhetskopierar viktig data, t.ex. adressboken.

1. Logga in som maskinadministratör via kontrollpanelen.
2. Tryck på [Systeminställning].
3. Tryck på [Admin.verktyg].
4. Tryck på [▼Nästa] två gånger.
5. Tryck på [Krypteringsinställningar för maskinens data].

6. **Tryck på [Kryptera].**



7. **Välj vilken data som ska föras över till hårddisken samt vilken data som inte ska raderas.**

   För att överföra all data till hårddisken, välj [All Data]. För att endast överföra data för maskinens inställningar, välj [Endast filsystemsdata]. För att radera all data, välj [Formatera all data].

8. **Välj hur du vill säkerhetskopiera krypteringsnyckeln.**

   Om du har valt [Spara på SD-kort] sätter du i ett SD-kort i kortplatsen på sidan av kontrollpanelen och trycker på [OK] för att säkerhetskopiera maskinens datakrypteringskod.

   För information om hantering och anslutning av SD-kortet, se handboken Getting Started (Komma igång).

   Om du har valt [Skriv ut på ppr] trycker du på [Start] och skriver ut maskinens datakrypteringsnyckel.

9. **Tryck på [OK].**
10. **Tryck på [Avsluta].**
11. **Tryck på [Avsluta].**
12. **Logga ut.**
13. **Stäng av huvudströmbrytaren och slå sedan på den igen.**

    Maskinen börjar att konvertera datan på minnet när du slår på den. Vänta till meddelandet "Minneskonvertering slutförd. Stäng av huvudströmbrytaren." visas och slå sedan av huvudströmmen igen.

    För information om hur du stänger av huvudströmmen, se handboken Komma igång.

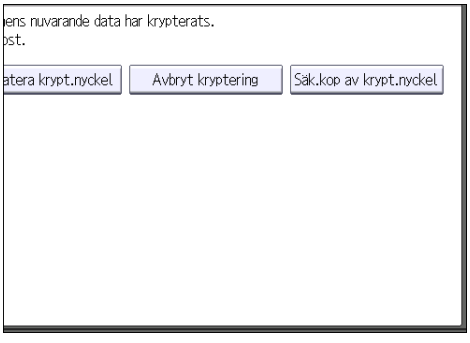
Säkerhetskopiera krypteringsnyckeln

Du kan säkerhetskopiera krypteringsnyckeln utan att ändra krypteringsinställningarna.

Viktigt

- **Krypteringsnyckel krävs för att återställa data om det är fel på maskinen. Se till att förvara krypteringskoden säkert för att återfå säkerhetskopierad data.**

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa] två gånger.**
5. **Tryck på [Krypteringsinställningar för maskinens data].**
6. **Tryck på [Säk.kop av krypt.nyckel].**



7. **Välj hur du vill säkerhetskopiera krypteringsnyckeln.**

   Om du har valt [Spara på SD-kort] sätter du i ett SD-kort i kortplatsen på sidan av kontrollpanelen och trycker på [OK]. När maskinens datakrypteringskod är säkerhetskopierad, tryck på [Avsluta].

   För information om hantering och anslutning av SD-kortet, se handboken Getting Started (Komma igång).

   Om du har valt [Skriv ut på ppr] trycker du på [Start] och skriver ut maskinens datakrypteringsnyckel.

8. **Tryck på [Avsluta].**
9. **Logga ut.**

Uppdatera krypteringskoden

Du kan uppdatera krypteringsnyckeln. Att tillämpa den nya krypteringsnyckeln tar lika lång tid som det gör att starta krypteringen. Uppdateringar är möjliga när maskinen fungerar normalt.

Viktigt

- **Maskinen kan inte användas medan krypteringsnyckeln uppdateras.**
- **Krypteringskod krävs för återställande om det är fel på maskinen. Se till att förvara krypteringskoden säkert för att återfå säkerhetskopierad data.**
- **När krypteringskoden uppdateras utförs kryptering med den nya koden. När du har genomfört processen på maskinens kontrollpanel, stäng av huvudströmmen och starta om maskinen så att de nya inställningarna aktiveras. Omstarten kan gå långsamt när det finns data att föra över till hårddisken.**

- När uppdateringen av krypteringsnyckeln startas kan den inte stoppas. Se till att maskinens strömförsörjning inte bryts under krypteringsprocessen. Om maskinens ström slås av under krypteringsprocessen kommer hårddisken att förstöras och all data kommer att bli oanvändbar.
- Om uppdateringen av krypteringsnyckeln inte avslutades kommer den skapade krypteringsnyckeln inte vara giltig.

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa] två gånger.**
5. **Tryck på [Krypteringsinställningar för maskinens data].**
6. **Tryck på [Uppdatera krypt.nyckel].**

7. **Välj vilken data som ska föras över till hårddisken samt vilken data som inte ska raderas.**

   För att överföra all data till hårddisken, välj [All Data]. Om du bara vill överföra data för maskinens inställningar, välj [Endast filsystems data]. För att radera all data, välj [Formatera all data].

8. **Välj hur du vill säkerhetskopiera krypteringsnyckeln.**

   Om du har valt [Spara på SD-kort] sätter du i ett SD-kort i kortplatsen på sidan av kontrollpanelen och trycker på [OK] för att säkerhetskopiera maskinens datakrypteringskod.

   För information om hantering och anslutning av SD-kortet, se handboken Getting Started (Komma igång).

   Om du har valt [Skriv ut på ppr] trycker du på [Start] och skriver ut maskinens datakrypteringsnyckel.

9. **Tryck på [OK].**
10. **Tryck på [Avsluta].**
11. **Tryck på [Avsluta].**
12. **Logga ut.**

13. **Stäng av huvudströmbrytaren och slå sedan på den igen.**

    Maskinen börjar att konvertera datan på minnet när du slår på den. Vänta till meddelandet "Minneskonvertering slutförd. Stäng av huvudströmbrytaren." visas och slå sedan av huvudströmmen igen.

    För information om hur du stänger av huvudströmmen, se handboken Komma igång.

Avbryta datakryptering

Gör på följande sätt för att avbryta krypteringsinställningarna när kryptering inte behövs längre. Det tar lika lång tid att aktivera som att avaktivera krypteringsinställningarna.

Viktigt

- **Maskinen kan inte användas medan datakrypteringen avbryts.**
- **När du har utfört denna process på maskinens kontrollpanel, stäng av huvudströmmen och starta om maskinen så att de nya inställningarna aktiveras. Omstarten kan gå långsamt när det finns data att föra över till hårddisken.**
- **När avbrytandet av krypteringsprocessen har inletts kan det inte avbrytas. Se till att maskinens strömförsörjning inte bryts under krypteringsprocessen. Om maskinens ström slås av under krypteringsprocessen kommer hårddisken att förstöras och all data kommer att bli oanvändbar.**
- **Vid avyttring av en maskin, radera minnet helt och hållet. För mer information om hur du raderar allt minne, se s. 80 "Radera data på maskinen".**

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa] två gånger.**
5. **Tryck på [Krypteringsinställningar för maskinens data].**
6. **Tryck på [Avbryt kryptering].**
7. **Välj vilken data som ska föras över till hårddisken samt vilken data som inte ska raderas.**

    För att överföra all data till hårddisken, välj [All Data]. Om du bara vill överföra data för maskinens inställningar, välj [Endast filsystems data]. För att radera all data, välj [Formatera all data].
8. **Tryck på [OK].**
9. **Tryck på [Avsluta].**
10. **Tryck på [Avsluta].**
11. **Logga ut.**
12. **Stäng av huvudströmbrytaren och slå sedan på den igen.**

    För information om hur du stänger av huvudströmmen, se handboken Komma igång.

Radera data på maskinen

Du kan förhindra dataläckage genom överskrivning av data som finns lagrade på maskinen.

Överskrivning av data kan ske på följande två sätt:

Automatisk radering av minne

De data som lagras tillfälligt på maskinens hårddisk för utskrift raderas automatiskt. För mer information, se s. 80 "Radera minnesinställning automatiskt".

Radera allt minne

Alla data som lagras på maskinens hårddisk raderas genom överskrivning. Enhetsinställningarna som finns lagrade i maskinens minne initialiseras. Genomför detta för att radera alla data och inställningar när du ska flytta på eller avyttra maskinen. För mer information, se s. 84 "Radera allt minne".

Radera minnesinställning automatiskt

Utskriftsdata som skickats från en skrivardrivrutin lagras tillfälligt på maskinens hårddisk. Även efter att jobbet är färdigt blir det kvar på hårddisken som tillfällig data. Med autoradering av minne raderar du tillfällig data från hårddisken genom att skriva över dem.

Överskrivningen startar automatiskt så snart jobbet är avslutat.

Skrivarfunktionen har prioritet över den automatiska raderingsfunktionen. Om ett utskriftsjobb pågår, utförs överskrivningen först när detta är klart.

Typer av data som inte kan överskrivas med hjälp av automatisk minnesradering

Data som skrivs över med Automatisk radering av minne

Skrivare

- Utskriftsjobb
- Provutskrift/Säker utskrift/Utskriftskö/Lagrad utskrift-jobb

  Ett Provutskrift/Säker utskrift/Utskriftskö-jobb kan bara skrivas över efter att det har verkställts. Ett Lagrad utskrift-jobb skrivs över när det har raderats.
- Spoolutskriftsjobb

Annat

- Information som registreras i adressboken

  Data som lagrats i adressboken kan endast skrivas över efter att den har ändrats eller raderats.
- Program som använder Embedded Software Architecture

Embedded Software Architecture-programmens data kan endast skrivas över efter att den har raderats.

Data som inte skrivs över med Automatisk radering av minne

- Räkneverk lagrade under respektive användarkod

Överskrivningsmetoder

Du kan välja en metod för överskrivning enligt följande:

- NSA

  Temporär data skrivs över två gånger med slumpmässigt valda siffror och en gång med nollor.

- DoD

  Varje dataobjekt skrivs över med slumpvisa siffror, sedan med dess komplement, sedan med andra slumpvisa siffror och bekräftas sedan.

- Slumpm. siffror

  Temporär data skrivs över flera gånger med slumpvisa siffror. Antalet överskrivningar kan väljas från 1 till 9.

Obs

- Standardmetoden för överskrivning är "Slumpvisa siffror" och standardantalet överskrivningar är 3.
- NSA står för "National Security Agency", U.S.A.
- DoD står för "Department of Defense", U.S.A.

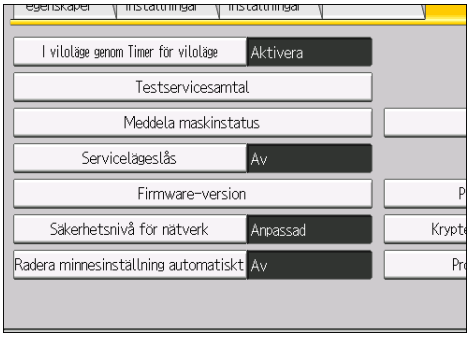
Använda Radera minne automatiskt

Viktigt

- **När Autoradera minne är inställt på [På], kan det hända att temporär data som fanns kvar på hårddisken när Autoradera minne var [Av] inte har skrivits över.**
- **Om huvudströmbrytaren på maskinen slås av innan automatisk minnesradering är klar, upphör överskrivningen och resterande data förblir kvar på hårddisken.**
- **Stoppa inte överskrivningen mitt i processen. Om så sker kan hårddisken skadas.**
- **Om maskinens huvudströmbrytare slås av innan Autoradera minnesinställningar är slutförd, återupptas den när maskinen slås på igen.**
- **Om ett fel uppstår innan överskrivningen är slutförd ska du stänga av strömmen. Sätt på strömmen igen och upprepa sedan från steg 1.**
- **Maskinen övergår inte i viloläge förrän överskrivningen har slutförts.**

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**

3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa] två gånger.**
5. **Tryck på [Radera minnesinställning automatiskt].**



6. **Tryck på [På].**
7. **Välj vilken metod för överskrivning som du vill använda.**

   Om du väljer [NSA] eller [DoD] fortsätter du till steg 10.

   Om du väljer [Slumpm. siffror], ska du gå vidare till steg 8.
8. **Tryck på [Ändra].**
9. **Använd siffertangenterna för att ange antal gånger som minnet ska skrivas över och tryck sedan på [#].**
10. **Tryck på [OK].**

    Autoradera minne är angivet.
11. **Logga ut.**

Obs

- Om du aktiverar både överskrivning och datakryptering, krypteras även data som skrivs över.

Avbryta Autoradera minne

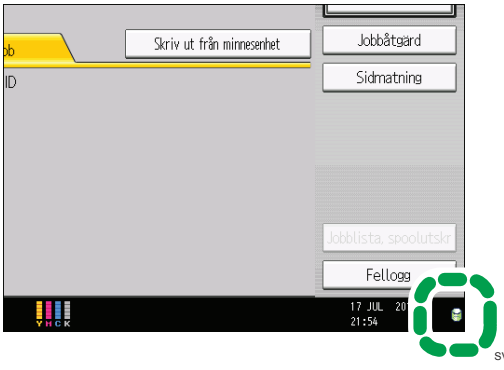
1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa] två gånger.**
5. **Tryck på [Radera minnesinställning automatiskt].**
6. **Tryck på [Av].**
7. **Tryck på [OK].**

   Autoradering av minne är avaktiverat.

8. **Logga ut.**

Överskrivningsikon

När automatisk radering av minneär aktiverat kommer ikonen för dataöverskrivning att visas i det nedre högra hörnet på kontrollpanelen på din maskin.



Ikon	Namn på ikon	Förklaring
	Otömd	Den här ikonen tänds när det finns tillfällig data som ska skrivas över och blinkar under överskrivning.
	Raderad	Den här ikonen tänds när ingen temporära data finns i minnet.

Viktigt

- **Ikonen för dataöverskrivning visar "Tömd" när det finns jobb för provutskrift/säker utskrift/ utskriftskö/lagrad utskrift.**

Obs

- Om ikonen för överskrivning av data inte visas, kontrollera då först om Radera minnesinställning automatiskt är inställt på [Av]. Kontakta din servicerepresentant om ikonen visas trots att den här inställningen är [På].
- Om maskinen övergår till energisparläge under överskrivningen kan du återställa displayen genom att trycka på knappen [Energibesparing] och kontrollera ikonen.
- Om dataöverskrivningsikonen fortsätter att vara "Otömd" när det inte finns någon data att skriva över, stäng då av huvudströmmen till maskinen. Slå sedan på den igen för att se om symbolen ändras till "Tömd". Om den inte gör det kontaktar du försäljaren eller en servicerepresentant.

Radera allt minne

Skriv över och radera all data som finns lagrad på hårddisken när du ska flytta på eller avyttra maskinen. Enhetsinställningarna som finns lagrade i maskinens minne initialiseras.

Om du vill ha mer information om hur du använder maskinen när Radera allt minne har slutförts ska du kontakta din säljare.

Viktigt

- **Om maskinens huvudströmbrytare slås av innan "Radera allt minne" har slutförts, stoppas överskrivningen och data kommer att finnas kvar på hårddisken.**
- **Stoppa inte överskrivningen mitt i processen. Om så sker kan hårddisken skadas.**
- **Vi rekommenderar att du använder Device Manager NX för att säkerhetskopiera adressboken innan du raderar hårddisken. Du kan även göra en säkerhetskopia av adressboken med Web Image Monitor. Mer information finns i hjälpen till Device Manager NX eller Web Image Monitor.**
- **Den enda åtgärden som är möjlig under processen "Radera allt minne" är att pausa. Om "Slumpvisa siffror" är valt och det är inställt att skriva över 3 gånger tar processen "Radera allt minne" upp till 5 timmar och 15 minuter.**
- **Funktionen "Radera allt minne" raderar även maskinens säkerhetsinställningar, så att varken maskin- eller användaradministration är möjligt. Säkerställ att användarna inte sparar data på maskinen när Radera allt minne har slutförts.**

Typer av data som kan skrivas över med Radera allt minne

Skrivare

- Utskriftsjobb
- Provutskrift/Säker utskrift/Utskriftskö/Lagrad utskrift-jobb
- Spoolutskriftsjobb

Annat

- Information som registreras i adressboken
- Räkneverk lagrade under respektive användarkod
- Program som använder Embedded Software Architecture

Systeminställningar eller andra inställningar som är relaterade till enheten kommer att initieras.

Metoder för radering

Du kan välja en metod för radering från följande:

- NSA

  Data skrivs över två gånger med slumpmässigt valda siffror och en gång med nollor.

- DoD

  Data skrivs över med en slumpvis siffra, sedan med dess komplement, sedan med en annan slumpvis siffra och därefter bekräftas den.

- Slumpm. siffror

  Data skrivs över flera gånger med slumpvisa siffror. Antalet överskrivningar kan väljas från 1 till 9.

- BSI/VSITR

  Data skrivs över 7 gånger med följande mönster: 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA.

- Säker radering

  Data skrivs över med hjälp av en algoritm som finns inbyggd i hårddiskenheten.

- Format

  Hårddisken är formaterad. Datan är inte överskriven.

Obs

- Standardmetoden för radering är "Slumpvisa siffror" och standardantalet överskrivningar är 3.
- NSA står för "National Security Agency", U.S.A.
- DoD står för "Department of Defense", U.S.A.

Använda Radera allt minne

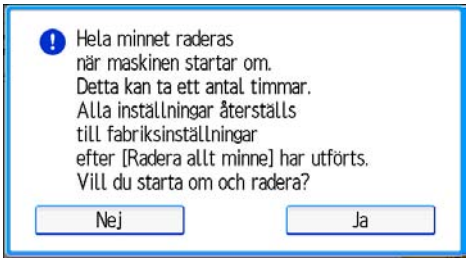
1. **Koppla bort kommunikationskablar som är anslutna till maskinen.**
2. **Logga in som maskinadministratör via kontrollpanelen.**
3. **Tryck på [Systeminställning].**
4. **Tryck på [Admin.verktyg].**
5. **Tryck på [▼Nästa] två gånger.**
6. **Tryck på [Radera allt minne].**

7. **Välj raderingsmetod.**

   Om du väljer [NSA], [DoD], [BSI/VSITR], [Säker radering] eller [Formattera] ska du fortsätta till steg 10.

   Om du väljer [Slumpm. siffror], ska du gå vidare till steg 8.

8. **Tryck på [Ändra].**
9. **Använd siffertangenterna för att ange antal gånger som minnet ska skrivas över och tryck sedan på [#].**
10. **Tryck på [Radera].**
11. **Tryck på [Ja].**



12. **När raderingen är färdig, tryck på [Avsluta] och slå sedan av huvudströmbrytaren.**

    För information om hur du stänger av huvudströmmen, se handboken Komma igång.

Obs

- Om skrivarens huvudströmbrytare slås av innan "Radera allt minne" har slutförts, startar överskrivningen om när maskinen slås på igen.
- Om ett fel uppstår innan överskrivningen är slutförd ska du stänga av strömmen. Sätt på strömmen igen och repetera sedan från steg 2.

Avbryta Radera allt minne

För att stänga av strömmen till maskinen medan Radera allt minne är aktiverat måste du först pausa Radera allt minne. Radera allt minne återupptas när du slår på strömmen igen.

Viktigt

- **Processen kan inte avbrytas om [Säker radering] eller [Formatering] har valts.**
- **Radera allt minne kan däremot inte avbrytas helt.**

1. **Tryck på [Avbryt] medan Radera allt minne är igång.**
2. **Tryck på [Ja].**

   Radera allt minne pausas.

3. **Stäng av huvudströmmen.**

   För information om hur du stänger av huvudströmmen, se handboken Komma igång.

5. Utökad nätverkssäkerhet

I detta kapitel beskrivs de funktioner som är avsedda att öka säkerheten när maskinen är ansluten till nätverket.

Åtkomstkontroll

Den här maskinen kan kontrollera TCP/IP-åtkomst.

Begränsa IP-adresserna från vilka åtkomst är möjlig genom att specificera ett intervall för åtkomstkontroll.

Om du till exempel vill ange ett intervall för åtkomstkontroll som [192.168.15.16]-[192.168.15.20], kommer de klient-PC-adresser med åtkomst att bli de från [192.168.15.16] till [192.168.15.20].

Viktigt

- **Med hjälp av åtkomstkontroll kan du begränsa åtkomster från LPR, RCP/RSH, FTP, ssh/sftp, Bonjour, SMB, WSD (enhet), WSD (skrivare), IPP, DIPRINT, RHPP eller Web Image Monitor. Du kan inte begränsa åtkomst från telnet eller Device Manager NX när SNMPv1 används för övervakning.**

1. **Logga in som nätverksadministratör från Web Image Monitor.**
2. **Peka på [Enhetshantering] och klicka sedan på [Konfiguration].**
3. **Klicka på [Åtkomstkontroll] under "Säkerhet".**
4. **För att ange en IPv4-adress, skriv in en IP-adress som har åtkomst till maskinen i "Intervall för åtkomstkontroll".**

   För att ange en IPv6-adress, skriv in en IP-adress som har åtkomst till maskinen i "Område" under "Intervall för åtkomstkontroll" eller skriv in en IP-adress i "Mask" samt ange "Masklängd".
5. **Klicka på [OK].**
6. **"Uppdaterar..." visas. Avvakta i 1 eller 2 minuter och klicka sedan på [OK].**

   Om den föregående skärmbilden inte visas igen när du klickar på [OK], vänta en stund och klicka sedan på uppdateringsknappen i webbläsaren.
7. **Logga ut.**

Aktivera och avaktivera protokoll

Ange om du ska aktivera eller avaktivera funktionen för varje protokoll. Genom att göra den här inställningen kan du ange vilka protokoll som ska vara tillgängliga och därmed förhindra obehörig åtkomst över nätverket. Nätverksinställningar kan anges på kontrollpanelen eller med Web Image Monitor, telnet, Device Manager NX eller Remote Communication Gate S.

Protokoll	Port	Inställningsmetod	När avaktiverad
IPv4	-	• Kontrollpanel • Web Image Monitor • Telnet	Alla program som körs över IPv4 kan inte användas. Om du använder IPv4-överföring kan det inte inaktiveras med Web Image Monitor.
IPv6	-	• Kontrollpanel • Web Image Monitor • Telnet	Alla program som används över IPv6 kan inte användas.
IPsec	-	• Kontrollpanel • Web Image Monitor • Telnet	Krypterad överföring med IPsec är avaktiverad.
FTP	TCP:21	• Web Image Monitor • Telnet • Device Manager NX • Remote Communication Gate S	Funktioner som kräver FTP kan inte användas. Du kan hindra att personlig information visas genom att göra inställningar på kontrollpanelen med "Begränsa visning av användarinformation".
ssh/sftp	TCP:22	• Web Image Monitor • Telnet • Device Manager NX • Remote Communication Gate S	Funktioner som kräver sftp kan inte användas. Du kan hindra att personlig information visas genom att göra inställningar på kontrollpanelen med "Begränsa visning av användarinformation".
telnet	TCP:23	• Web Image Monitor • Device Manager NX	Kommandon som använder telnet är avaktiverade.

Protokoll	Port	Inställningsmetod	När avaktiverad
SMTP	TCP:25 (variabel)	• Kontrollpanel • Web Image Monitor • Device Manager NX • Remote Communication Gate S	Funktioner för e-postmeddelanden som kräver SMTP-mottagning kan inte användas.
HTTP	TCP:80	• Web Image Monitor • Telnet	Funktioner som kräver HTTP kan inte användas. Kan inte skriva ut med IPP på port 80.
HTTPS	TCP:443	• Web Image Monitor • Telnet	Funktioner som kräver HTTPS kan inte användas. @Remote kan inte användas. Du kan också göra inställningar så att det krävs SSL-överföring för att använda kontrollpanelen eller Web Image Monitor.
SMB	TCP:139	• Kontrollpanel • Web Image Monitor • Telnet • Device Manager NX • Remote Communication Gate S	SMB-utskriftsfunktioner kan inte användas.
NBT	UDP:137 UDP:138	• Telnet	SMB-utskriftsfunktioner via TCP/IP kan inte användas, inte heller NetBIOS-funktioner på WINS-servern.
SNMPv1,v2	UDP:161	• Web Image Monitor • Telnet • Device Manager NX • Remote Communication Gate S	Funktioner som kräver SNMPv1, v2 kan inte användas. Med kontrollpanelen, Web Image Monitor eller Telnet kan du ange att inställningar för SNMPv1, v2 är skrivskyddade och därmed inte redigerbara.

Protokoll	Port	Inställningsmetod	När avaktiverad
SNMPv3	UDP:161	• Web Image Monitor • Telnet • Device Manager NX • Remote Communication Gate S	Funktioner som kräver SNMPv3 kan inte användas. Du kan också ange inställningar för att kräva SNMPv3-krypterad överföring och begränsa användningen av andra överföringsmetoder genom kontrollpanelen, Web Image Monitor eller telnet.
RSH/RCP	TCP:514	• Web Image Monitor • Telnet • Device Manager NX • Remote Communication Gate S	Funktioner som kräver RSH-funktion kan inte användas. Du kan hindra att personlig information visas genom att göra inställningar på kontrollpanelen med "Begränsa visning av användarinformation".
LPR	TCP:515	• Web Image Monitor • Telnet • Device Manager NX • Remote Communication Gate S	LPR-funktioner kan inte användas. Du kan hindra att personlig information visas genom att göra inställningar på kontrollpanelen med "Begränsa visning av användarinformation".
IPP	TCP:631	• Web Image Monitor • Telnet • Device Manager NX • Remote Communication Gate S	IPP-funktioner kan inte användas.
SSDP	UDP:1900	• Web Image Monitor • Telnet	Enhetsidentifiering med UPnP från Windows kan inte användas.
Bonjour	UDP:5353	• Web Image Monitor • Telnet	Bonjour-funktioner kan inte användas.
@Remote	TCP:7443 TCP:7444	• Kontrollpanel • Telnet	@Remote kan inte användas.

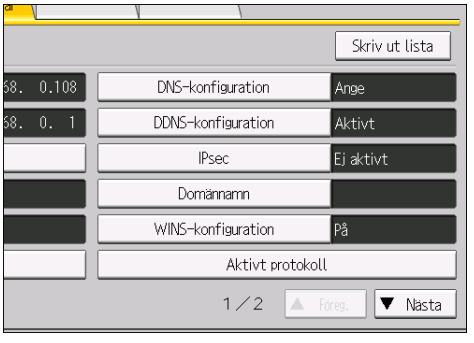
Protokoll	Port	Inställningsmetod	När avaktiverad
DIPRINT	TCP:9100	• Web Image Monitor • Telnet • Device Manager NX • Remote Communication Gate S	DIPRINT-funktioner kan inte användas.
RFU	TCP:10021	• Kontrollpanel • Telnet	Du kan uppdatera firmware via FTP.
NetWare	(IPX/SPX)	• Kontrollpanel • Web Image Monitor • Telnet • Device Manager NX • Remote Communication Gate S	Kan inte skriva ut med NetWare. SNMP över IPX kan inte användas.
WSD (Enhet)	TCP:53000 (variabel)	• Web Image Monitor • Telnet	WSD-funktioner (enhet) kan inte användas.
WSD (Skrivare)	TCP:53001 (variabel)	• Web Image Monitor • Telnet	WSD-funktioner (skrivare) kan inte användas.
	(variabel)		
WS-Discovery	UDP/TCP: 3702	• Telnet	WSD (enhet, skrivare)-sökfunktion kan inte användas.
RHPP	TCP:59100	• Web Image Monitor • Telnet	Kan inte skriva ut med RHPP.
LLTD	-	• Telnet	Funktionen enhetssökning med hjälp av LLTD kan inte användas.
LLMNR	UDP:5355	• Web Image Monitor • Telnet	Förfrågningar om namnmatchning med hjälp av LLMNR kan inte besvaras.

Obs

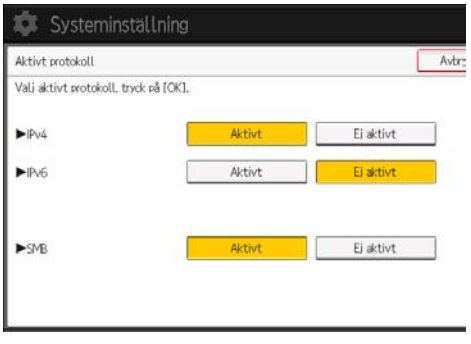
- "Begränsa visning av användarinformation" är en av funktionerna för Utökad säkerhet. Information om hur du anger den här inställningen finns i s. 193 "Ange Utökade säkerhetsfunktioner".

Aktivera och avaktivera protokoll med kontrollpanelen

1. Logga in som nätverksadministratör via kontrollpanelen.
2. Tryck på [Systeminställning].
3. Tryck på [Gränssnittsinst].
4. Tryck på [Aktivt protokoll].



5. Välj vilket protokoll du vill aktivera eller inaktivera.



6. Tryck på [OK].
7. Logga ut.

Aktivera och avaktivera protokoll med Web Image Monitor

1. Logga in som nätverksadministratör från Web Image Monitor.
2. Peka på [Enhetshantering] och klicka sedan på [Konfiguration].
3. Klicka på [Nätverkssäkerhet] under "Säkerhet".
4. Välj vilket protokoll du vill aktivera eller inaktivera, eller välj vilken port du vill öppna eller stänga.
5. Klicka på [OK].

6. **"Uppdaterar..." visas. Avvakta i 1 eller 2 minuter och klicka sedan på [OK].**

   Om den föregående skärmbilden inte visas igen när du klickar på [OK], vänta en stund och klicka sedan på uppdateringsknappen i webbläsaren.

7. **Logga ut.**

Ange Säkerhetsnivåer för nätverk

Inställningen låter dig ändra säkerhetsnivåerna så att obehörig åtkomst begränsas. Du kan konfigurera säkerhetsnivåinställningarna för nätverk via kontrollpanelen eller via Web Image Monitor. Observera att de protokoll som kan anges skiljer sig åt.

Viktigt

- **Med vissa verktyg kan kommunikation eller inloggning misslyckas beroende på nätsäkerhetsnivån.**

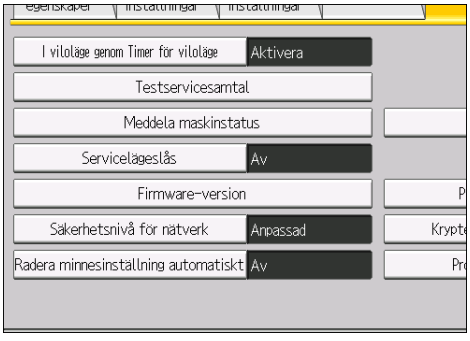
Nätverkssäkerhetsnivåer

Säkerhetsnivå	Beskrivning
[Nivå 0]	Välj [Nivå 0] för att använda alla funktioner. Använd den här inställningen när du inte har någon information som behöver skyddas utifrån.
[Nivå 1]	Välj [Nivå 1] för måttlig säkerhet för att skydda viktig information. Använd den här inställningen om maskinen är ansluten till ett trådlöst lokalt nätverk (LAN).
[FIPS140]	Ger en säkerhetsstyrka mellan [Nivå 1] och [Nivå 2]. Du kan endast använda koder som har rekommenderats av myndigheterna i USA och dess kodnings-/autentiseringsalgoritm. Övriga inställningar än samma som för [Nivå 2].
[Nivå 2]	Välj [Nivå 2] för maximalt skydd av konfidentiell information. Använd den här inställningen när det är nödvändigt att skydda informationen utifrån.
[Anpassad]	För konfigurationer utöver nivåerna ovan. Konfigurera med Web Image Monitor.

Ange nätverkets säkerhetsnivåer via kontrollpanelen

1. **Logga in som nätverksadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa] två gånger.**

5. **Tryck på [Säkerhetsnivå för nätverk].**



6. **Välj den säkerhetsnivå för nätverket som du vill ha.**

   Välj [Nivå 0], [Nivå 1], [Nivå 2] eller [FIPS140].

7. **Tryck på [OK].**
8. **Logga ut.**

Ange nätverkets säkerhetsnivå med Web Image Monitor.

1. **Logga in som nätverksadministratör från Web Image Monitor.**
2. **Peka på [Enhetshantering] och klicka sedan på [Konfiguration].**
3. **Klicka på [Nätverkssäkerhet] under "Säkerhet".**
4. **Välj säkerhetsnivå för nätverket i "Säkerhetsnivå".**
5. **Klicka på [OK].**
6. **"Uppdaterar..." visas. Avvakta i 1 eller 2 minuter och klicka sedan på [OK].**

   Om den föregående skärmbilden inte visas igen när du klickar på [OK], vänta en stund och klicka sedan på uppdateringsknappen i webbläsaren.

7. **Logga ut.**

Funktionsstatus på varje nätverkssäkerhetsnivå

TCP/IP

Funktion	Nivå 0	Nivå 1	FIPS 140	Nivå 2
TCP/IP	Aktivt	Aktivt	Aktivt	Aktivt
HTTP> Port 80	Öppen	Öppen	Öppen	Öppen
IPP> Port 80	Öppen	Öppen	Öppen	Öppen

Funktion	Nivå 0	Nivå 1	FIPS 140	Nivå 2
IPP> Port 631	Öppen	Öppen	Stäng (Close)	Stäng (Close)
SSL/TLS> Port 443	Öppen	Öppen	Öppen	Öppen
SSL/TLS> Tillåt kommunikation via SSL/TLS	Chiffertextprioritet	Chiffertextprioritet	Endast chiffertext	Endast chiffertext
SSL/TLS-version> TLS1.2	Aktivt	Aktivt	Aktivt	Aktivt
SSL/TLS-version > TLS1.1	Aktivt	Aktivt	Aktivt	Aktivt
SSL/TLS-version> TLS1.0	Aktivt	Aktivt	Aktivt	Aktivt
SSL/TLS-version > SSL3.0	Aktivt	Aktivt	Ej aktivt	Ej aktivt
Inställning för krypteringsgrad> AES	128bit/ 256bit	128bit/ 256bit	128bit/ 256bit	128bit/ 256bit
Inställning för krypteringsgrad> 3DES	168bit	168bit	168bit	-
Inställning för krypteringsgrad>RC4	-	-	-	-
DIPRINT	Aktivt	Aktivt	Ej aktivt	Ej aktivt
LPR	Aktivt	Aktivt	Ej aktivt	Ej aktivt
FTP	Aktivt	Aktivt	Aktivt	Aktivt
sftp	Aktivt	Aktivt	Aktivt	Aktivt
ssh	Aktivt	Aktivt	Aktivt	Aktivt
RSH/RCP	Aktivt	Aktivt	Ej aktivt	Ej aktivt
TELNET	Aktivt	Ej aktivt	Ej aktivt	Ej aktivt
Bonjour	Aktivt	Aktivt	Ej aktivt	Ej aktivt
SSDP	Aktivt	Aktivt	Ej aktivt	Ej aktivt
SMB	Aktivt	Aktivt	Ej aktivt	Ej aktivt
NetBIOS över TCP/IPv4	Aktivt	Aktivt	Ej aktivt	Ej aktivt
WSD (enhet)	Aktivt	Aktivt	Aktivt	Aktivt
WSD (Skrivare)	Aktivt	Aktivt	Aktivt	Aktivt

Funktion	Nivå 0	Nivå 1	FIPS 140	Nivå 2
WSD (krypterad kommunikation för enhet)	Ej aktivt	Ej aktivt	Aktivt	Aktivt
RHPP	Aktivt	Aktivt	Ej aktivt	Ej aktivt

Samma inställningar tillämpas på IPv4 och IPv6.

TCP-/IP-inställningen kontrolleras inte av säkerhetsnivån. Ange om den här inställningen ska aktiveras eller avaktiveras manuellt.

NetWare

Funktion	Nivå 0	Nivå 1	FIPS 140	Nivå 2
NetWare	Aktivt	Aktivt	Ej aktivt	Ej aktivt

Om NetWare inte används i nätverket gäller inte följande inställningar.

SNMP

Funktion	Nivå 0	Nivå 1	FIPS 140	Nivå 2
SNMP	Aktivt	Aktivt	Aktivt	Aktivt
Tillåt inställningar via SNMPv1 och v2	På	Av	Av	Av
Funktion SNMPv1,v2	Aktivt	Aktivt	Ej aktivt	Ej aktivt
Funktion SNMPv3	Aktivt	Aktivt	Aktivt	Aktivt
Tillåt SNMPv3-kommunikation	Krypterat/ Okrypterat	Krypterat/ Okrypterat	Endast kryptering	Endast kryptering

TCP/IP krypteringsgrad

Funktion	Nivå 0	Nivå 1	FIPS 140	Nivå 2
ssh > Encryption Algorithm	DES/3DES/ AES-128/ AES-192/ AES-256/ Blowfish/ Arcfour	3DES/ AES-128/ AES-192/ AES-256/ Arcfour	3DES/ AES-128/ AES-192/ AES-256	3DES/ AES-128/ AES-192/ AES-256

Funktion	Nivå 0	Nivå 1	FIPS 140	Nivå 2
SNMPv3 > Autentiseringsalgoritm	MD5	SHA1	SHA1	SHA1
SNMPv3 > Encryption Algorithm	DES	DES	AES-128	AES-128
Kerberos-autentisering > Encryption Algorithm	AES256-CTS-HMAC-SHA1-96/ AES128-CTS-HMAC-SHA1-96/ DES3-CBC-SHA1/RC4-HMAC/DES-CBC-MD5	AES256-CTS-HMAC-SHA1-96/ AES128-CTS-HMAC-SHA1-96/ DES3-CBC-SHA1/RC4-HMAC	AES256-CTS-HMAC-SHA1-96/ AES128-CTS-HMAC-SHA1-96/ DES3-CBC-SHA1	AES256-CTS-HMAC-SHA1-96/ AES128-CTS-HMAC-SHA1-96
Krypteringskod för drivrutin > Krypteringsgrad	Enkel kryptering	DES	AES	AES

Skydda kommunikationsvägar via ett enhetscertifikat

Den här maskinen kan skydda sina kommunikationsvägar och etablera krypterad kommunikation med hjälp av SSL/TLS, IPsec eller IEEE 802.1X.

För att använda dessa funktioner måste du först skapa och installera ett enhetscertifikat för maskinen.

Följande typer av enhetscertifikat kan användas:

- självsignerat certifikat skapat av maskinen
- Certifikat utfärdat av certifikatutfärdare

Viktigt

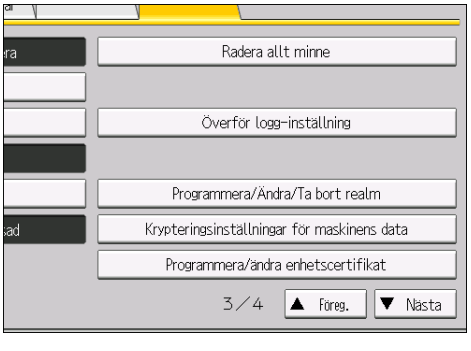
- **Administratören måste hantera utgången av certifikat och förnya certifikat innan de löper ut.**
- **Administratören måste kontrollera certifikatutfärdarens giltighet.**

Skapa och installera ett enhetscertifikat från kontrollpanelen (självsignerat certifikat)

Skapa och installera enhetscertifikatet från kontrollpanelen.

Detta avsnitt beskriver hur man använder ett självsignerat certifikat som enhetscertifikat.

1. **Logga in som nätverksadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck 3 gånger på [▼Nästa].**
5. **Tryck på [Programmera/ändra enhetscertifikat].**



6. **Kontrollera att [Programmera] är valt.**
7. **Tryck på [Certifikat 1].**

   Endast [Certifikat 1] kan skapas från kontrollpanelen.

8. **Konfigurera nödvändiga inställningar.**
9. **Tryck på [OK].**

   "Installerad" visas under "Certifikatsstatus" för att visa att ett enhetscertifikat för maskinen har installerats.
10. **Logga ut.**

Obs

- Välj [Radera] för att radera enhetscertifikatet från maskinen.

Skapa och installera ett enhetscertifikat från Web Image Monitor (självsignerat certifikat)

Skapa och installera enhetscertifikatet med Web Image Monitor. Mer information om visade och valbara poster finns i Web Image Monitors Hjälp.

Detta avsnitt beskriver hur man använder ett självsignerat certifikat som enhetscertifikat.

1. **Logga in som nätverksadministratör från Web Image Monitor.**
2. **Peka på [Enhetshantering] och klicka sedan på [Konfiguration].**
3. **Klicka på [Enhetens certifikat] under"Säkerhet".**
4. **Kontrollera alternativknappen bredvid antalet certifikat du vill skapa.**

   För att använda SSL/TLS, välj [Certifikat 1]. För att använda något annat protokoll väljer du det certifikatnummer du vill använda.
5. **Klicka på [Skapa].**

   Klicka på [Ta bort] för att ta bort enhetscertifikatet från maskinen.
6. **Konfigurera nödvändiga inställningar.**
7. **Klicka på [OK].**

   Inställningen ändras.
8. **Klicka på [OK].**
9. **Om en säkerhetsvarning visas, kontrollera informationen och välj sedan "Fortsätt till denna webbplats".**

   "Installerad" visas under "Certifikatsstatus" för att visa att ett enhetscertifikat för maskinen har installerats.
10. **Logga ut.**

Skapa ett enhetscertifikat (utfärdat av en certifikatutfärdare)

Skapa enhetscertifikatet med Web Image Monitor. Mer information om visade och valbara poster finns i Web Image Monitors Hjälp.

Detta avsnitt beskriver användningen av ett certifikat utfärdat av en certifikatutfärdare, som enhetscertifikat.

1. **Logga in som nätverksadministratör från Web Image Monitor.**
2. **Peka på [Enhetshantering] och klicka sedan på [Konfiguration].**
3. **Klicka på [Enhetens certifikat] under"Säkerhet".**
4. **Kontrollera alternativknappen bredvid antalet certifikat du vill skapa.**

   För att använda SSL/TLS, välj [Certifikat 1]. För att använda något annat protokoll väljer du det certifikatnummer du vill använda.
5. **Klicka på [Ansökan].**
6. **Konfigurera nödvändiga inställningar.**
7. **Klicka på [OK].**

   Inställningen ändras.
8. **Klicka på [OK].**

   "Ansöker" visas för "Certifikatsstatus".
9. **Logga ut.**
10. **Ansök hos certifikatutfärdaren om enhetscertifikatet.**

    Ansökningsprocessen beror på certifikatsutfärdaren. Kontakta utfärdaren för närmare information.

    För programmet, klicka på Web Image Monitor Information och använd informationen som visas under "Certifikatinformation".

Obs

- Utfärdandeplatsen kanske inte visas om du ansöker om 2 certifikat samtidigt. När du installerar ett certifikat, se till att kontrollera certifikatets mål och installationsprocess.
- Web Image Monitor kan användas för att skapa enhetens certifikat, men inte för att begära certifikatet från certifikatutfärdaren.
- Klicka på [Avbryt ansökan] för att avbryta ansökan om enhetscertifikatet.

Installation av ett enhetscertifikat (utfärdat av en certifikatutfärdare)

Installera enhetscertifikatet med Web Image Monitor. Mer information om visade och valbara poster finns i Web Image Monitors Hjälp.

Detta avsnitt beskriver användningen av ett certifikat utfärdat av en certifikatutfärdare, som enhetscertifikat.

Ange enhetscertifikatets innehåll som är utfärdat av certifikatutfärdaren.

1. **Logga in som nätverksadministratör från Web Image Monitor.**
2. **Peka på [Enhetshantering] och klicka sedan på [Konfiguration].**
3. **Klicka på [Enhetens certifikat] under"Säkerhet".**
4. **Kryssa för alternativknappen bredvid numret på det certifikat du vill installera.**

   För att använda SSL/TLS, välj [Certifikat 1]. För att använda något annat protokoll väljer du det certifikatnummer du vill använda.
5. **Klicka på [Installera].**
6. **Ange enhetscertifikatets innehåll.**

   I certifikatsrutan anger du innehållet i enhetens certifikat som du fått från certifikatsutfärdaren.

   Om du installerar ett mellanliggande certifikat, ange även innehållet i det mellanliggande certifikatet.

   Mer information om visade och valbara poster finns i Web Image Monitors Hjälp.
7. **Klicka på [OK].**
8. **Avvakta i 1 eller 2 minuter och klicka sedan på [OK].**

   "Installerad" visas under "Certifikatsstatus" för att visa att ett enhetscertifikat för maskinen har installerats.
9. **Logga ut.**

Installera ett mellanliggande certifikat (utfärdat av en certifikatutfärdare)

Det här avsnittet förklarar hur du använder Web Image Monitor för att istallera ett mellanliggande certifikat utfärdat av en certifikatutfärdare.

Om du inte har det mellanliggande certifikatet utfärdat av en certifikatutfärdare kommer ett varningsmeddelande att visas under kommunikationen. Om certifikatutfärdaren har utfärdat ett mellanliggande certifikat, rekommenderar vi att du installerar det mellanliggande certifikatet.

1. **Logga in som nätverksadministratör från Web Image Monitor.**
2. **Peka på [Enhetshantering] och klicka sedan på [Konfiguration].**
3. **Klicka på [Enhetens certifikat] under"Säkerhet".**
4. **Kryssa för alternativknappen bredvid numret på det certifikat du vill installera.**
5. **Klicka på [Installera mellanliggande certifikat].**

6. **Ange innehållet i det mellanliggande certifikatet.**

   I certifikatsrutan anger du innehållet i det mellanliggande certifikat som du fått från certifikatutfärdaren. För mer information om de poster som visas samt inställningar, se Web Image Monitors Hjälp.

7. **Klicka på [OK].**

8. **Avvakta i 1 eller 2 minuter och klicka sedan på [OK].**

   Det mellanliggande certifikatet kommer att installeras på enheten. Skärmen "Certifikatinformation" kommer att indikera om det mellanliggande certifikatet har installerats eller inte. För information om skärmen "Certifikatinformation", se hjälpen till Web Image Monitor.

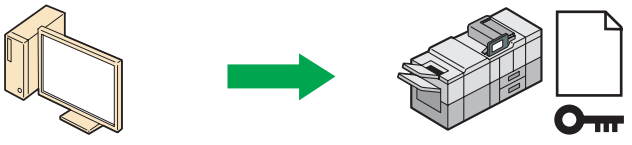
9. **Logga ut.**

Konfigurera inställningar för SSL/TLS

Att konfigurera maskinen för att använda SSL/TLS gör det möjligt att kryptera kommunikation. Genom att göra det förhindrar du att data fångas upp, knäcks eller manipuleras under överföringen.

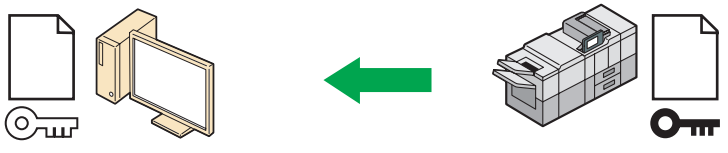
Flöde av SSL/TLS-krypterad kommunikation

1. För att få åtkomst till maskinen från en användares dator, be om SSL/TLS-enhetscertifikat och publik nyckel.



CZB002

2. Enhetens certifikat och publik nyckel sänds från maskinen till användarens dator.



CZB003

3. Den delade nyckel som skapats med datorn krypteras med den publika nyckeln, som skickas till maskinen och avkrypteras med den privata nyckeln i maskinen.

CZB004

4. Den delade nyckeln används för kryptering och dekryptering av data och därigenom uppnås säker överföring.

CZB005

Konfigurationsflöde vid användning av ett självsignerat certifikat

1. Skapa och installera enhetscertifikatet:

Skapa och installera ett enhetscertifikat från kontrollpanelen eller Web Image Monitor.

2. Aktivera SSL/TLS:

   Aktivera SSL-/TLS-inställningen med hjälp av Web Image Monitor.

Konfigurationsflöde vid användning av certifikat från certifikatutfärdare

1. Skapa ett enhetscertifikat och ansök hos utfärdaren:

   Efter att du har skapat ett enhetscertifikat i Web Image Monitor, ansök hos certifikatutfärdare.

   Hantering av program efter skapandet av certifikatet beror på certifikatsutfärdaren. Följ instruktionerna från utfärdaren av certifikatet.

2. Installera enhetscertifikatet:

   Installera enhetscertifikatet med Web Image Monitor.

3. Aktivera SSL/TLS:

   Aktivera SSL-/TLS-inställningen med hjälp av Web Image Monitor.

Obs

- Du kontrollerar att SSL/TLS-konfigurationen är aktiverad genom att ange "https://(maskinens IP-adress eller värdnamn)/" i adressfältet på din webbläsare för att få åtkomst till den här maskinen. Om meddelandet "Sidan kan inte visas" kommer upp är den aktuella SSL/TLS-konfigurationen ogiltig. Kontrollera konfigurationen.
- Om du aktiverar SSL/TLS för IPP (skrivarfunktioner) krypteras skickade data, vilket förhindrar att de fångas upp, analyseras eller manipuleras.

Aktivera SSL/TLS

Efter att enhetscertifikatet har installerats i maskinen, aktivera SSL/TLS-inställningen.

Gör på följande sätt för ett självsignerat certifikat eller ett certifikat utfärdat av en certifikatsutfärdare.

1. **Logga in som nätverksadministratör från Web Image Monitor.**
2. **Peka på [Enhetshantering] och klicka sedan på [Konfiguration].**
3. **Klicka på [SSL/TLS] under "Säkerhet".**
4. **För IPv4 och IPv6 väljer du "Aktivt" om du vill aktivera SSL/TLS.**
5. **Ställ krypteringskommunikationsläget på "Tillåt kommunikation via SSL/TLS".**
6. **Om du vill avaktivera ett protokoll klickar du på [Ej aktivt] bredvid "TLS1.2", "TLS1.1", "TLS1.0", eller "SSL3.0".**

   Minst ett av dessa protokoll måste vara aktiverat.

7. **Under "Inställning för krypteringsgrad" anger du den krypteringssgrad som ska tillämpas för "AES", "3DES", och/eller "RC4". Du måste välja minst en kryssruta.**

   Observera att tillgängliga krypteringsgrader varierar beroende på vilka inställningar du har angett för "TLS1.2", "TLS1.1", "TLS1.0" eller "SSL3.0".

8. **Klicka på [OK].**
9. **"Uppdaterar..." visas. Avvakta i 1 eller 2 minuter och klicka sedan på [OK].**

   Om den föregående skärmbilden inte visas igen när du klickar på [OK], vänta en stund och klicka sedan på uppdateringsknappen i webbläsaren.

10. **Logga ut.**

Obs

- När "Tillåt kommunikation via SSL/TLS" står på [Endast chiffertext] är kommunikation inte möjlig om du väljer ett protokoll som inte stödjer en webbläsare eller anger endast en inställning för krypteringsgrad. Om så är fallet aktivera kommunikation genom att ange [Tillåt kommunikation via SSL/TLS] till [Chiffertxt/Okrypt. Txt] på maskinens kontrollpanel och ange sedan rätt protokoll och krypteringsnivå.
- Inställningar för SSL/TLS-version och krypteringsnivå kan även ändras under [Nätverkssäkerhet].
- Beroende på tillstånden du anger för "TLS1.2", "TLS1.1", "TLS1.0" och "SSL3.0", kan maskinen kanske inte ansluta till en extern LDAP-server.
- Följande typer av kommunikation och information krypteras alltid via SSL3.0: kommunikation via @Remote och loggar överförda till Remote Communication Gate S.

Användarinställning för SSL/TLS

Vi rekommenderar att du efter installation av ett självsignerat certifikatet eller enhetscertifikat från en privat certifikatsutfärdare på en huvudenhet, och efter aktivering av SSL/TLS (kommunikationskryptering) instruerar användare att installera certifikatet på sina datorer. Det är särskilt viktigt för användare som skriver ut via IPP-SSL från Windows Vista/7/8/8.1 och Windows Server 2008/2008 R2/2012/2012 R2 att installera certifikatet. Nätverksadministratören måste uppmana samtliga användare att installera certifikatet.

Välj [Betrodda rotcertifikatutfärdare] för lagringsplats för certifikatet vid åtkomst till maskinen via IPP.

Obs

- Vidta lämpliga åtgärder när du får en fråga från en användare angående problem som ett utgånget certifikat.
- Om ett certifikat utfärdat av en certifikatutfärdare är installerat på maskinen, kontrollera certifikatets lagringsplats med certifikatutfärdaren.
- För att ändra värdnamnet eller IP-adressen i [Nätverksnamn] för enhetscertifikatet när du använder operativsystemets standard-IPP-port i Windows Vista/7/8/8.1 eller Windows Server

2008/2008 R2/2012/2012 R2, tar du först bort den tidigare konfigurerade PC-skrivaren och installerar den igen efter ändring av [Nätverksnamn]. För att även ändra inställningar för användarautentisering (användarnamn och lösenord), ta först bort den tidigare konfigurerade PC-skrivaren och installera den igen när autentiseringsinställningarna har ändrats.

Ange SLL-/TLS-krypteringsläge

Genom att ange SSL-/TLS-krypterat kommunikationsläge kan du ändra säkerhetsnivåer.

Krypterat kommunikationsläge

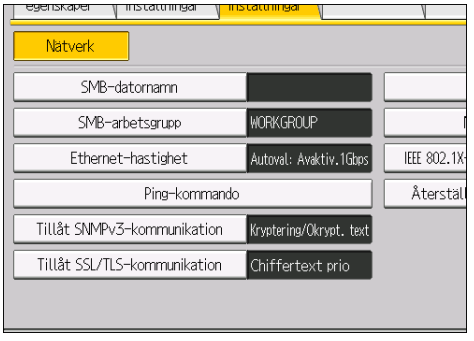
Genom att använda krypterat kommunikationsläge kan du ange krypterad kommunikation.

Krypterat kommunikationsläge	Beskrivning
Endast chiffertext	Tillåter enbart krypterad kommunikation. Om kryptering inte är möjlig kommunicerar inte maskinen.
Chiffertextprioritet	Utför krypterad kommunikation när detta är möjligt. Om kryptering inte är möjlig kommunicerar skrivaren utan kryptering.
Chiffertxt/Okrypt. Txt	Kommunicerar med eller utan kryptering enligt inställningen.

När du har installerat ett enhetscertifikat anger du det SSL-/TLS-krypterade kommunikationsläget. Genom att konfigurera den här inställningen kan du ändra säkerhetsnivån.

1. **Logga in som nätverksadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Gränssnittsinst].**
4. **Tryck på [▼Nästa].**

5. **Tryck på [Tillåt SSL/TLS-kommunikation].**



6. **Välj det krypterade kommunikationsläget som du vill använda.**

   Välj [Endast chiffertext], [Chiffertext prioritet] eller [Chiffertext/Okrypterad text] som krypterat kommunikationsläge.

7. **Tryck på [OK].**

8. **Logga ut.**

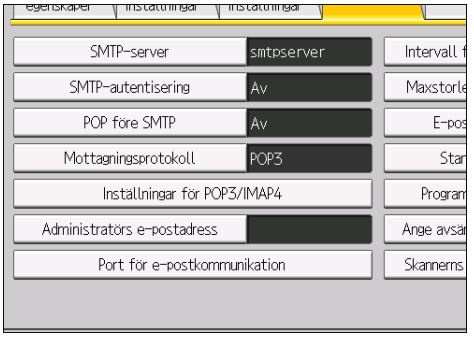
Obs

- SSL-/TLS-krypterat kommunikationsläge kan också anges via Web Image Monitor. För mer information, se hjälpen till Web Image Monitor.

Aktivera SSL för SMTP-anslutningar

Använd följade metod för att aktivera SSL-kryptering för SMTP-anslutningar.

1. **Logga in som nätverksadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Filöverföring].**
4. **Tryck på [SMTP-server].**



5. **I "Använd säker anslutning (SSL)", tryck på [På].**

   Om du inte använder SSL för SMTP-anslutning, tryck på [Av].

   När "Använd säker anslutning (SSL)" är ställt till [På] ändras portnumret till 465.

6. **Tryck på [OK].**

7. **Logga ut.**

Konfigurera IPsec-inställningar

För kommunikationssäkerhetens skull stöder den här maskinen IPsec. IPsec överför säkra datapaket på IP-protokollnivå med krypteringsmetoden dela kod, där både avsändare och mottagare behåller samma kod. Den här maskinen använder automatiskt kodbyte för att konfigurera den delade koden för båda parter. Med inställningen för automatiskt byte kan du förnya de delade kodbytesinställningarna inom en angiven giltighetsperiod och uppnå högre säkerhet vid överföring.

Viktigt

- **När "Inaktiv" anges för "Uteslut HTTPS-kommunikation" kan åtkomst till Web Image Monitor gå förlorad om huvudinställningarna inte är korrekt konfigurerade. För att förhindra det kan du ange IPsec så att HTTPS-överföring utesluts genom att välja "Aktiv". När du vill inkludera HTTPS-överföring rekommenderar vi att du väljer "Inaktiv" för "Uteslut HTTPS-kommunikation" när du bekräftat att IPsec är korrekt konfigurerat. När "Aktiv" har valts för "Uteslut HTTPS-kommunikation", även om HTTPS-överföring inte riktas av IPsec, kan Web Image Monitor bli oanvändbart när TCP riktas av IPsec från datorsidan.**
- **Om du inte har åtkomst till Web Image Monitor pga IPsec-konfigurationsproblem, avaktiverar du Systeminställning på kontrollpanelen och går sedan till Web Image Monitor.**
- **För mer information om hur du aktiverar och inaktiverar IPsec via kontrollpanelen, se Connecting the Machine/ System Settings.**
- **IPsec tillämpas inte på data som erhållits genom DHCP, DNS eller WINS.**

Operativsystem som stöds

Operativsystem	OBS!
• Windows Server 2003/2003 R2	IPsec över IPv4 kan användas.
• Windows Vista/7/8/8.1 • Windows Server 2008/2008 R2/2012/2012 R2 • Mac OS X 10.4.8 eller senare • Red Hat Enterprise Linux WS 4.0 • Solaris 10	IPsec över både IPv4 och IPv6 kan användas.

Vissa inställningsobjekt stöds inte beroende på operativsystemet. Se till att de IPsec-inställningar du har angivit stämmer överens med operativsystemets IPsec-inställningar.

Kryptering och autentisering av IPsec

IPsec består av 2 huvudfunktioner: krypteringsfunktionen som säkerställer att data förblir konfidentiell och autentiseringsfunktionen som verifierar datans avsändare samt dataintegriteten. Den här maskinens

IPsec-funktion stöder 2 säkerhetsprotokoll: ESP-protokoll som aktiverar båda IPsec-funktionerna samtidigt och AH-protokoll som enbart aktiverar autentiseringsfunktionen.

">ESP-protokoll

ESP-protokollet tillhandahåller säker överföring genom både kryptering och autentisering. Det här protokollet tillhandahåller inte rubrikautentisering.

- För att krypteringen ska lyckas måste både avsändaren och mottagaren ange samma krypteringsalgoritm och krypteringskod. Om du använder metoden för automatiskt byte av krypteringskod anges krypteringsalgoritmen och krypteringskoden automatiskt.
- För att autentiseringen ska lyckas måste avsändaren och mottagaren ange samma autentiseringsalgoritm och autentiseringskod. Om du använder metoden för automatiskt byte av krypteringskod, anges autentiseringsalgoritmen och autentiseringskoden automatiskt.

AH-protokoll

AH-protokollet ger säker överföring enbart genom autentisering av paket, inklusive rubriker.

- För att autentiseringen ska lyckas måste avsändaren och mottagaren ange samma autentiseringsalgoritm och autentiseringskod. Om du använder metoden för automatiskt byte av krypteringskod, anges autentiseringsalgoritmen och autentiseringskoden automatiskt.

AH-protokoll + ESP-protokoll

När ESP- och AH-protokollen kombineras tillhandahåller de säker överföring genom både kryptering och autentisering. Dessa protokoll tillhandahåller rubrikautentisering.

- För att krypteringen ska lyckas måste både avsändaren och mottagaren ange samma krypteringsalgoritm och krypteringskod. Om du använder metoden för automatiskt byte av krypteringskod anges krypteringsalgoritmen och krypteringskoden automatiskt.
- För att autentiseringen ska lyckas måste avsändaren och mottagaren ange samma autentiseringsalgoritm och autentiseringskod. Om du använder metoden för automatiskt byte av krypteringskod, anges autentiseringsalgoritmen och autentiseringskoden automatiskt.

Obs

- Vissa operativsystem använder termen Överensstämmelse istället för Autentisering.

Inställningar för automatiskt byte av krypteringsnycklar

För konfigurering av kod stödjer den här maskinen automatiskt kodutbyte för att ange överenskommelser som IPsec-algoritmen och kod för både avsändare och mottagare. Sådana överensstämmelser utgör det som är känt som SA (säkerhetsassociation). IPsec-kommunikation är möjlig endast om mottagarens och avsändarens SA-inställningar är identiska.

Om du använder metoden för automatiskt byte för att ange krypteringskoden, konfigureras SA-inställningarna automatiskt på båda parternas maskiner. Innan du ställer in IPsec SA autokonfigureras även inställningarna för ISAKMP SA (Fas 1). Efter detta autokonfigureras inställningarna för IPsec SA (fas 2), som gör faktisk IPsec-överföring möjlig.

För ytterligare säkerhet kan SA periodvis uppdateras automatiskt genom att man tillämpar en giltighetsperiod (tidsbegränsning) för dess inställningar. Den här maskinen stöder endast IKEv1 för automatiskt byte av krypteringskod.

Observera att det är möjligt att konfigurera flera SA:s.

Inställningar 1-4 och standardinställning

Med hjälp av metoden automatiskt utbyte, kan du konfigurera fyra separata uppsättningar SA-detaljer (så som olika delade koder och IPsec-algoritmer. I standardinställningarna för dessa uppsättningar kan du ta med inställningar som fälten för uppsättning 1 till 4 inte kan innehålla.

När IPsec är aktiverat har uppsättning 1 högsta prioritet och uppsättning 4 har den lägsta. Du kan använda detta prioriteringssystem för att sätta IP-adresser som mål på ett mer säkert sätt. Ställ till exempel in det bredaste IP-intervallet på lägsta prioritet (4) och ställ sedan in särskilda IP-adresser på en högre prioritetsnivå (3 eller högre). På det sättet kommer de högre inställningarna att tillämpas när IPsec-överföringen aktiveras för en särskild IP-adress.

IPsec-inställningar

IPsec-inställningar för den här maskinen kan göras i Web Image Monitor. Följande tabell förklarar enskilda inställningsposter.

Poster för IPsec-inställningar

Inställning	Beskrivning	Inställningsvärde
IPsec	Ange om du ska aktivera eller avaktivera IPsec.	• Aktivt • Ej aktivt
Uteslut HTTPS-kommunikation	Ange om du ska aktivera IPsec för HTTPS-kommunikation.	• Aktivt • Ej aktivt Ange "Aktiv" om du inte vill använda IPsec för HTTPS-kommunikation.

IPsec-inställningen kan även konfigureras från kontrollpanelen.

Säkerhetsnivå för automatiskt byte av krypteringsnycklar

När du väljer säkerhetsnivå konfigureras vissa säkerhetsinställningar automatiskt. Följande tabell förklarar säkerhetsnivåernas egenskaper.

Säkerhetsnivå	Egenskaper för säkerhetsnivå
Enbart autentisering	Välj den här nivån om du vill autentisera överföringspartnern och förhindra obehörig datamanipulering, men inte utföra kryptering av datapaket. Eftersom data skickas som okrypterad text är datapaket sårbara för avlyssning. Välj inte detta om du håller på att utbyta känslig information.
Autentisering och låg krypteringsnivå	Välj den här nivån om du vill kryptera datapaketen och även autentisera överföringspartnern och förhindra obehörig paketmanipulering. Paketkryptering hjälper till att förhindra tjuvlyssningsattacker. Den här nivån tillhandahåller mindre säkerhet än "Autentisering och hög krypteringsnivå".
Autentisering och hög krypteringsnivå	Välj den här nivån om du vill kryptera datapaketen och även autentisera överföringspartnern och förhindra obehörig paketmanipulering. Paketkryptering hjälper till att förhindra tjuvlyssningsattacker. Den här nivån ger större säkerhet än "Autentisering och låg krypteringsnivå".

Följande tabell är en lista över inställningar som automatiskt konfigureras i enligt säkerhetsnivån.

Inställning	Enbart autentisering	Autentisering och låg krypteringsnivå	Autentisering och hög krypteringsnivå
Säkerhetspolicy	Använd	Använd	Använd
Inkapslingsläge	Transport	Transport	Transport
Kravnivå för IPsec	Använd när det är möjligt	Använd när det är möjligt	Alltid nödvändigt
Autentiseringsmetod	PSK	PSK	PSK
Fas 1 Hash-algoritm	MD5	SHA1	SHA256
Fas 1 Krypteringsalgoritm	DES	3DES	AES-128-CBC
Fas 1 Diffie-Hellman-grupp	2	2	2

Inställning	Enbart autentisering	Autentisering och låg krypteringsnivå	Autentisering och hög krypteringsnivå
Fas 2 Säkerhetsprotokoll	AH	ESP	ESP
Fas 2 Autentiseringsalgoritm	HMAC-SHA1-96/ HMAC-SHA256-128/ HMAC-SHA384-192/ HMAC-SHA512-256	HMAC-SHA1-96/ HMAC-SHA256-128/ HMAC-SHA384-192/ HMAC-SHA512-256	HMAC-SHA256-128/ HMAC-SHA384-192/ HMAC-SHA512-256
Fas 2 Rättighet att använda krypteringsalgoritmer	Okrypterad text (NULL-kryptering)	3DES/AES-128/ AES-192/AES-256	AES-128/AES-192/ AES-256
Fas 2 PFS	Ej aktivt	Ej aktivt	2

Inställningsobjekt för automatiskt byte av krypteringsnycklar

När du anger en säkerhetsnivå, konfigureras de motsvarande säkerhetsinställningarna automatiskt men andra inställningar som adresstyp, lokal adress och fjärradress måste fortfarande konfigureras manuellt.

När du har angivit en säkerhetsnivå, kan du fortfarande göra ändringar i de automatiskt konfigurerade inställningarna. När du ändrar en automatiskt konfigurerad inställning övergår säkerhetsnivån automatiskt till "Användarinställningar".

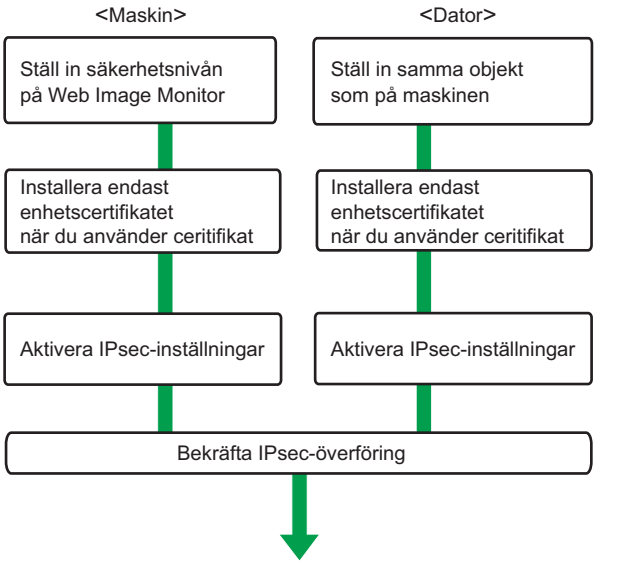
Inställning	Beskrivning	Inställningsvärde
Adresstyp	Ange adresstypen som IPsec-överföringen används för.	• Ej aktivt • IPv4 • IPv6 • IPv4/IPv6 (Endast Standardinställningar)

Inställning	Beskrivning	Inställningsvärde
Lokal adress	Ange maskinens adress. Om du använder flera adresser i IPv6 kan du också ange ett adressintervall.	Maskinens IPv4- eller IPv6-adress. Om du inte ställer in ett adressintervall, ange 32 efter en IPv4-adress eller ange 128 efter en IPv6-adress.
Fjärradress	Ange adressen för IPsec-överföringspartnern. Du kan också ange ett adressintervall.	IPsec-överföringspartnerns IPv4- eller IPv6-adress. Om du inte ställer in ett adressintervall, ange 32 efter en IPv4-adress eller ange 128 efter en IPv6-adress.
Säkerhetspolicy	Ange hur IPsec ska hanteras.	• Använd • Passera • Kassera
Inkapslingsläge	Ange inkapslingsläget. (automatisk inställning)	• Transport • Tunnel Om du anger "Tunnel" måste du också ange "Tunnelns ändpunkter", vilka utgörs av den första och den sista IP-adressen. Ställ in samma adress för begynnelsepunkt som du ställt in för "Lokal adress".
Kravnivå för IPsec	Ange om du bara vill överföra med IPsec eller om du vill tillåta okrypterad överföring när IPsec inte kan etableras. (automatisk inställning)	• Använd när det är möjligt • Alltid nödvändigt

Inställning	Beskrivning	Inställningsvärde
Autentiseringsmetod	Ange metoden för att autentisera överföringspartners. (automatisk inställning)	• PSK • Certificat Om du anger "PSK" måste du även ange PSK-text (med ASCII-tecken). Om du använder "PSK" ska du ange ett PSK lösenord med upp till 32 ASCII-tecken. Om du väljer "Certifikat" måste certifikatet för IPsec installeras och anges innan det kan användas.
Text till PSK (PreShared Key)	Ange den på förhand delade nyckeln för PSK-autentisering.	Ange den på förhand delade koden för PSK-autentisering.
Fas 1 Hash-algoritm	Ange den HASH-algoritm som ska användas i fas 1. (automatisk inställning)	• MD5 • SHA1 • SHA256 • SHA384 • SHA512
Fas 1 Krypteringsalgoritm	Ange krypteringsalgoritmen som ska användas i fas 1. (automatisk inställning)	• DES • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC
Fas 1 Diffie-Hellman-grupp	Ange det Diffie-Hellman-gruppnummer som används för generering av IKE-krypteringsnyckel. (automatisk inställning)	• 1 • 2 • 14
Fas 1 Giltighetsperiod	Ange den tidsperiod då SA-inställningarna i fas 1 ska vara giltiga.	Ange i sekunder från 300 s (5 min) till 172800 s (48 h).

Inställning	Beskrivning	Inställningsvärde
Fas 2 Säkerhetsprotokoll	Ange det säkerhetsprotokoll som ska användas i fas 2. För att använda både kryptering och autentisering på skickad data anger du "ESP" eller "ESP+AH". För att endast använda autentiseringsdata anger du "AH". (automatisk inställning)	• ESP • AH • ESP+AH
Fas 2 Autentiseringsalgoritm	Ange den autentiseringsalgoritm som ska användas i fas 2. (automatisk inställning)	• HMAC-MD5-96 • HMAC-SHA1-96 • HMAC-SHA256-128 • HMAC-SHA384-192 • HMAC-SHA512-256
Fas 2 Rättighet att använda krypteringsalgoritmer	Ange krypteringsalgoritmen som ska användas i fas 2. (automatisk inställning)	• Okrypterad text (NULL-kryptering) • DES • 3DES • AES-128 • AES-192 • AES-256
Fas 2 PFS	Ange om du vill aktivera PFS. Om PFS aktiveras, välj sedan Diffie-Hellmangruppen. (automatisk inställning)	• Ej aktivt • 1 • 2 • 14
Fas 2 Giltighetsperiod	Ange den tidsperiod då SA-inställningarna i fas 2 ska vara giltiga.	Ange en period (i sekunder) från 300 (5 min) till 172 800 (48 h).

Inställningar för automatiskt byte av krypteringsnycklar Konfigurationsflöde



Viktigt

- För att använda ett certifikat för att autentisera överföringspartnern med inställningarna för automatiskt byte av krypteringskod måste ett enhetscertifikat vara installerat.
- När du har konfigurerat IPsec kan du använda Ping-kommandot för att kontrollera om anslutningen är korrekt etablerad. Du kan dock inte använda Ping-kommandot när ICMP är uteslutet från IPsec-överföring på datorns sida. Eftersom maskinen reagerar långsamt under inledande kodbyte kan det ta lite tid att bekräfta att överföringen har etablerats.

Ange Inställningar för automatiskt byte av krypteringsnycklar

För att ändra metoden för automatiskt byte av krypteringskod för en överföringspartner till "Certifikat" måste du först installera och tilldela ett certifikat. Information om hur du skapar och installerar ett enhetscertifikat finns i s. 99 "Skydda kommunikationsvägar via ett enhetscertifikat". För information om hur man tilldelar installerade certifikat till IPsec, se s. 119 "Välja certifikat för IPsec".

1. **Logga in som nätverksadministratör från Web Image Monitor.**
2. **Peka på [Enhetshantering] och klicka sedan på [Konfiguration].**
3. **Klicka på [IPsec] under "Säkerhet".**
4. **Klicka på [Redigera] under "Inställningar för automatiskt byte av krypteringsnycklar".**

5. **Gör inställningar för automatiskt byte av krypteringskod under [Inställningar 1].**

   Om du vill göra flera inställningar, markera antalet inställningar och lägg till inställningar.

6. **Klicka på [OK].**
7. **Välj [Aktivt] vid IPsec: i IPsec.**
8. **Ställ in "Uteslut HTTPS-kommunikation" på [Aktiv] om du inte vill använda IPsec för HTTPS-kommunikation.**
9. **Klicka på [OK].**
10. **"Uppdaterar..." visas. Avvakta i 1 eller 2 minuter och klicka sedan på [OK].**

    Om den föregående skärmbilden inte visas igen när du klickar på [OK], vänta en stund och klicka sedan på uppdateringsknappen i webbläsaren.

11. **Logga ut.**

Välja certifikat för IPsec

Använd Web Image Monitor för att välja det certifikat som ska användas för IPsec. Du måste installera certifikatet innan det kan användas. Information om hur du skapar och installerar ett enhetscertifikat finns i s. 99 "Skydda kommunikationsvägar via ett enhetscertifikat".

1. **Logga in som nätverksadministratör från Web Image Monitor.**
2. **Peka på [Enhetshantering] och klicka sedan på [Konfiguration].**
3. **Klicka på [Enhetens certifikat] under"Säkerhet".**
4. **Välj det certifikat som ska användas för IPsec på listmenyn i "IPsec" under "Certifikat".**
5. **Klicka på [OK].**

   Certifikatet för IPsec har angivits.

6. **"Uppdaterar..." visas. Avvakta i 1 eller 2 minuter och klicka sedan på [OK].**

   Om den föregående skärmbilden inte visas igen när du klickar på [OK], vänta en stund och klicka sedan på uppdateringsknappen i webbläsaren.

7. **Logga ut.**

Ange datorns IPsec-inställningar

Konfigurera datorns IPsec SA-inställningar så att de matchar maskinens säkerhetsnivå exakt. Inställningsmetoderna varierar efter datorns operativsystem. I det här exemplet används Windows 7 när säkerhetsnivån "Autentisering och låg krypteringsnivå" har valts.

1. **På [Start]-menyn, klicka på [Kontrollpanel], klicka på [System och säkerhet] och klicka sedan på [Administrationsverktyg].**

   Under Windows 8, dra muspekaren över övre och nedre högra hörnet av skärmen och klicka sedan på [Inställningar], [Kontrollpanel], [System och säkerhet] och sedan [Administrationsverktyg].

2. **Dubbelklicka på [Lokal säkerhetspolicy].**

   Om dialogrutan "Kontroll av användarkonto" visas, klicka på [Ja].

3. **Klicka på [IP-säkerhetsprincip på lokal dator].**
4. **I Åtgärdsmenyn, klicka på [Skapa IP-säkerhetsprincip].**

   Guiden IP Säkerhetsprincip visas.

5. **Klicka på [Nästa].**
6. **Ange ett namn för säkerhetsprincipen under "Namn" och klicka sedan på [Nästa].**
7. **Avmarkera kryssrutan "Aktivera standardresponsregeln" och klicka på [Nästa].**
8. **Välj "Redigera egenskaper" och klicka sedan på [Slutför].**
9. **På fliken "Allmänt", klicka på [Inställningar].**
10. **I "Autentisera och generera en ny kod efter varje" anger du samma giltighetstid (i minuter) som angivits på maskinen under "Inställningar för automatiskt byte av krypteringsnycklar Fas 1". Klicka sedan på [Metoder].**
11. **Kontrollera att hashalgoritmen ("Integrity"), krypteringsalgoritmen ("Encryption") och inställningar för "Diffie-Hellman-grupp" i "Ordning för säkerhetsmetod" matchar det som angetts i "Inställningar för automatiskt byte av krypteringsnycklar Fas 1".**

    Om inställningarna inte visas, klicka på [Lägg till].

12. **Klicka på [OK] två gånger.**
13. **Klicka på [Lägg till] på fliken "Regler".**

    Guiden Säkerhetsregel visas.

14. **Klicka på [Nästa].**
15. **Välj "Den här regeln anger inte någon tunnel" och klicka på [Nästa].**
16. **Välj typ av nätverk för IPsec och klicka på [Nästa].**
17. **Klicka på [Lägg till] i listan med IP-filter.**
18. **Under [Namn], ange ett IP-filternamn. Klicka sedan på [Lägg till].**

    Guiden IP-filter visas.

19. **Klicka på [Nästa].**
20. **Vid behov anger du en beskrivning av IP-filtret och klickar sedan på [Nästa].**
21. **Välj "Min IP-adress" i fältet "Källadress" och klicka sedan på [Nästa].**

22. **Välj "En specifik IP-adress eller subnät" i "Destinationsadress", ange maskinens IP-adress och klicka på [Nästa].**
23. **Välj protokolltyp för IPsec och klicka på [Nästa].**

    Om du använder IPsec med IPv6, välj "58" som protokollnummer för mål-protokolltypen "Annat".
24. **Klicka på [Slutför].**
25. **Klicka på [OK].**
26. **Välj IP-filtret som just skapades och klicka på [Nästa].**
27. **Klicka på [Lägg till].**

    Guiden filteråtgärder visas.
28. **Klicka på [Nästa].**
29. **Under [Namn], ange ett IP-filteråtgärdsnamn. Klicka sedan på [Nästa].**
30. **Välj "Förhandla om säkerhetsnivå" och klicka sedan på [Nästa].**
31. **Välj "Tillåt osäker kommunikation om det inte går att upprätta en skyddad anslutning." och klicka sedan på [Nästa].**
32. **Välj "Anpassad" och klicka på [Inställningar].**
33. **I "Integrationsalgoritm" väljer du den autentiseringsalgoritm som angivits på maskinen "Inställningar för automatiskt byte av krypteringsnycklar Fas 2".**
34. **I "Krypteringsalgoritm" väljer du den krypteringsalgoritm som angivits på maskinen i "Inställningar för automatiskt byte av krypteringsnycklar Fas 2".**
35. **I "Inställningar för Sessionskod", välj "Skapa en ny kod efter" och ange den giltighetsperiod (i sekunder) som angivits för maskinen i "Inställningar för automatiskt byte av krypteringsnycklar Fas 2".**
36. **Klicka på [OK].**
37. **Klicka på [Nästa].**
38. **Klicka på [Slutför].**
39. **Välj filteråtgärden som just skapades och klicka sedan på [Nästa].**

    Om du anger "Inställningar för automatiskt byte av krypteringsnycklar" till "Autentisering och hög krypteringsnivå" ska du välja den IP-filter-åtgärd som precis skapades. Klicka på [Redigera] och markera sedan "Använd sessionsnyckel för PFS (Perfect Forward Secrecy)" i dialogrutan för egenskaper för filteråtgärder. När du använder PFS i Windows, förhandlas PFS-gruppnumret som används i fas 2 automatiskt i fas 1 från Diffie-Hellman-Gruppnumret (inställt i steg 11). Om du ändrar säkerhetsnivån som anger automatiska inställningar på maskinen och "Användarinställning" visas, måste du ställa in samma gruppnummer för "Fas 1 Diffie-Hellman Group" och "Fas 2 PFS" på maskinen för att skapa en IPsec-överföring.

40. **Välj autentiseringsmetod och klicka sedan på [Nästa].**

    Om du väljer "Certificate" som autentiseringsmetod i "Inställningar för automatiskt byte av krypteringsnycklar" på maskinen ska du ange enhetscertifikatet. Om du väljer "PSK", ange då samma PSK-text som angivits på maskinen med den i förväg delade nyckeln.

41. **Klicka på [Slutför].**

42. **Klicka på [OK].**

    Den nya IP-säkerhetsrincipen (IPsec-inställningar) anges.

43. **Välj den säkerhetsprincip som precis skapades, högerklicka och klicka på [Tilldela].**

    Datorns IPsec-inställningar är aktiverade.

Obs

- För att avaktivera datorns IPsec-inställningar, markera säkerhetspolicy, högerklicka och klicka sedan på [Tilldela inte].

telnet-inställningskommandon

Du kan använda Telnet för att bekräfta IPsec-inställningar och göra ändringar i inställningarna. Detta avsnitt förklarar telnet-kommandon för IPsec. För mer information om användarnamn och lösenord för att logga in på telnet, fråga administratören. För mer information om hur du loggar in på telnet och telnet-funktioner, se handboken Anslut maskinen/Systeminställningar.

Viktigt

- **Om du använder ett certifikat som autentiseringsmetod i inställningarna för automatiskt byte av krypteringskod (IKE), installera certifikatet med Web Image Monitor. Ett certifikat kan inte installeras med telnet.**

ipsec

För att visa information om inställningarna av IPsec, använd kommandot: "ipsec".

Visa aktuella inställningar

```
msh> ipsec
```

Visar följande information om IPsec-inställningar:

- Inställningsvärden för IPsec
- Inställningar för automatiskt byte av krypteringskod, IKE-inställning med värde 1-4
- Inställningar för automatiskt byte av krypteringskod, IKE-standardinställningsvärden

Visa aktuella inställningsdelar

```
msh> ipsec -p
```

- Visar information om IPsec-inställningar del för del.

ipsec exkludera

För att visa eller ange protokoll som uteslutits av IPsec, använd kommandot: "ipsec exclude".

Visa aktuella inställningar

```
msh> ipsec exclude
```

- Visar de protokoll som just nu är uteslutna från IPsec-överföring.

Ange protokoll att utesluta

```
msh> ipsec exclude {https|dns|dhcp|wins|all} {on|off}
```

- Ange protokollet och ange sedan [on] för att utesluta det eller [off] för att inkludera det för IPsec-överföring. Om du väljer [all] anges alla protokoll tillsammans.

ipsec ike

För att visa eller ange inställningar för automatiskt utbyte av krypteringsnyckel, använd kommandot: "ipsec ike".

Visa aktuella inställningar

```
msh> ipsec ike {1|2|3|4|default}
```

- För att se inställningarna 1-4, ange nummer [1-4].
- För att visa standardinställningen ska du ange: [default].
- Anger man inte något värde visas samtliga inställningar.

Avaktivera inställningar

```
msh> ipsec ike {1|2|3|4|default} disable
```

- För att avaktivera inställningarna 1-4, ange nummer [1-4].
- För att avaktivera standardinställningarna ska du ange: [default].

Ange den användarspecifika lokala adressen/fjärradressen.

```
msh> ipsec ike {1|2|3|4} {ipv4|ipv6} "local address" "remote address"
```

- Ange det separata inställningsnumret [1-4] och adresstypen för att ange lokal adress och fjärradress.
- För att ställa in värden för lokala adresser/fjärradresser, ange masklen genom att ange [/] och ett heltal mellan 0-32 när du ställer in en IPv4-adress. När du ställer in en IPv6-adress, ange masklen genom att ange [/] och ett heltal mellan 0-128.
- Att inte ange ett adressvärde gör att aktuell inställning visas.

Ange adresstypen i standardinställning

```
msh> ipsec ike default {ipv4|ipv6|any}
```

- Ange adresstypen för standardinställningen.
- För att ange både IPv4 och IPv6 ska du ange: [any].

Inställning av säkerhetspolicy

```
msh> ipsec ike {1|2|3|4|default} proc {apply|bypass|discard}
```

- Ange det separata inställningsnumret [1-4] eller [default] och ange säkerhetspolicyn för den adress som har angivits i den markerade inställningen.
- För att använda IPsec på relevanta paket ska du ange: [apply]. För att använda IPsec ska du ange: [bypass].
- Om du anger [discard] kasseras alla paket som IPsec kan tillämpas på.
- Anger man inte en säkerhetspolicy visas aktuell inställning.

Inställning av säkerhetsprotokoll

```
msh> ipsec ike {1|2|3|4|default} proto {ah|esp|dual}
```

- Ange det separata inställningsnumret [1-4] eller [default] och ange säkerhetsprotokollet.
- För att ange AH ska du ange: [ah]. För att ange ESP ska du ange: [esp]. För att ange AH och ESP ska du ange: [dual].
- Att inte ange ett protokoll gör att den aktuella inställningen visas.

Inställning av IPsec kravnivå

```
msh> ipsec ike {1|2|3|4|default} level {require|use}
```

- Ange det separata inställningsnumret [1-4] eller [default] och ange kravnivån för IPsec.
- Om du anger [require] kommer data inte att överföras när IPsec inte kan användas. Om du anger [use] kommer data att överföras normalt när IPsec inte kan användas. När IPsec kan användas utförs IPsec-överföring.
- Anger man inte en kravnivå visas den aktuella inställningen.

Inställning för inkapslingsläge

```
msh> ipsec ike {1|2|3|4|default} mode {transport|tunnel}
```

- Ange det separata inställningsnumret [1-4] eller [default] och ange inkapslingsläget.
- För att ange transportläge ska du ange: [transport]. För att ange tunnelläge ska du ange: [tunnel].
- Om du har ställt in adresstypen i standardinställningen till [any] kan du inte använda [tunnel] i inkapslingsläge.
- Att inte ange ett inkapslingsläge gör att den aktuella inställningen visas.

Inställning av tunneländpunkt

```
msh> ipsec ike {1|2|3|4|default} tunneladdr "beginning IP address" "ending IP
address"
```

- Ange det separata inställningsnumret [1-4] eller [default] och ange slutet på tunneln som börjar och avslutar IP-adressen.
- Anger man inte vare sig start- eller slutadress visas den aktuella inställningen.

Inställning av autentiseringsmetod för IKE-partner

```
msh> ipsec ike {1|2|3|4|default} auth {psk|rsasig}
```

- Ange det separata inställningsnumret [1-4] eller [default] och ange autentiseringsmetoden.
- Ange [psk] för att använda en delad nyckel som autentiseringsmetod. Ange [rsasig] för att använda ett certifikat som autentiseringsmetod.
- Du måste även ange PSK-teckensträngen när du väljer [psk].
- Observera att om du väljer "Certifikat" måste certifikatet för IPsec installeras och anges innan det kan användas. Använd Web Image Monitor för att installera och ange certifikatet.

Inställning av PSK-teckensträng

```
msh> ipsec ike {1|2|3|4|default} psk "PSK character string"
```

- Om du väljer PSK som autentiseringsmetod ska du ange det separata inställningsnumret [1-4] eller [default] och ange PSK-teckensträngen.
- Ange teckensträngen med ASCII-tecken. Det går inte med förkortningar.

Inställning av hash-algoritm för ISAKMP SA (fas 1)

```
msh> ipsec ike {1|2|3|4|default} ph1 hash {md5|sha1|sha256|sha384|sha512}
```

- Ange det separata inställningsnumret [1-4] eller [default] och ange hash-algoritmen för ISAKMP SA (fas 1).
- Anger man inte hash-algoritm visas den aktuella inställningen.

Inställning av krypteringsalgoritm för ISAKMP SA (fas 1)

```
msh> ipsec ike {1|2|3|4|default} ph1 encrypt {des|3des|aes128|aes192|aes256}
```

- Ange det separata inställningsnumret [1-4] eller [default] och ange krypteringsalgoritmen för ISAKMP SA (fas 1).
- Anger man inte en krypteringsalgoritm visas den aktuella inställningen.

Inställning av Diffie-Hellmangrupp för ISAKMP SA (fas 1)

```
msh> ipsec ike {1|2|3|4|default} ph1 dhgroup {1|2|14}
```

- Ange det separata inställningsnumret [1-4] eller [default] och ange Diffie-Hellman-gruppnumret för ISAKMP SA (fas 1).
- Ange vilket gruppnummer som ska användas.
- Anger man inte något gruppnummer visas den aktuella inställningen.

Inställning av giltighetsperiod för ISAKMP SA (fas 1)

```
msh> ipsec ike {1|2|3|4|default} ph1 lifetime "validity period"
```

- Ange det separata inställningsnumret [1-4] eller [default] och ange giltighetsperioden för ISAKMP SA (fas 1).
- Ange giltighetsperioden (i sekunder) från 300 till 172 800.
- Anger man inte en giltighetsperiod visas den aktuella inställningen.

Inställning av autentiseringsalgoritm för IPsec SA (fas 2)

```
msh> ipsec ike {1|2|3|4|default} ph2 auth {hmac-md5|hmac-sha1|hmac-sha256|hmac-sha384|hmac-sha512}
```

- Ange det separata inställningsnumret [1-4] eller [default] och ange autentiseringsalgoritmen för IPsec SA (fas 2).
- Skilj multipla poster åt i autentiseringsalgoritmen med ett komma (,). De aktuella inställningsvärdena visas i högsta prioritetsordning.
- Anger man ingen autentiseringsalgoritm visas den aktuella inställningen.

Inställning av krypteringsalgoritm för IPsec SA (fas 2)

```
msh> ipsec ike {1|2|3|4|default} ph2 encrypt {null|des|3des|aes128|aes192|aes256}
```

- Ange det separata inställningsnumret [1-4] eller [default] och ange krypteringsalgoritmen för IPsec SA (fas 2).
- Skilj multipla poster åt i autentiseringsalgoritmen med ett komma (,). De aktuella inställningsvärdena visas i högsta prioritetsordning.
- Anger man inte en krypteringsalgoritm visas den aktuella inställningen.

Inställning av PFS för IPsec SA (fas 2)

```
msh> ipsec ike {1|2|3|4|default} ph2 pfs {none|1|2|14}
```

- Ange det separata inställningsnumret [1-4] eller [default] och ange Diffie-Hellman-gruppnumret för IPsec SA (fas 2).
- Ange vilket gruppnummer som ska användas.
- Anger man inte något gruppnummer visas den aktuella inställningen.

Inställning av giltighetsperiod för IPsec SA (fas 2)

```
msh> ipsec ike {1|2|3|4|default} ph2 lifetime "validity period"
```

- Ange det separata inställningsnumret [1-4] eller [default] och ange giltighetsperioden för IPsec SA (fas 2).
- Ange giltighetsperioden (i sekunder) från 300 till 172 800.
- Anger man inte en giltighetsperiod visas den aktuella inställningen.

Nollställa inställningsvärden

```
msh> ipsec ike {1|2|3|4|default|all} clear
```

- Ange det enskilda inställningsnumret [1-4] eller [default] och återställ sedan den angivna inställningen. Om du anger [all] återställs alla inställningar inklusive standardinställningen.

Konfigurera IEEE 802.1X-autentisering

IEEE 802.1X är en autentiseringsstandard som använder autentiseringsservern (RADIUS-server).

Du kan välja 4 typer av autentiseringsmetoder för EAP: EAP-TLS, LEAP, EAP-TTLS och PEAP. Notera att varje EAP autentiseringsmetod har olika konfigurationsinställningar och autentiseringsförfaranden.

Följande typer och krav på certifikat finns:

EAP-typ	Certifikat som krävs
EAP-TLS	Webbplatscertifikat, enhetscertifikat (IEEE 802.1X-klientcertifikat)
LEAP	-
EAP-TTLS	Webbplatscertifikat
PEAP	Webbplatscertifikat
PEAP (Fas 2 är endast för TLS)	Webbplatscertifikat, enhetscertifikat (IEEE 802.1X-klientcertifikat)

Installera ett Webbplatscertifikat

Installera ett webbplatscertifikat (rot-CA-certifikat) för verifiering av autentiseringsserverns tillförlitlighet. Du måste ha minst ett utfärdat certifikat från certifikatutfärdaren som signerade servercertifikatet, eller ett certifikat från en överordnad certifikatutfärdare.

Endast PEM-webbplatscertifikat (Base64-kodade X.509) kan importeras.

1. **Logga in som nätverksadministratör från Web Image Monitor.**
2. **Peka på [Enhetshantering] och klicka sedan på [Konfiguration].**
3. **Klicka på [Webbplatscertifikat] under "Säkerhet".**
4. **Klicka på [Bläddra] för "Webbplatscertifikat att importera" och välj det CA-certifikat som du ska hämta.**
5. **Klicka på [Öppna].**
6. **Klicka på [Importera].**
7. **Kontrollera att det importerade certifikatets [Status] är "Tillförlitlig".**

   Om [Kontroll av webbplatscertifikat] är [Aktivt] och [Status] för certifikatet visar [Inte tillförlitlig], är kommunikation inte möjlig.
8. **Klicka på [OK].**
9. **Logga ut.**

Välja Device Certificate

Välj det certifikat som du vill använda under IEEE 802.1X bland enhetscertifikaten som redan har skapats och installerats på maskinen. Information om hur du skapar och installerar ett enhetscertifikat finns i s. 99 "Skydda kommunikationsvägar via ett enhetscertifikat".

1. **Logga in som nätverksadministratör från Web Image Monitor.**
2. **Peka på [Enhetshantering] och klicka sedan på [Konfiguration].**
3. **Klicka på [Enhetens certifikat] under"Säkerhet".**
4. **Välj det certifikat som ska användas för IEEE 802.1X från listmenyn i "IEEE 802.1X" under "Certifikat".**
5. **Klicka på [OK].**
6. **"Uppdaterar..." visas. Avvakta i 1 eller 2 minuter och klicka sedan på [OK].**

   Om den föregående skärmbilden inte visas igen när du klickar på [OK], vänta en stund och klicka sedan på uppdateringsknappen i webbläsaren.
7. **Logga ut.**

Inställningsposter för IEEE 802.1X för Ethernet

1. **Logga in som nätverksadministratör från Web Image Monitor.**
2. **Peka på [Enhetshantering] och klicka sedan på [Konfiguration].**
3. **Klicka på [IEEE 802.1X] under "Säkerhet".**
4. **I fältet "Användarnamn" anger du det användarnamn som är inställt på RADIUS-servern.**
5. **Ange domännamnet i "Domännamn".**
6. **Välj "EAP-typ". Konfigurationen kan vara olika beroende på EAP-typ.**

   EAP-TLS

   - Gör följande inställningar beroende på operativsystemet som du använder.
     - Välj [På] eller [Av] i "Autentisera servercertifikat".
     - Välj [På] eller [Av] i "Lita på mellanliggande certifikatsutfärdare".
     - Ange värdnamn för RADIUS-servern i "Server-ID".
     - Välj [På] eller [Av] i fönstret "Tillåt underdomän".

   LEAP

   - Klicka på [Ändra] i "Lösenord" och ange sedan lösenordet som är inställt på RADIUS-servern.

   EAP-TTLS

   - Klicka på [Ändra] i "Lösenord" och ange sedan lösenordet som är inställt på RADIUS-servern.

- Klicka på [Ändra] i "Användarnamn för Fas 2" och ange användarnamnet som är inställt på RADIUS-servern.
- Välj [CHAP], [MSCHAP], [MSCHAPv2], [PAP] eller [MD5] i "Metod för Fas 2".

  Vissa metoder är inte tillgängliga beroende på vilken RADIUS-server du vill använda.
- Gör följande inställningar beroende på operativsystemet som du använder.
  - Välj [På] eller [Av] i "Autentisera servercertifikat".
  - Välj [På] eller [Av] i "Lita på mellanliggande certifikatsutfärdare".
  - Ange värdnamnet för RADIUS-servern i "Server-ID".
  - Välj [På] eller [Av] i fönstret "Tillåt underdomän".

PEAP

- Klicka på [Ändra] i "Lösenord" och ange sedan lösenordet som är inställt på RADIUS-servern.

  Om [TLS] har valts för "Metod för Fas 2" behöver du inte ange ett lösenord.
- Klicka på [Ändra] i "Användarnamn för Fas 2" och ange sedan det användarnamn som är inställt på RADIUS-servern.
- Välj [MSCHAPv2] eller [TLS] i "Metod för Fas 2".

  Om du väljer [TLS] måste du installera "IEEE 802.1X-klientcertifikat".
- Gör följande inställningar beroende på operativsystemet som du använder.
  - Välj [På] eller [Av] i "Autentisera servercertifikat".
  - Välj [På] eller [Av] i "Lita på mellanliggande certifikatsutfärdare".
  - Ange värdnamn för RADIUS-servern i "Server-ID".
  - Välj [På] eller [Av] i fönstret "Tillåt underdomän".

7. **Klicka på [OK].**
8. **"Uppdaterar..." visas. Avvakta i 1 eller 2 minuter och klicka sedan på [OK].**

   Om den föregående skärmbilden inte visas igen när du klickar på [OK], vänta en stund och klicka sedan på uppdateringsknappen i webbläsaren.
9. **Klicka på [Gränssnittsinställningar] under "Gränssnitt".**
10. **Välj [Aktivt] i "Ethernet-säkerhet".**
11. **Klicka på [OK].**
12. **"Uppdaterar..." visas. Avvakta i 1 eller 2 minuter och klicka sedan på [OK].**

    Om den föregående skärmbilden inte öppnas när du klickar på [OK] väntar du ett tag och klickar sedan på uppdateringsikonen i webbläsaren.
13. **Logga ut.**

Obs

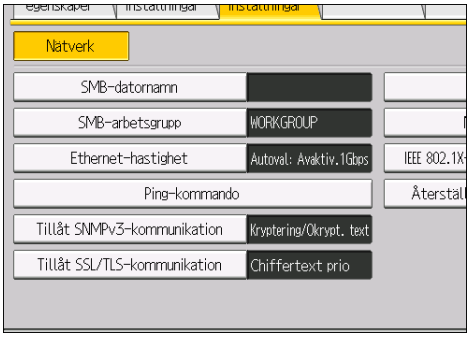
- Om ett problem uppstår med inställningarna kan du eventuellt inte kommunicera med maskinen. Gå i så fall in i [Skriv ut lista] i[Gränssnittsinställningar] i kontrollpanelen och skriv sådan ut nätverkssammanfattningen för att kontrollera status.
- Om du inte kan identifiera problemet, verkställ[Återställ IEEE 802.1X-autentisering till standard] i[Nätverk] i [Gränssnittsinställningar] i kontrollpanelen och repetera sedan processen.

SNMPv3-kryptering

Om du använder Device Manager NX eller ett annat program som kommunicerar via SNMPv3 kan du kryptera överförd data/information.

Genom att göra den här inställningen kan du skydda data från att manipuleras.

1. **Logga in som nätverksadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Gränssnittsinst].**
4. **Tryck på [▼Nästa].**
5. **Tryck på [Tillåt SNMPv3-kommunikation].**



6. **Tryck på [Endast kryptering].**
7. **Tryck på [OK].**
8. **Logga ut.**

Obs

- För att använda Device Manager NX vid kryptering av inställningsinformationen måste du ange nätverksadministratörens inställningar för [Krypteringslösen] och [Krypterat lösenord] i [SNMP-kontoinställning] i Device Manager NX, förutom att ange [Tillåt SNMPv3-kommunikation] på maskinen. För information om hur [Krypterat lösenord] anges i Device Manager NX, se Hjälpen till Device Manager NX.
- Om inställningen för nätverksadministratörens [Krypteringslösen] inte har angivits blir kanske de uppgifter som ska överföras inte krypterade eller skickade. För mer information om hur du anger inställningar för nätverksadministratörens [Krypteringslösen], se s. 14 "Registrera och ändra administratörer".

Kryptera överförda lösenord

Konfigurering av krypteringskod för drivrutin och lösenordskryptering för IPP-autentisering möjliggör kommunikation med krypterade lösenord och ökar skyddet mot att de knäcks. För att ytterligare öka säkerheten, rekommenderar vi att du använder IPsec, SNMPv3 och SSL/TLS.

Kryptera också lösenordet för administratör- och användarautentisering.

Krypt.kod för drivrutin

Denna kod är en teckensträng som används för att kryptera lösenord för inloggning eller dokumentlösenord som skickas från varje drivrutin när användarautentisering är aktiverad.

För att kryptera lösenordet ska du ange drivrutinens krypteringskod på maskinen och på skrivardrivrutinen som är installerad på användarens dator.

Lösenord för IPP-autentisering

För att kryptera lösenordet för IPP-autentisering på Web Image Monitor, ställ in "Authentication" på [DIGEST] och ange därefter lösenordet för IPP-autentisering som ställts in på maskinen.

Du kan använda Telnet eller FTP för att hantera lösenord för IPP-autentisering, men det rekommenderas inte.

Obs

- Mer information om hur man krypterar lösenord för administratörsautentisering, se s. 14 "Registrera och ändra administratörer".

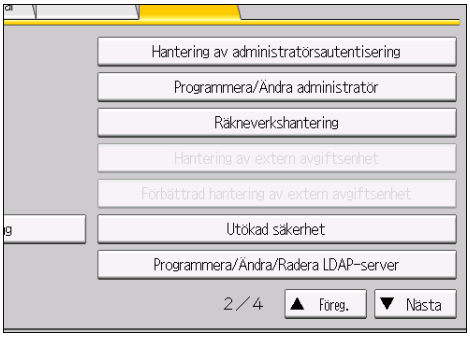
Ange en Krypteringskod för drivrutin

Ange Krypteringskod för drivrutinen på maskinen.

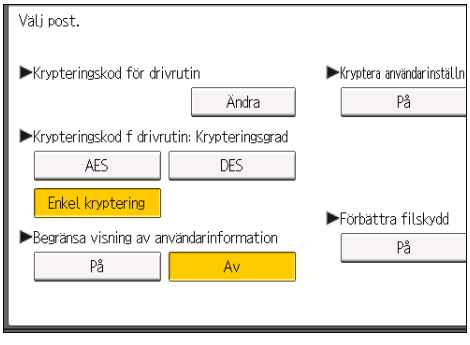
Denna inställning möjliggör krypterad överföring av inloggningslösenord och stärker skyddet mot knäckning av det.

1. **Logga in som nätverksadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa].**

5. **Tryck på [Utökad säkerhet].**



6. **För "Krypteringskod för drivrutin", tryck på [Ändra].**



7. **Skriv in krypteringskoden för drivrutinen och tryck sedan på [OK].**

   Ange drivrutinens krypteringsnyckel med upp till 32 alfanumeriska tecken.

   Nätverksadministratören måste dela ut krypteringskoden till den drivrutin som angetts på maskinen till användarna, så att de kan registrera den på sina datorer. Var noga med att skriva in samma krypteringskod som den som angetts för maskinen.

8. **Tryck på [OK].**
9. **Logga ut.**

Obs

- För information om hur man anger krypteringsnyckeln för skrivardrivrutinen, se drivrutinens Hjälp.

Ange ett lösenord för IPP-autentisering Lösenord

Ange ett IPP-autentiseringslösenord för denna maskin. Denna inställning aktiverar krypterad överföring av IPP-autentiseringslösenord och stärker skyddet mot lösenordsknäckning.

1. **Logga in som nätverksadministratör från Web Image Monitor.**
2. **Peka på [Enhetshantering] och klicka sedan på [Konfiguration].**
3. **Klicka på [IPP-autentisering] under "Säkerhet".**

4. **Välj [DIGEST] i listan "Authentication".**
5. **Ange användarnamnet i rutan "Användarnamn".**
6. **Ange lösenordet i rutan "Lösenord".**
7. **Klicka på [OK].**

   IPP-autentisering specificeras.
8. **"Uppdaterar..." visas. Avvakta i 1 eller 2 minuter och klicka sedan på [OK].**

   Om den föregående skärmbilden inte visas igen när du klickar på [OK], vänta en stund och klicka sedan på uppdateringsknappen i webbläsaren.
9. **Logga ut.**

Krypteringsinställningar för Kerberos-autentisering

När Kerberos-autentisering är aktiverat kan du ange krypterad överföring mellan maskinen och KDC-servern.

Användning av Kerberosautentisering med Windows eller LDAP-autentisering garanterar en säker kommunikation.

Den krypteringsalgoritm som stöds varierar beroende på typ av KDC-server. Välj den algoritm som passar din miljö.

KDC-server	Krypteringsalgoritmer som stöds
Windows Server 2003 Active Directory	• RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5
Windows Server 2008	• AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5
Windows Server 2008 R2/2012/2012 R2	• AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5*
Heimdal	• AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • DES3-CBC-SHA1 • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5

* För att använda Kerberos-autentisering, aktivera denna i operativsystem-inställningarna.

1. **Logga in som maskinadministratör från Web Image Monitor.**
2. **Peka på [Enhetshantering] och klicka sedan på [Konfiguration].**
3. **Klicka på [Kerberos-autentisering] under "Enhetsinställningar".**
4. **Välj den krypteringsalgoritm du vill aktivera.**

   Se till att välja en eller flera krypteringsalgoritmer.

5. Klicka på [OK].
6. Logga ut.

6. Förhindra spridning av dokument

I detta kapitel beskrivs hur du skyddar dokument som lagrats på eller skrivits ut från maskinen.

Hantera säkra utskriftsfiler

Beroende på skrivarens placering kan det vara svårt att förhindra att obehöriga personer läser utskrifter som ligger i skrivarens utmatningsfack. Använd därför funktionen Säker utskrift när du skriver ut konfidentiella dokument.

Säker utskrift

- Genom att använda skrivarens funktion Säker utskrift kan du lagra filer på maskinen som filer för Säker utskrift. Skriv sedan ut filerna från kontrollpanelen och ta med dem direkt så att andra inte kan läsa dem.

Obs

- Konfidentiella dokument kan skrivas ut oavsett inställningar för användarautentisering.
- För att tillfälligt lagra filer väljer du [Lagrad utskrift] i skrivardrivrutinen. Om du väljer [Lagrad utskrift (Delad)] kan dessa filer delas med andra.
- För mer information om hur du använder funktionen Säker utskrift, se handboken Print (Skrivare).

Radera Säkra utskriftsfiler

Detta kan specificeras av filadministratören eller ägaren.

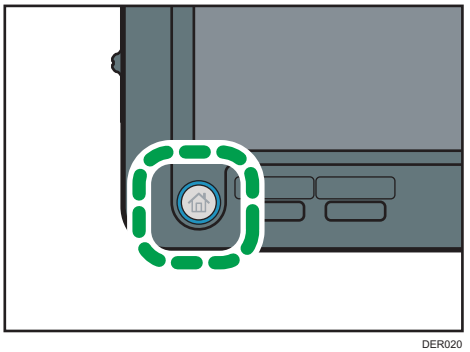
För att ägaren ska kunna ta bort en säker utskriftsfil, krävs lösenordet för att komma åt filen. Om ägaren har glömt lösenordet, kan filadministratören ändra det.

Lösenordet krävs inte för att filadministratören ska ta bort filer med Säker utskrift.

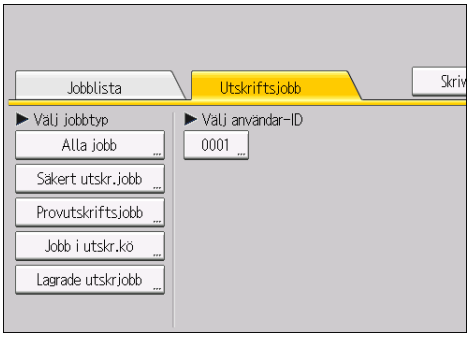
1. **Logga in som filadministratör eller ägare från kontrollpanelen.**
2. **Tryck på [Användarverktyg] för att stänga menyn Användarverktyg.**

   Om meddelandet "Du har inte rättighet att använda den här funktionen." visas, tryck på [Avsluta].
3. **Tryck på [Startsida] på kontrollpanelen och tryck sedan på ikonen [Skrivare] på skärmen.**

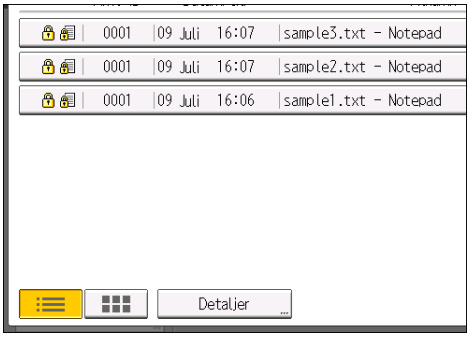
   Om ikonen [Skrivare] inte visas, tryck på ikonen högst upp i högra hörnet av skärmen för att växla till menyskärmen.



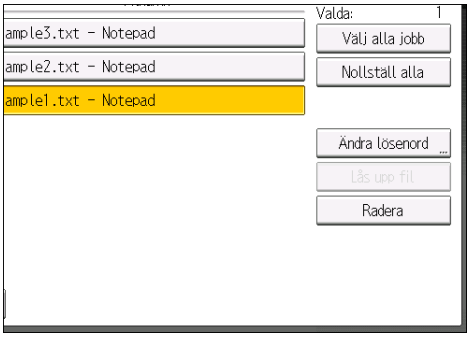
4. **Tryck på [Utskriftsjobb].**
5. **Tryck på [Säkert utskr.jobb].**



6. **Välj filen.**



7. **Tryck på [Radera].**



8. **Om en skärm för att ange ett lösenord visas ska du ange lösenordet för den säkra utskriftsfilen och trycka på [OK].**

   Skärmen för att ange lösenord visas inte om filadministratören är inloggad.

9. **Tryck på [Ja].**
10. **Logga ut.**

Obs

- Du kan konfigurera maskinen så att lagrade filer raderas automatiskt genom att ställa in menyvalet "Ta bort tillf. utskr.jobb automatiskt" till [På]. För mer information om "Ta bort tillf. utskr.jobb automatiskt", se Utskrift.
- Det kan även anges via Web Image Monitor. För mer information, se hjälpen till Web Image Monitor.

Ändra lösenordet för en fil med Säker utskrift

Detta kan specificeras av filadministratören eller ägaren.

Om ägaren har glömt lösenordet, kan filadministratören ändra det.

1. **Logga in som filadministratör eller ägare från kontrollpanelen.**
2. **Tryck på [Användarverktyg] för att stänga menyn Användarverktyg.**

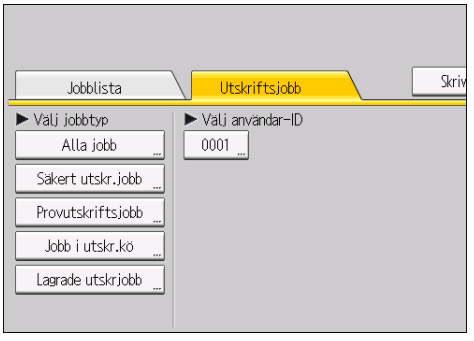
   Om meddelandet "Du har inte rättighet att använda den här funktionen." visas, tryck på [Avsluta].

3. **Tryck på [Startsida] på kontrollpanelen och tryck sedan på ikonen [Skrivare] på skärmen.**

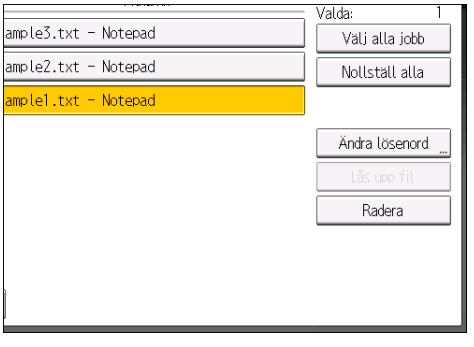
   Om ikonen [Skrivare] inte visas, tryck på ikonen högst upp i högra hörnet av skärmen för att växla till menyskärmen.

4. **Tryck på [Utskriftsjobb].**

5. **Tryck på [Säkert utskr.jobb].**



6. **Välj filen.**
7. **Tryck på [Ändra lösenord].**



8. **Om en skärm för att ange ett lösenord visas ska du ange lösenordet för den lagrade filen och trycka på [OK].**

   Skärmen för att ange lösenord visas inte om filadministratören är inloggad.
9. **Ange det nya lösenordet för den lagrade filen och tryck sedan på [OK].**
10. **Ange lösenordet på nytt för att bekräfta, och tryck sedan på [OK].**
11. **Logga ut.**

Obs

- Det kan även anges via Web Image Monitor. För mer information, se hjälpen till Web Image Monitor.

Låsa upp en säker utskriftsfil

Endast filadministratören kan låsa upp filer.

Om du anger [På] för "Förbättra filskydd" kommer filen att låsas och bli otillgänglig om ett ogiltigt lösenord anges 10 gånger. I det här avsnittet förklaras hur filer kan låsas upp.

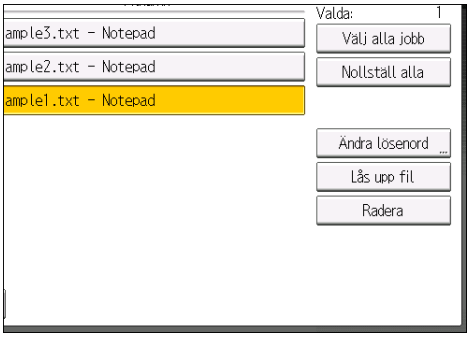
"Förbättra filskydd" är en av de utökade säkerhetsfunktionerna. Information om den här och andra utökade säkerhetsfunktioner finns i s. 193 "Ange Utökade säkerhetsfunktioner".

1. **Logga in som filadministratör via kontrollpanelen.**
2. **Tryck på [Användarverktyg] för att stänga menyn Användarverktyg.**

   Om meddelandet "Du har inte rättighet att använda den här funktionen." visas, tryck på [Avsluta].
3. **Tryck på [Startsida] på kontrollpanelen och tryck sedan på ikonen [Skrivare] på skärmen.**

   Om ikonen [Skrivare] inte visas, tryck på ikonen högst upp i högra hörnet av skärmen för att växla till menyskärmen.
4. **Tryck på [Utskriftsjobb].**
5. **Tryck på [Säkert utskr.jobb].**
6. **Välj filen.**

   Ikonen visas bredvid en fil som är låst med funktionen Förbättra filskydd.
7. **Tryck på [Lås upp fil].**



8. **Tryck på [Ja].**

   Ikonen försvinner.
9. **Logga ut.**

Obs

- Det kan även anges via Web Image Monitor. För mer information, se hjälpen till Web Image Monitor.

Skydd mot obehörig kopiering/Datasäkerhet för kopiering

Skrivarfunktionen låter dig bädda in ett mönster i utskrivna kopior för att förhindra obehörig kopiering.

Om funktionen Skydd mot obehörig kopiering har aktiverats, visas inbäddade textmönster (t.ex. ett varningsmeddelande som "Ingen kopiering") när dokumenten kopieras olagligt. Följaktligen kan otillåten kopiering förhindras.

Om funktionen Datasäkerhet för kopiering används och inställningar för specialmönster inbäddade i dokumenten har aktiverats, skrivs kopior av dokumenten med inbäddade mönster ut som en grå kopia. Följaktligen kan informationsläckor förhindras. För att skydda dokument med grå överskrivning, måste kopiatorn eller multifunktionsskrivaren installeras med Copy Data Security Unit.

För mer information, se informationen nedan:

Använda Skydd mot obehörig kopiering

1. Aktivera utskrift av det inbäddade mönstret. Maskinadministratören konfigurerar denna inställning. För mer information om hur inställningen konfigureras, se s. 142 "Aktivera utskrift av mönster".
2. Ange inställningen Skydd mot obehörig kopiering i skrivarfunktionen. Rättigheten att ange inställningen beror på inställningen som anges i [Obligatoriskt skydd mot obehörig kopiering]. För mer information, se s. 142 "Aktivera utskrift av mönster".

Använda Datasäkerhet för kopiering

1. Aktivera inställningen för utskrift med inbäddat mönster. Maskinadministratören konfigurerar denna inställning. För mer information om hur inställningen konfigureras, se s. 142 "Aktivera utskrift av mönster".
2. Ange inställningen Datasäkerhet för kopiering i skrivarfunktionen. Rättigheten att ange inställningen beror på inställningen som anges i [Obligatoriskt skydd mot obehörig kopiering]. För mer information, se s. 142 "Aktivera utskrift av mönster".

Aktivera utskrift av mönster

Du kan aktivera inbäddade tryckmönster för att motverka eller förhindra otillåten kopiering.

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa] två gånger.**
5. **Tryck på [Skydd mot obehörig utskrift: Skrivare].**
6. **Tryck på [Ändra] för "Inst f skydd mot obehörig kopiering".**

7. **Tryck på [På], följt av [OK].**
8. **Tryck på [Ändra] för "Obligatoriskt skydd mot obehörig kopiering".**
9. **Ange om utskrift av det inbäddade mönstret ska vara obligatoriskt eller inte.**
   - [Drivrut./Kommando]

     Utskrift av det inbäddade mönstret är inte obligatoriskt.

     Med hjälp av skrivardrivrutinen kan användarna välja om det inbäddade mönstret ska skrivas ut och kan ange inställningarna.
   - [Drivrutin/Kommando (de flesta inst.)]

     Utskrift av det inbäddade mönstret är obligatoriskt.

     Med hjälp av skrivardrivrutinen kan användare ange inställningar för det inbäddade mönstret utom för typ, färg och tjocklek.
   - [Maskininställning(ar)]

     Utskrift av det inbäddade mönstret är obligatoriskt.

     Användare kan inte ange inställningar för inbäddade mönster i skrivardrivrutinen.
10. **Tryck på [OK] två gånger.**
11. **Logga ut.**

Obs

- Mer information om inställningarna för att ange mönstret med hjälp av maskinen finns i Connecting the Machine/ System Settings.

Obligatorisk lagring av dokument som ska skrivas ut på en skrivare

Genom att göra det obligatoriskt att lagra jobb i maskinen innan de skrivs ut, kan du förhindra informationsläckage genom att du inte lämnar utskrifter obevakade. Det är obligatoriskt att lagra följande utskriftsjobb.

- Normal utskrift
- Provutskrift
- Lagra och skriv ut

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Skrivaregenskaper].**
3. **Tryck på [System].**
4. **Tryck på [▼Nästa].**
5. **Tryck på [Begränsa direktutskriftsjobb].**
6. **Tryck på [Lagra jobba automatiskt].**
7. **Tryck på [OK].**
8. **Logga ut.**

- Om du väljer [Avbr alla dir.utkskrjobb] kommer utskiftsjobben att avbrytas utan att lagras.
- För mer information om hur du skriver ut lagrade dokument, se Skrivare.

7. Hantera maskinen

I detta kapitel beskrivs hur du förbättrar maskinsäkerheten och hur du effektivt manövrerar maskinen.

Hantera loggfiler

Genom att samla in loggarna som är lagrade i maskinen kan du spåra detaljerade uppgifter angående maskinåtkomst, användaridentiteter, maskinanvändning samt felhistorik.

Loggarna kan raderas periodvis för att frigöra plats på hårddisken.

Loggarna kan visas via Web Image Monitor eller logghämtningsservern. Insamlade loggar kan konverteras till CSV-filer och laddas ner, alla på samma gång. De kan inte läsas direkt från hårddisken.

Loggtyper

3 typer av loggar lagras på maskinen: jobblogg, åtkomstlogg och miljöanpassad logg.

- Jobblogg

  Lagrar filer med användarrelaterade funktioner som utskrift, samt kontrollpanelsfunktioner som utskrift av rapporter (t.ex. konfigurationslistor).

- Åtkomstlogg

  Lagrar information om inloggnings- och utloggningsaktiviteter, lagrade filåtgärder som att skapa, redigera och radera, kundteknikerhantering som formatering av hårddisk, systemåtgärder som granskning av resultaten av loggöverföringar samt säkerhetsåtgärder som att ange inställningar för kryptering, upptäckt av obehörig åtkomst, användarutelåsning och firmware-autentisering.

- Miljöanpassad logg

  Lagrar information om huvudströmbrytarens PÅ, AV, strömstatusövergångar, körtider eller tidsintervaller mellan jobb, pappersförbrukning per timme, strömförbrukning.

Obs

- Mer information om logghämtning finns i handboken för logghämtningsservern.
- Om du använder logghämtningsservern måste du konfigurera inställningarna för loggöverföring på logghämtningsservern.

AnvändaWeb Image Monitor för att hantera loggfiler

Du kan ange vilka typer av loggar som ska lagras på maskinen samt logghämtningsnivå. Du kan även ta bort loggfiler i grupp eller ladda ner dem.

Loggar som kan hanteras med Web Image Monitor

Följande tabeller förklarar de poster i jobbloggen och åtkomstloggen som maskinen skapar när du aktiverar logghämtning med Web Image Monitor. Om du kräver logghämtning använder du Web Image Monitor för att konfigurera det. Den här inställningen kan anges i [Loggar] under [Konfiguration] i Web Image Monitor.

Informationsposter för jobbloggar

Poster i jobbloggen	Attribut för loggtyp	Innehåll
Skrivare: Utskrift	Printer: Printing	Detaljer för normala utskriftsjobb.
Skrivare: Säker utskrift (ofullständig)	Printer: Locked Print (Incomplete)	Logg som visar Säker utskrift-dokument som lagras tillfälligt på maskinen.
Skrivare: Säker utskrift	Printer: Locked Print	Logg som visar dokument för Säker utskrift som tillfälligt lagrats på maskinen och som skrivits ut från kontrollpanelen eller via Web Image Monitor.
Skrivare: Provutskrift (ofullständig)	Printer: Sample Print (Incomplete)	Logg som visar Provutskrift-dokument som lagras tillfälligt på maskinen.
Skrivare: Provutskrift	Printer: Sample Print	Logg som visar dokument för Provutskrift som tillfälligt lagrats på maskinen och som skrivits ut från kontrollpanelen eller via Web Image Monitor.
Skrivare: Utskriftskö (ofullständig)	Printer: Hold Print (Incomplete)	Logg som visar Utskriftskö-dokument som tillfälligt lagras på maskinen.
Skrivare: Utskriftskö	Printer: Hold Print	Logg som visar dokument i Utskriftskö som tillfälligt lagrats på maskinen och som skrivits ut från kontrollpanelen eller via Web Image Monitor.

Poster i jobbloggen	Attribut för loggtyp	Innehåll
Skrivare: Lagrad utskrift	Printer: Stored Print	Detaljer för Lagrad utskrift-filer som lagras på maskinen.
Skrivare: Lagra och Normal utskrift	Printer: Store and Normal Print	Detaljer för Lagrad utskrift-filer som skrevs ut vid lagring (när "Jobbtyp:" var inställt på "Lagra och skriv ut" i skrivaregenskaperna).
Skrivare: Utskrift av lagrad fil	Printer: Stored File Printing	Detaljer för Lagrad utskrift-filer som skrivits ut från kontrollpanelen eller Web Image Monitor.
Rapportutskrift	Report Printing	Detaljer för rapporter utskrivna från kontrollpanelen.
Skrivare: Utskrift av fil i utskriftskö	Printer: Hold Print File Printing	När ett dokument förvaras i utskriftskö och lagras tillfälligt på maskinen, noteras det klockslag då användaren anger att dokumentet ska skrivas ut via kontrollpanelen eller Web Image Monitor.

Informationsposter i åtkomstloggar

Poster i åtkomstloggen	Attribut för loggtyp	Innehåll
Inloggning	Login	Tider för inloggning och identitet för inloggade användare.
Utloggning	Logout	Tider för utloggning och identitet för utloggade användare.
HDD-format	HDD Format	Detaljer för hårddisksformatering.
Borttagning av alla loggar	All Logs Deletion	Detaljer för borttagning av alla loggar.
Ändring av logginställningar	Log Setting Change	Detaljer för ändringar av logginställningar.
Resultat för loggöverföring	Transfer Log Result	En logg med loggöverföringsresultat till Remote Communication Gate S.

Poster i åtkomstloggen	Attribut för loggtyp	Innehåll
Ändring av logghämtningsposter	Log Collection Item Change	Detaljer för ändringar av jobbhämtningsnivåer, åtkomsthämtningsnivåer och typer av loggar som hämtas.
Hämta krypterade kommunikationsloggar	Collect Encrypted Communication Logs	Logg över krypterade överföringar mellan verktyget, Web Image Monitor eller externa enheter.
Åtkomstöverträdelse	Access Violation	Detaljer för misslyckade åtkomstförsök.
Utelåsning	Lockout	Detaljer för utelåsningsaktivering.
Firmware: Uppdatering	Firmware: Update	Detaljer för firmware-uppdateringar.
Firmware: Strukturförändring	Firmware: Structure Change	Detaljer för strukturförändringar som uppstod när ett SD-kort sattes in eller togs ut eller när ett inkompatibelt SD-kort sattes in.
Firmware: Struktur	Firmware: Structure	Detaljer för kontroll över förändringar av firmwaremodulens struktur gjorda när maskinen slagits på.
Ändring av datakrypteringsnyckel	Machine Data Encryption Key Change	Detaljer för ändringar gjorda i krypteringskoder med inställningen "Ändring av datakrypteringsnyckel".
Firmware: Ogiltig	Firmware: Invalid	Detaljer för kontroller av firmwaregiltighet gjorda när maskinen slagits på.
Ändring av datum/tid	Date/Time Change	Detaljer för ändringar gjorda av datum- och tidsinställningar.
Ändring av filåtkomsträttigheter	File Access Privilege Change	Logg för ändringar av åtkomstbehörigheter till de lagrade filerna.
Ändring av lösenord	Password Change	Detaljer för ändringar gjorda av inloggningslösenordet.
Ändring av administratör	Administrator Change	Information om ändringar som utförts av administratörer.
Ändring av adressbok	Address Book Change	Detaljer för ändringar gjorda i adressboksposter.

Poster i åtkomstloggen	Attribut för loggtyp	Innehåll
Machine Configuration	Machine Configuration	Logg för ändringar av maskinens inställningar.
Säkerhetskopiera adressbok	Back Up Address Book	Logg för säkerhetskopiering av adressbok.
Återställ adressbok	Restore Address Book	Logg över återställning av adressbok.
Utökad begränsad utskriftsvolym: Resultat, behörighet för spårning	Enhanced Print Volume Use Limitation: Tracking Permission Result	Logg över fel som inträffar vid spårning.
Resultat nollställ räkneverk: Vald(a) användare	Counter Clear Result: Selected User(s)	Logg över nollställning av en enskild användares räkneverk.
Resultat nollställ räkneverk: Alla användare	Counter Clear Result: All Users	Logg över nollställning av alla användares räkneverk.
Importera info om enhetsinställning	Import Device Setting Information	Logg över import av en enhetsinställningsfil.
Exportera info om enhetsinställning	Export Device Setting Information	Logg över export av en enhetsinställningsfil.

Det finns ingen logg för "Inloggning" för SNMPv3.

Om hårddisken formateras raderas alla loggposter som skapats innan formateringen och en loggpost skapas som indikerar att formateringen har slutförts.

"Åtkomstöverträdelse" indikerar att systemet har utsats för frekventa, fjärr-DoS-attacker som har involverat inloggningsförsök genom användarautentisering.

Den första logg som skapas efter att strömmen slås på är loggen "Firmware: Struktur".

Informationsposter för miljöanpassade loggar

Post i miljöanpassad logg	Attribut för loggtyp	Innehåll
Huvudström på	Main Power On	Logg över när huvudströmmen är påslagen.
Huvudström av	Main Power Off	Logg över när huvudströmbrytaren är avstängd.

Post i miljöanpassad logg	Attribut för loggtyp	Innehåll
Resultat övergång av energistatus	Power Status Transition Result	Logg över resultaten från övergång av energistatus.
Jobbrelaterad information	Job Related Information	Logg över jobbrelaterad information.
Pappersförbrukning	Paper Usage	Logg över pappersförbrukning.
Strömförbrukning	Power Consumption	Logg över strömförbrukning.

Attribut för loggar du kan ladda ner

Om du använder Web Image Monitor för att hämta loggar, skapas en CSV-fil som innehåller de informationsposter som visas i följande tabell.

Observera att ett tomt fält anger en post som inte finns i en logg.

Utdataformat för fil

- Teckenkodning: UTF-8
- Utformat: CSV (Comma-Separated Values)
- Filnamn för jobbloggar och åtkomstloggar: "maskinnamn +_log.csv"
- Filnamn för miljöanpassade loggar: "maskinnamn +_ecolog.csv"

Loggposters ordning

Loggposter skrivs ut i stigande ordning enligt Logg-ID.

Filstruktur

Datarubriken skrivs ut på filens första rad (rubrikraden).

Skillnader i logginformationsformat

- Jobblogg

  Flera rader visas i ordningen för gemensamma poster (jobblogg och åtkomstlog), Källa (jobbets indata) och Mål (jobbets utdata). Samma logg-ID tilldelas alla rader som motsvarar en enda jobbloggspost.

	Start Date/Time	···	Result	···	Access Result	Source	···	Print File Name	Target	···	Stored File Name
1	20XX-12-03T15:43:03.0	···	Completed	···			···			···	
2		···	Completed	···		Report	···			···	
3		···	Completed	···			···		Print	···	

CJD022

1. **Vanliga poster**

   Varje post i vanliga poster visas på en separat rad.

2. **Källa**

   "Result" och "Status" i vanliga poster och jobblogg visas (indata).

   Om det finns flera källor visas flera rader.

3. **Mål**

   "Result" och "Status" i vanliga poster och jobblogg visas (utdata).

   Om det finns flera mål visas flera rader.

- Åtkomstlogg

  De vanliga posterna och poster i åtkomstloggen visas på separata rader.

- Miljöanpassad logg

  Miljöanpassade loggposter visas på separata rader.

Vanliga poster (jobblogg och åtkomstlogg)

Start Date/Time

Anger startdatum och tid för en åtgärd eller en händelse.

End Date/Time

Anger slutdatum och tid för en åtgärd eller en händelse.

Log Type

Information om loggtyp.

För mer information om informationsposterna i varje typ av logg, se s. 146 "Loggar som kan hanteras med Web Image Monitor".

Result

Anger resultatet av en åtgärd eller händelse.

Följande loggposter redovisas endast när de loggade åtgärderna utförts utan problem:

"Printer: Stored File Printing" (Jobbloggar)

Värde	Innehåll
Succeeded	Åtgärden eller händelsen slutfördes utan problem.
Failed	Åtgärden eller händelsen misslyckades.
<Tomt>	Åtgärden eller händelsen pågår fortfarande.

Operation Method

Anger åtgärdens process.

Värde	Innehåll
Control Panel	Kontrollpanel
Driver	Drivrutin
Utility	Verktyg
Web	Webb
Email	E-post

Status

Anger status för en åtgärd eller händelse.

Värde	Innehåll
Completed	Åtgärden eller händelsen slutfördes utan problem vid en jobbloggpost.
Failed	Åtgärden eller händelsen misslyckades vid en jobbloggpost.
Succeeded	Åtgärden eller händelsen slutfördes utan problem vid en åtkomstloggpost.
Password Mismatch	Ett åtkomstfel har inträffat på grund av att lösenorden inte stämmer överens.
User Not Programmed	En åtkomstfel har inträffat på grund av att användaren inte är registrerad.
Other Failures	Ett åtkomstfel har inträffat på grund av ett ospecificerat fel.
User Locked Out	Ett åtkomstfel har uppstått på grund av att användaren är utelåst.
Communication Failure	Ett åtkomstfel har inträffat på grund av ett kommunikationsfel.
Communication Result Unknown	Ett åtkomstfel har inträffat på grund av ett okänt kommunikationsresultat.
Failure in some or all parts	Att nollställa användarspecifikt räkneverk eller räkneverket för alla användare misslyckades.
Importing/Exporting by Other User	Import eller export körs av en annan användare.

Värde	Innehåll
Connection Failed with Remote Machine	En anslutning till en utskriftsmottagare misslyckades.
Write Error to Remote Machine	Ett fel inträffade vid utskrift till en mottagare.
Specified File: Incompatible	Den angivna filen är inkompatibel.
Specified File: Format Error	Ett formatfel inträffade med den angivna filen.
Specified File: Not Exist	Den angivna filen kan inte hittas.
Specified File: No Privileges	Behörighet saknas för åtkomst till angiven fil.
Specified File: Access Error	Ett fel inträffar vid åtkomst av den angivna filen.
Memory Storage Device Full	Det externa mediet är fullt.
Memory Storage Device Error	Det finns ett fel i det externa mediet.
Encryption Failed	Kryptering misslyckades.
Decoding Failed	Avkodning misslyckades.
Common Key Not Exist	Den gemensamma nyckeln saknas.
Connection Error	Ett kommunikationsfel inträffade.
Specified Server Error	En åtkomstfel har inträffat på grund av att servern inte är korrekt konfigurerad.
Specified Client Error	En åtkomstfel har inträffat på grund av att klienten inte är korrekt konfigurerad.
Authentication Settings Mismatch	Adressbokens specifikationer matchar inte.
Authentication Method Mismatch	Autentiseringsmetoderna matchar inte.
Maximum Limit of Registered Number	Maximalt antal maskiner som kan registreras.
Invalid Password	Det angivna lösenordet är ogiltigt.
Processing	Jobbet bearbetas.
Error	Ett fel har uppstått.

Värde	Innehåll
Suspended	Jobbet har pausats.

Cancelled: Details

Visar status där åtgärd eller händelse misslyckades.

Värde	Innehåll
Cancelled by User	En användare avbröt en åtgärd.
Input Failure	En inmatning avbröts på ett onormalt sätt.
Output Failure	En utmatning avbröts på ett onormalt sätt.
Other Error	Ett fel upptäcktes innan ett jobb utfördes eller något annat fel har inträffat.
Power Failure	Strömmen bröts.
External Charge Unit Disconnected	Redovisningsenheten bortkopplades under drift.
Timeout	Timeout inträffade.
Memory Full	Minnet för att bearbeta data är fullt.
Print Data Error	Ett försök har gjorts att använda en PDL eller en port som inte är installerad på datorn.
Data Transfer Interrupted	Ärenden som kan noteras är följande: • Den drivrutin som används stämmer inte. • Ett nätverksfel inträffar.
Over Job Limit	Begränsningen för antalet jobb som kan tas emot överskreds.
Authentication Failed (Access Restricted)	Enhetsautentisering misslyckades.
Exceeded Print Volume Use Limitation	Begränsningen av pappersanvändning för den inloggade användaren överskreds.
No Privilege	Användaren har inte behörighet att komma åt ett dokument eller en funktion.
Not Entered Document Password	Lösenordet för ett dokument angavs inte.

Värde	Innehåll
Invalid Device Certificate	Ärenden som kan noteras är följande: • Enhetens certifikat saknas. • Giltighetsperioden har löpt ut. • Om administratörens e-postadress och intyget inte stämmer överens.
Book Function Error	Ett funktionsfel med bokbindning har uppstått.
Fold Function Error	Ett funktionsfel för vikning har uppstått.
Print Cancelled (Error)	Utskriftsjobbet avbröts pga ett systemfel.

User Entry ID

Anger användarens ID.

Detta är ett hexadecimalt ID som identifierar användare som genomfört jobb- eller åtkomstloggrelaterade åtgärder.

Värde	Innehåll
0x00000000	Systemdrift, åtgärder som utförs av ej behöriga användare
0x00000001 - 0xffffeff	För allmänna användare och användarkod
0xffffff80	Systemdrift
0xffffff81	Systemdrift, åtgärder som utförs av ej behöriga användare
0xffffff86	Övervakare
0xffffff87	Administratör
0xffffff88	Administratör 1
0xffffff89	Administratör 2
0xffffff8a	Administratör 3
0xffffff8b	Administratör 4

User Code/User Name

Identifierar användarkod eller användarnamn för den användare som utförde åtgärden.

Om en administratör genomförde åtgärden innehåller hans eller hennes ID administratörens användarnamn för inloggning.

Log ID

Anger det ID som tilldelats loggen.

Detta är ett hexadecimalt ID som identifierar loggen.

Informationsposter i åtkomstloggar

Access Log Type

Anger typ av åtkomst.

Värde	Innehåll
Authentication	Åtkomst till användarautentisering
Stored File	Åtkomst till lagrad fil
System	Systemåtkomst
Network Attack Detection/ Encrypted Communication	Nätverksangrepp eller krypterad kommunikationsåtkomst
Firmware	Åtkomst till firmware verifiering
Address Book	Åtkomst till adressbok
Device Settings	Ändringar som görs i en inställning i menyn Användarverktyg.

Authentication Server Name

Anger namnet på den server där autentiseringen försökte genomföras.

No. of Authentication Server Switches

Anger det antal gånger som serverväxling inträffat när autentiseringsservern var otillgänglig.

Du kan kontrollera om autentiseringsservern är tillgänglig.

Antalet serverväxlingar anges som 0 till 4.

"0" anger att autentiseringsservern är tillgänglig.

Logout Mode

Utloggningsläge.

Värde	Innehåll
by User's Operation	Manuell utloggning av användaren
by Auto Logout Timer	Automatisk utloggning efter en timeout

Login Method

Anger den väg som autentiseringen tar.

Värde	Innehåll
Control Panel	Inloggningen utfördes genom kontrollpanelen.
via Network	Inloggningen utfördes på distans genom en nätverksdator.
Others	Inloggningen utfördes med en annan metod.

Login User Type

Anger typ av inloggad användare.

Värde	Innehåll
User	Allmän användare
Guest	Gästanvändare
User Administrator	Användaradministratör
Machine Administrator	Maskinadministratör
Network Administrator	Nätverksadministratör
File Administrator	Filadministratör
Supervisor	Övervakare
Customer Engineer (Service Mode)	Kundtekniker
Others	Inloggningsförfrågningar från andra användare än de som anges ovan

Target User Entry ID

Anger ingångs-ID för målanvändaren.

Detta är ett hexadecimalt id som indikerar användare som har följande inställningar:

- Lockout
- Password Change

Target User Code/User Name

Användarkod eller användarnamn för den användare vars data användes.

Om administratörens data användes, loggas administratörens användarnamn.

Address Book Registration No.

Anger registreringsnumret för användaren som utför åtgärden.

Address Book Operation Mode

Anger metod som används för att ändra data som registrerats i adressboken.

Address Book Change Item

Indikerar vilken post i adressboken som ändrades.

Address Book Change Request IP Address

Anger typ av IP-adress (IPv4/IPv6) för användaren med hjälp av adressboken.

Lockout/Release

Anger status på utlåsning.

Värde	Innehåll
Lockout	Aktivering av lösenordsutlåsning
Release	Inaktivering av lösenordsutlåsning

Lockout/Release Method

Anger den metod som används för att frigöra utlåsningen.

Värde	Innehåll
Manual	Maskinen låses upp manuellt.
Auto	Maskinen låses upp av utlåsningens frigöringstimer.

Lockout Release Target Administrator

Indikerar vilken/vilka administratörer som släpps när en upplåsning inträffar.

Counter to Clear

Anger vilket räkneverk som återställs för varje användare.

Export Target

Indikerar vilka inställningar som ska ingå i enhetens inställningsfil som ska exporteras.

Värde	Innehåll
System Settings	Systeminställningar
Printer Features	Skrivarfunktioner
Web Image Monitor Setting	Web Image Monitor-inställning

Värde	Innehåll
Web Service Settings	Webbserviceinställningar
System/Copier SP	System SP
Printer SP	Skrivare SP

Target File Name

Anger namnet på den enhetsinformationsfil som ska importeras eller exporteras.

Delete File Type

Anger typ av filborttagning.

Värde	Innehåll
Delete Normal File	Normal filborttagning
Delete Editing File	Radering under redigering
Auto Delete	Automatisk filborttagning
Others	Filborttagning av annan orsak

Collect Job Logs

Anger status för inställningen för hämtning av jobblogg.

Värde	Innehåll
Active	Inställningen för hämtning av jobblogg har aktiverats.
Inactive	Inställningen för hämtning av jobblogg har avaktiverats.
Not Changed	Inga ändringar har gjorts i inställningen för hämtning av jobblogg.

Collect Access Logs

Anger status för inställningen för hämtning av åtkomstlogg.

Värde	Innehåll
Active	Inställningen för hämtning av åtkomstlogg har aktiverats.
Inactive	Inställningen för hämtning av åtkomstlogg har avaktiverats

Värde	Innehåll
Not Changed	Inga ändringar har gjorts i inställningen för hämtning av åtkomstlogg.

Collect Eco-friendly Logs

Anger status på inställningen för hämtning av miljöanpassad logg.

Värde	Innehåll
Active	Inställningen för hämtning av miljöanpassad logg har aktiverats.
Inactive	Inställningen för hämtning av miljöanpassad logg har avaktiverats.
Not Changed	Inga ändringar har gjorts i inställningen för hämtning av miljöanpassad logg.

Transfer Logs

Anger status för inställning av överföringslogg.

Värde	Innehåll
Active	Inställning av överföringslogg har aktiverats.
Inactive	Inställning av överföringslogg har avaktiverats.
Not Changed	Inga ändringar har gjorts i inställning av överföringslogg.

Log Type

Om en loggs hämtningsnivå har ändrats anger denna funktion hur den har ändrats.

Värde	Innehåll
Job Log	Jobblogg
Access Log	Åtkomstlogg
Eco-friendly Log	Miljöanpassad logg

Log Collect Level

Anger nivån för en loggs hämtningsnivå.

Värde	Innehåll
Level 1	Nivå 1
Level 2	Nivå 2
User Settings	Användarinställningar

Encryption/Cleartext

Anger om kommunikationskryptering är aktiverat eller avaktiverat.

Värde	Innehåll
Encryption Communication	Kryptering har aktiverats.
Cleartext Communication	Kryptering har avaktiverats.

Machine Port No.

Anger skrivarens portnummer.

Protocol

Mottagarprotokoll.

"Unknown" anger att mottagarens protokoll inte har identifierats.

IP-adress

Mottagarens IP-adress.

Port No.

Mottagarens portnummer.

Portnummer anges med decimaler.

MAC-adress

Mottagarens (fysiska) MAC-adress.

Primary Communication Protocol

Anger namnet för det primära kommunikationsprotokollet.

Secondary Communication Protocol

Anger namnet för det sekundära kommunikationsprotokollet.

Encryption Protocol

Anger det protokoll som används för att kryptera kommunikationen.

Communication Direction

Anger kommunikationsriktning.

Värde	Innehåll
Communication Start Request Receiver (In)	Maskinen fick en förfrågan om att kommunicera.
Communication Start Request Sender (Out)	Maskinen skickade en förfrågan om att kommunicera.

Communication Start Log ID

Anger logg-id för kommunikationens starttid.

Detta är ett hexadecimalt id som indikerar tiden för kommunikationsstarten.

Communication Start/End

Anger den tid när kommunikationen startades och avslutades.

Network Attack Status

Anger maskinens status när nätverksattacker inträffar.

Värde	Innehåll
Violation Detected	En nätverksattack upptäcktes.
Recovered from Violation	Nätverket återställdes från en attack.
Max. Host Capacity Reached	Maskinen slutade fungera på grund av att mängden inkommande data nådde max värdkapacitet.
Recovered from Max. Host Capacity	Maskinen slutade fungera igen efter att volymen av inkommande data minskades.

Network Attack Type

Identifierar nätverkets attacktyper.

Värde	Innehåll
Password Entry Violation	Lösenordsknäckning
Device Access Violation	Denial-of-Service attack (DoS)
Request Falsification Violation	Förfalskning av begäran

Network Attack Type Details

Visar uppgifter om nätverkets attacktyper.

Värde	Innehåll
Authentication Error	Autentiseringsfel
Encryption Error	Krypteringsfel

Network Attack Route

Identifierar vägen för nätverksattacken.

Värde	Innehåll
Attack from Control Panel	Attack från en obehörig åtgärd via maskinens kontrollpanel
Attack from Other than Control Panel	Attack av en annan obehörig åtgärd via maskinens kontrollpanel

Login User Name used for Network Attack

Anger det användarnamn som nätverksangreppet utfördes av.

Add/Update/Delete Firmware

Anger den metod som användes för att lägga till, uppdatera eller radera maskinens firmware.

Värde	Innehåll
Updated with SD Card	Ett SD-kort användes för att utföra firmware-uppdateringen.
Added with SD Card	Ett SD-kort användes för att installera firmware.
Deleted with SD Card	Ett SD-kort användes för att radera firmware.
Moved to Another SD Card	Firmware flyttades till ett annat SD-kort.
Updated via Remote	Firmware uppdaterades från en fjärrdator.
Updated for Other Reasons	Uppdatering av firmware utfördes med en annan metod än någon av de ovanstående.

Module Name

Firmware-modulnamn.

Parts Number

Firmware-modulens artikelnummer.

Version

Firmware-version.

Machine Data Encryption Key Operation

Anger den typ av kryperingsnyckelprocess som utförts.

Värde	Innehåll
Back Up Machine Data Encryption Key	En säkerhetskopiering av krypteringsnyckeln utfördes.
Restore Machine Data Encryption Key	En krypteringsnyckel återställdes.
Clear NVRAM	NVRAM avmarkerades.
Start Updating Machine Data Encryption Key	En uppdatering av krypteringsnyckeln startades.
Finish Updating Machine Data Encryption Key	En uppdatering av krypteringsnyckeln slutfördes.

Machine Data Encryption Key Type

Identifierar typ av krypteringsnyckel.

Värde	Innehåll
Encryption Key for Hard Disk	Krypteringsnyckel för hårddisk
Encryption Key for NVRAM	Krypteringsnyckel för NVRAM
Device Certificate	Enhetscertifikat

Validity Error File Name

Anger namnet på den fil där ett giltighetsfel upptäcktes.

Configuration Category

Visar kategorierna med ändrade inställningar.

Värde	Innehåll
User Lockout Policy	Princip om utelåsning
Auto Logout Timer	Timer för automatisk utloggning
Device Certificate	Enhetscertifikat
IPsec	IPsec

Värde	Innehåll
WIM Auto Logout Timer	Web Image Monitor auto logout timer
Extended Security	Utökad säkerhet
Firmware Update Start	Uppdatering av firmware
Prohibit printing stored files from Web Image Monitor	Förhindra att lagrade filer skrivs ut från Web Image Monitor

Configuration Name/Configuration Value

Anger attribut för kategorierna.

Anger värden för attributen.

Attribut	Beskrivning
Lockout	Huruvida utelåsningen är aktiv (Active) eller inaktiv (Inactive) registreras.
Number of Attempts before Lockout	Antalet gånger en användare kan ange ett lösenord registreras.
Lockout Release Timer	Huruvida timern för utelåsning är aktiv (Active) eller inaktiv (Inactive) registreras.
Lock Out User for	Tid fram till utelåsning registreras.
Auto Logout Timer	Om automatisk utloggning är inställt på (On) eller (Off) registreras.
Auto Logout Timer(seconds)	Tid fram till automatisk utloggning registreras.
Operation Mode	Åtgärdstyp registreras.
Certificate No.	Numret på det certifikat som ska användas registreras.
Certificate No.: IEEE 802. 1X (WPA/WPA2)	Numret på det certifikat som ska användas för program registreras. När inget certifikat används registreras "Do not Use".
Certificate No.: IPsec	Numret på det certifikat som ska användas för program registreras. När inget certifikat används registreras "Do not Use".

Attribut	Beskrivning
IPsec	Huruvida IPsec är aktivt (Active) eller inaktivt (Inactive) registreras.
Encryption Key Auto Exchange: Setting1-4: Remote Address	Fjärradressen registreras.
Encryption Key Auto Exchange: Setting1-4, Default: Security Level	Säkerhetsnivån registreras. När [Enbart autentisering] har valts registreras "Authentication Only". När [Autentisering och låg krypteringsnivå] har valts registreras "Authentication and Low Level Encryption". När [Autentisering och hög krypteringsnivå] har valts registreras "Authentication and High Level Encryption". När [Användarinställningar] har valts registreras "User Settings".
Encryption Key Auto Exchange: Setting1-4, Default: Authentication Method	Den autentiseringsmetod som används för automatiskt byte av nyckelformat registreras. Antingen "PSK" eller "Certificate" registreras.
WIM Auto Logout Timer (minutes)	Web Image Monitors logg av timern för automatisk utloggning registreras i steg om en minut.
Update Firmware	En loggpost som rapporterar ändringar i inställningarna för [Uppdatera firmware] har registrerats. "Prohibit" eller "Do not Prohibit" har registrerats.
Change Firmware Structure	En loggpost som rapporterar ändringar i inställningarna för [Ändra firmwarestruktur] har registrerats. "Prohibit" eller "Do not Prohibit" har registrerats.
Firmware Update Start	En loggpost som rapporterar uppdatering av firmware har registrerats.
Prohibit printing stored files from Web Image Monitor	En loggpost som rapporterar ändringar i inställningarna för [Förhindra att lagrade filer skrivs ut från Web Image Monitor] har registrerats. "Prohibit" eller "Do not Prohibit" har registrerats.

Destination Server Name

Anger namnet på målservern dit spårningsinformationen inte skickades när loggtypen är "Enhanced Print Volume Use Limitation: Tracking Permission Result".

Anger namnet på den server från vilken uppgifterna om export- eller importbegäran utfärdades när loggtypen är för import eller export av inställningsinformation.

HDD Format Partition

Visar orsaken till formatering av hårddisken.

Värde	Innehåll
HDD Exchange	Hårddisken har bytts ut.
Problem with HDD Encryption Key	Problem med hårddiskens krypteringsnyckel.
Problem with Disk Label	Diskens etikett kan inte läsas.
Problem with File System	Problem med filsystemet.

Access Result

Indikerar resultaten av loggade åtgärder.

Värde	Innehåll
Completed	En åtgärd har slutförts.
Failed	En åtgärd misslyckades.

Jobblogg (källa)

Source

Anger källan för jobbfilen.

Värde	Innehåll
Printer	Jobbfilen skickades från skrivardrivrutinen.
Report	Jobbfilen var en utskriven rapport.

Start Date/Time

Visar när "Printer"-jobbet satts igång.

End Date/Time

Visar när "Printer"-jobbet avslutats.

Print File Name

Namn på "Printer"-filer.

Jobblogg (mål)

Target

Typ av jobbmål.

Värde	Innehåll
Print	Skriv ut

Start Date/Time

Visar när "Print"-jobbet startats.

End Date/Time

Indikerar när "Print"-jobbet avslutats.

Informationsposter för miljöanpassade loggar

Start Date/Time

Händelsens startdatum och starttid registreras.

End Date/Time

Händelsens slutdatum och sluttid registreras.

Log Type

Typ av miljöanpassad logg registreras.

Värde	Innehåll
Main Power On	Huvudström på
Main Power Off	Huvudström av
Power Status Transition Result	Resultat för strömstatusövergång
Job Related Information	Jobbrelaterad information
Paper Usage	Pappersförbrukning
Power Consumption	Effektförbrukning

Log Result

Om händelsen har avslutats eller inte visas.

Värde	Innehåll
Completed	Slutförd
Failed	Misslyckades

Result

Resultatet av händelsen registreras.

Värde	Innehåll
Succeeded	Lyckades
Failed	Misslyckades

Log ID

Anger det ID som tilldelats loggen. Detta är ett hexadecimalt ID som identifierar loggen.

Power Mode

Maskinens strömstatus (efter statusövergång) loggas.

Värde	Innehåll
Standby	Vänteläge
Low Power	Låg effektförbrukning, status
Silent	Ljudlös, status
HDD On	HD på, status
Engine Off	Motor av, status
Controller Off	Controller av, status
STR	STR, status
Silent Print	Ljudlös utskrift, status
Low Power Print	Låg effektförbrukning, utskriftsstatus
Fusing Unit Off	Fixeringsenhet Av, status

Log Type

Jobbets loggtyp registreras.

Job Interval (seconds)

Indikerar förfluten tid från start av föregående jobb till start av aktuellt jobb.

Job Duration (seconds)

Indikerar förfluten tid från start till avslutat jobb.

Paper Usage (Large Size)

Indikerar antal ensidiga utskrifter per timma på stort format.

Stort format avser A3 (11 × 17 tum) eller större.

Paper Usage (Small Size)

Indikerar antal ensidiga utskrifter per timma på litet format.

Litet format avser mindre än A3 (11×17 tum) eller mindre.

Paper Usage (2 Sided: Large Size)

Indikerar antal dubbelsidiga utskrifter per timma på stort format.

Stort format avser A3 (11 × 17 tum) eller större.

Paper Usage (2 Sided: Small Size)

Indikerar antal dubbelsidiga utskrifter per timma på litet format.

Litet format avser mindre än A3 (11×17 tum) eller mindre.

Detected Power

Maskinens strömförbrukning mäts och registreras i loggen medan maskinen används.

Värde	Innehåll
Controller Standby	Controllers vänteläge
STR	Stäng av till RAM-läge (STR)
Main Power Off	Huvudströmbrytaren är frånslagen.
Printing	Maskinens utskriftsstatus
Engine Standby	Maskinens vänteläge
Engine Low	Maskinens lågeffektstatus
Engine Night	Maskinens ljudlösa status
Engine Total	Maskinens totala elförbrukning
Fusing Unit Off	Fixeringsenhet Av, status

Power Consumption(Wh)

Anger energiförbrukningen i varje energisparläge.

Ange inställningar för hämtning av loggar

Aktivera insamlingsinställningarna för varje loggtyp och konfigurera nivån för hämtning.

Nivå för hämtning av jobbloggar

Om "Nivå för Hämtning av Jobbloggar" ställs in på [Nivå 1] hämtas alla jobbloggar.

Nivå för hämtning av åtkomstloggar

Om "Nivå för hämtning av åtkomstloggar" ställs in på [Nivå 1] registreras följande information i åtkomstloggen:

- HDD-format
- Borttagning av alla loggar
- Ändring av logginställningar
- Ändring av logghämtningsposter

Om "Nivå för hämtning av åtkomstloggar" ställs in på [Nivå 2] hämtas alla åtkomstloggar.

Nivå för hämtning av miljöanpassade loggar

Om "Nivå för hämtning av miljöanpassade loggar" ställs in på [Nivå 1] hämtas inte miljöanpassade loggar.

Om "Nivå för hämtning av miljöanpassade loggar" ställs in på [Nivå 2] hämtas alla miljöanpassade loggar.

1. **Logga in som maskinadministratör från Web Image Monitor.**
2. **Peka på [Enhetshantering] och klicka sedan på [Konfiguration].**
3. **Klicka på [Loggar] under "Enhetsinställningar".**
4. **Välj [Aktivt] för funktionerna: "Hämta jobbloggar", "Hämta åtkomstloggar" och "Hämta miljöanpassade loggar".**
5. **Ange hämtningsnivå för var och en av funktionerna "Nivå för Hämtning av Jobbloggar", "Nivå för hämtning av åtkomstloggar" och "Nivå för hämtning av miljöanpassade loggar".**

   När en nivå ändras, ändras logguppgifternas valstatus därefter.

   För att ändra enskilda objekt i logguppgifterna, konfigurera inställningar för varje enskilt objekt. Även om hämtningsnivån är inställd på [Nivå 1] eller [Nivå 2] när varje objekt bland logguppgifterna ändras, så ändras nivån till [Användarinställningar].
6. **Klicka på [OK].**

7. **"Uppdaterar..." visas. Avvakta i 1 eller 2 minuter och klicka sedan på [OK].**

   Om den föregående skärmbilden inte visas igen när du klickar på [OK], vänta en stund och klicka sedan på uppdateringsknappen i webbläsaren.

8. **Logga ut.**

Obs

- Ju högre värde som anges för "Nivå för hämtning av åtkomstloggar", desto fler loggar samlas in.

Ladda ned loggar.

Använd följande process för att konvertera de loggar som är lagrade i maskinen till en CSV-fil för grupphämtning.

För att hämta loggar, konfigurerar du hämtningsinställningarna för jobbloggen, åtkomstloggen och den miljöanpassade loggen till [Aktivt].

Den här inställningen kan anges i [Loggar] under [Konfiguration] i Web Image Monitor.

1. **Logga in som maskinadministratör från Web Image Monitor.**
2. **Peka på [Enhetshantering] och klicka sedan på [Konfiguration].**
3. **Klicka på [Ladda ner loggar] under "Enhetsinställningar".**
4. **Välj vilken typ av logg som ska hämtas i rullgardinsmenyn i "Loggar att hämta".**

   Säkerhetsloggen innehåller 2 typer av loggar: jobblogg och åtkomstlogg.

5. **Klicka på [Hämta].**
6. **Ange i vilken mapp du vill spara filen.**
7. **Klicka på [Tillbaka].**
8. **Logga ut.**

Obs

- Nedladdade loggar innehåller data som registrerats fram till du klickar på knappen [Ladda ner]. Loggar som registreras efter att du klickar på knappen [Ladda ner] kommer inte att laddas ner. Fältet "Result", loggposten för ej genomförda arbeten kommer att vara tom.
- Nerladdningstiden kan variera beroende på antalet loggar.
- Om ett fel inträffar under tiden CSV-filen laddas ner eller skapas, avbryts nedladdningen och info om felet inkluderas i slutet av filen.
- Om en logg har laddats ner visas "Download completed." på den sista raden i loggfilen.
- Mer information om hur du sparar CSV-loggfiler finns i webbläsarens hjälp.
- I hämtade loggfiler används UTF-8-teckenkodning. Om du vill visa en loggfil öppnar du den med ett program som stödjer UTF-8.

- För mer information om poster som finns i loggarna, se s. 150 "Attribut för loggar du kan ladda ner".

Antal loggar som kan förvaras i maskinen

När begränsningen för antalet jobbloggar, åtkomstloggar eller miljöanpassade loggar som kan sparas i maskinen överskrids och nya loggar genereras skrivs de gamla loggarna över av de nya. Om loggar inte laddas ner med jämna mellanrum kan det hända att det inte går att spara de gamla loggarna på filer.

När du använder Web Image Monitor för att hantera loggar ska du hämta loggar enligt de villkor som visas i tabellen.

När du laddat ner loggarna ska du utföra en batchradering av loggarna.

Om du ändrar inställningen [Hämta] / [Hämta ej] för logginsamling måste du utföra en batchradering av loggarna.

Det högsta antalet loggar som kan lagras i maskinen

Loggtyper	Max antal loggar
Jobbloggar	4 000
Åtkomstloggar	12 000
Miljöanpassade loggar	4 000

Beräknat antal loggar som skapas per dag

Loggtyper	Antal loggar som skapas per dag
Jobbloggar	100
Åtkomstloggar	300 Detta antal baseras på 100 åtgärder, exempelvis start- och åtkomståtgärder över webben, samt 200 jobbposter (2 poster per jobb: 1 inloggnings- och 1 utloggningspost).
Miljöanpassade loggar	100

Enligt dessa villkor kan maskinen behålla loggar i 40 dagar utan att behöva skriva över. Vi rekommenderar att man laddar ner loggar var 20:e dag ifall fel skulle inträffa.

Maskinadministratören bör hantera nedladdade loggfiler på ett lämpligt sätt.

Obs

- Utför inga åtgärder som skapar nya loggposter under tiden loggar laddas ner, eftersom loggar inte kan registrera nya poster under nedladdning.
- Batchradering av loggar kan utföras från kontrollpanelen eller via Web Image Monitor.

Meddelande om åtgärd när antalet loggposter når maximalt antal

Om antalet loggar som kan lagras i skrivaren överskrider den angivna begränsningen, skrivs de äldsta loggarna över av nya. Maximalt antal loggar som kan lagras anges för varje jobblogg, åtkomstlogg och miljöanpassad logg.

Jobbloggen och åtkomstloggen hämtas hämtas båda som en enda fil.

"Om loggar hämtas utan att skrivas över" nedan indikerar att jobbloggen och åtkomstloggen har kombinerats efter att de laddats ned.

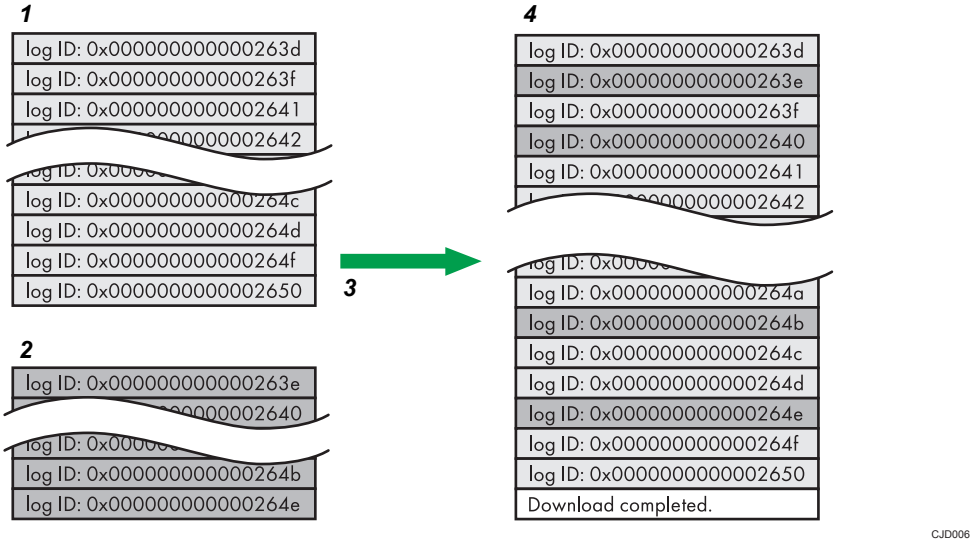
"Om loggar hämtas medan överskrivning pågår" nedan indikerar att delar av åtkomsloggen har skrivits över.

I detta exempel skrivs en del av åtkomstloggen över och tas bort då en annan logg hämtas.

Den miljöanpassade filen hämtas som en egen fil.

Loggposter skrivs över i prioritetsordning. Loggposter med högre prioritet skrivs inte över, eller tas inte bort.

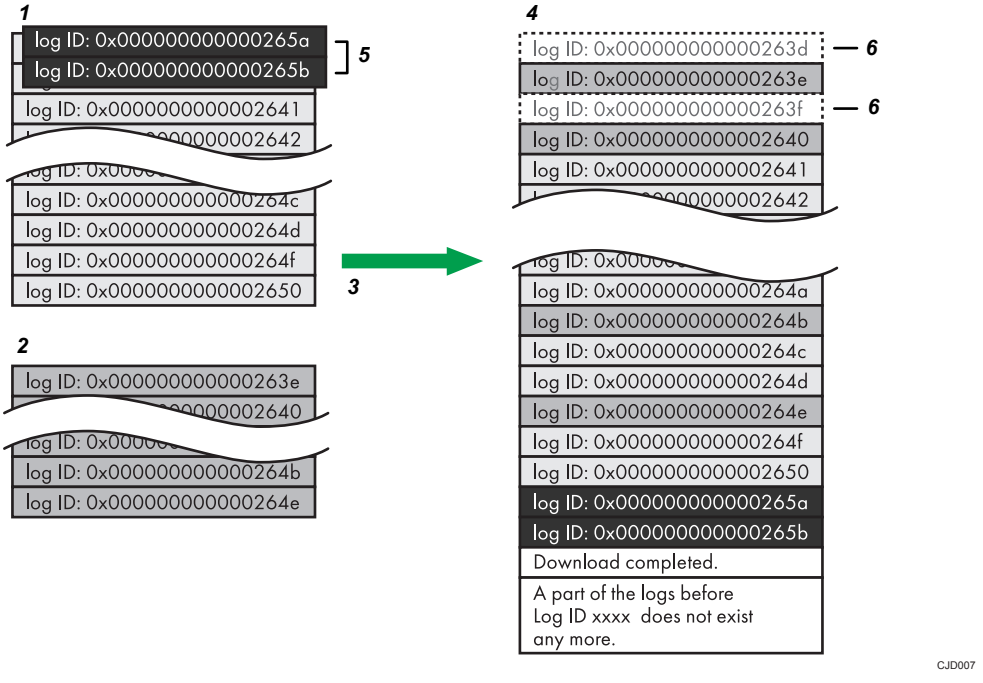
Om loggar laddas ner utan överskrivning



1. **Åtkomstlogg**
2. **Jobblogg**

3. **Ladda ner**
4. **Nerladdade loggar**

Om loggar laddas ner under överskrivning



1. **Åtkomstlogg**
2. **Jobblogg**
3. **Ladda ner**
4. **Nerladdade loggar**
5. **Överskrivning**
6. **Raderade genom överskrivning**

Kontrollera meddelandet på den sista raden av de nedladdade loggarna för att avgöra om överskrivning inträffade eller inte medan loggarna laddades ner.

- Om överskrivning inte inträffat kommer den sista raden att innehålla följande meddelande: Download completed.
- Om överskrivning skedde kommer den sista raden att innehålla följande meddelande: Download completed. A part of the logs before Log ID xxxx does not exist any more.

Obs

- Om överskrivning inträffar kommer en del av loggarna att raderas av överskrivningen. Kontrollera därför loggen "Log ID xxxx" samt nyare loggar.

Utskriftsjobbsloggar

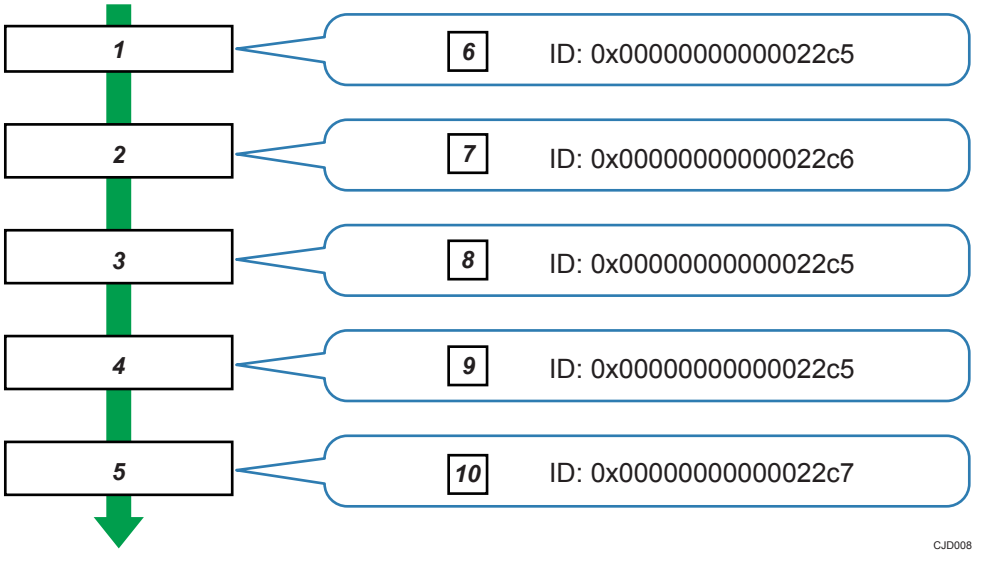
Utskriftsloggposter registreras innan inloggningsposten registreras i åtkomstloggen.

Information om jobb (mottagning, bearbetning, utmatning av jobbdata, osv.) registreras som enskilda poster.

När maskinen tar emot ett utskriftsjobb skapar den ett ID för jobbet och registrerar det i jobbloggen. Maskinen skapar sedan ett inloggnings-ID för utskriftsjobbet och registrerar det i åtkomstloggen. Efter detta skapar den en jobbloggpost för information om jobbet som bearbetats samt utmatning (under samma inloggnings-ID). När maskinen slutför bearbetning av jobbet skapar den en utloggningspost och registrerar den i åtkomstloggen.

Poster för information om åtgärder såsom mottagning, bearbetning och utmatning av utskriftsjobb skapas först i jobbloggen och registrerar sedan inloggnings- och utloggningsinformation om dessa jobb i åtkomstloggen.

Flödeschema över utskriftsjobb



1. **Utskriftsjobbdata har mottagits.**
2. **Autentiseringsdata (inloggning) har mottagits.**
3. **Utskriftsjobb bearbetas.**
4. **Utskriftsjobb matas ut.**
5. **Autentiseringsdata (inloggning) har mottagits.**
6. **Ett ID tilldelas utskriftjobbet och registreras som en post i jobbloggen.**
7. **Autentiseringsdata (inloggning) registreras som en post i åtkomstloggen.**
8. **Information om bearbetningen av utskriftsjobbet registreras som en post i jobbloggen (med hjälp av samma ID).**

9. **Information om utmatning av utskriftsjobbet registreras som en post i Jobbloggen (med hjälp av samma ID).**
10. **Autentiseringsdata (utloggning) regisreras som en post i Åtkomstloggen.**

Radera alla loggar

Använd följande metod för att ta bort alla loggar som är lagrade på maskinen.

"Radera alla loggar" visas om en av jobbloggarna, åtkomstloggarna eller de miljöanpassade loggarna är inställda på [Aktiv].

1. **Logga in som maskinadministratör från Web Image Monitor.**
2. **Peka på [Enhetshantering] och klicka sedan på [Konfiguration].**
3. **Klicka på [Loggar] under "Enhetsinställningar".**
4. **Klicka på [Ta bort] under "Radera alla loggar".**
5. **Klicka på [OK].**
6. **Logga ut.**

Avaktivera loggöverföring till logghämtningsservern

Använd följande process för att avaktivera loggöverföring till logghämtningsservern. Observera att du bara kan ändra inställningen för loggöverföring till [Ej aktivt] om den redan är inställd på [Aktivt].

1. **Logga in som maskinadministratör från Web Image Monitor.**
2. **Peka på [Enhetshantering] och klicka sedan på [Konfiguration].**
3. **Klicka på [Loggar] under "Enhetsinställningar".**
4. **Välj [Ej aktivt] i området [Överför loggar] under "Inställningar som är gemensamma för alla loggar".**
5. **Klicka på [OK].**
6. **Logga ut.**

Hantera loggar från maskinen

Du kan ange inställningar för t.ex. logghämtning, om loggar ska överföras till logghämtningsservern och om alla loggar ska tas bort.

Ange inställningar för hämtning av loggar

Aktivera hämtningsinställningarna för respektive loggtyp.

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck 3 gånger på [▼Nästa].**
5. **Tryck på [Samla in loggar].**
6. **Välj [Aktivt] för funktionerna: "Jobblogg", "Åtkomstlogg" och "Miljöanpassade loggar".**
7. **Tryck på [OK].**
8. **Logga ut.**
9. **Stäng av huvudströmbrytaren och slå sedan på den igen.**

Avaktivera loggöverföring till logghämtningsservern

Använd följande process för att avaktivera loggöverföring från maskinen till logghämtningsservern. Observera att du endast kan ändra inställningen för loggöverföring till [Av] om den är inställd på [På].

För mer information om logghämtningsservern, kontakta din säljare.

För mer information om inställningen för loggöverföring, se Handboken för logghämtningsservern.

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa] två gånger.**
5. **Tryck på [Överför logg-inställning].**
6. **Tryck på [Av].**
7. **Tryck på [OK].**
8. **Logga ut.**

Ange Radera alla loggar

Använd följande metod för att ta bort alla loggar som är lagrade på maskinen.

Du kan endast ta bort alla loggar från maskinen samtidigt om logghämtningsservern används, eller om inställningen för Web Image Monitor har angetts för att hämta jobblogg, åtkomstlogg eller miljöanpassad logg.

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa] två gånger.**
5. **Tryck på [Radera alla loggar].**
6. **Tryck på [Ja].**
7. **Tryck på [Avsluta].**
8. **Logga ut.**

Hantera loggar från logghämtningsservern

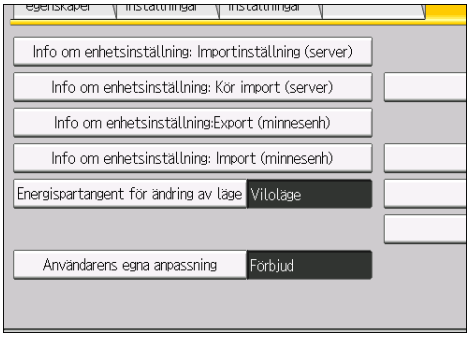
För mer information om hur du använder logghämtningsservern för att hantera loggfiler, se handboken som medföljer logghämtningsservern.

Konfigurera startskärmen för enskilda användare

Det gör det möjligt för varje användare att använda hans eller hennes startskärm.

När en användare loggar in visas den anpassade startskärmen.

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck 3 gånger på [▼Nästa].**
5. **Tryck på [Användarens egna anpassning].**



6. **Tryck på [Tillåt], följt av [OK].**
7. **Logga ut.**

Obs

- Detta kan även konfigureras via Web Image Monitor. För mer information, se hjälpen till Web Image Monitor.
- Startsidesinformationen för varje användare sparas även när "Användarens egna anpassning" är inställd på [Förhindra]. När inställningen ändras tillbaka till [Tillåt] kan informationen användas på nytt.

Varningar avseende användning av användares egna startskärmar

Observera dessa varningar innan du använder denna funktion.

- När en användare registreras i adressboken skapas en startsida för den användaren. Användarens egna startskärm konfigureras med standardinställningarna (placering av ikoner).
- Om Menyskydd är inställt på antingen [Nivå 1] eller [Nivå 2] kan användaren inte använda funktionens programregistrering, redigera eller ta bort skärmen. Användaren kan däremot lägga till ikoner på sin startskärm.

- När Menyskydd är inställt på antingen [Nivå 1] eller [Nivå 2] kan du be maskinadministratören att skapa alla nödvändiga program.
- Endast de ikoner som leder till funktioner som användaren har behörighet att använda visas.
- När en användare raderas från adressboken raderas även användarens startskärmsinformation.
- När en användare redigerar ett program reflekteras dessa ändringar på de användares startskärmar där denna programikon finns.
- När en användare tar bort ett program, tas programmets ikon bort från alla användares startskärmar där denna programikon fanns.
- Eftersom varje användare kan anpassa sin startskärm kan administratören inte kontrollera varje användares startinformation.

Hantera enhetsinformation

⚠FÖRSIKTIGT

- Se till att SD-kort och USB-minnen hålls utom räckhåll för barn. Kontakta läkare omdelbart om ett barn råkar svälja ett SD-kort eller USB-minne.

Maskinens enhetsinformation kan anges av en administratör med behörighet att hantera enheter, användare, nätverk och filer.

Maskinens enhetsinformation kan exporteras till en extern enhet i form av en informationsfil för enhetsinställning. Genom att importera en exporterad informationsfil med enhetsinställningar till maskinen, kan du använda den som en säkerhetskopia för att återställa enhetsinställningarna.

Genom att hantera informationsfilen med enhetsinställning via enhetshanteringsservern kan informationsfilen med enhetsinställning importeras regelbundet, antingen vid en viss tidpunkt eller varje gång enheten startas.

Data som kan importeras och exporteras

- Skrivarinställningar
- Inst f Web Image Monitor
- Inställningar för webbservice
- Systeminställningar

Data som inte kan importeras eller exporteras

- Vissa systeminställningar *1 *2

*1 Datuminställning, inställningar som kräver enhetscertifikat och inställningar som behöver justeras för varje maskin (t.ex. inställningar för bildjustering) kan varken importeras eller exporteras.

*2 Inställningar endast för utförande av funktioner och inställningar endast för visning kan inte importeras eller exporteras.

- Inställningar för utökade funktioner
- Adressbok
- Program (skrivarfunktion)
- Inställningar som kan anges via telnet
- @Remote-relaterad data
- Räknare
- Inställningar för extern skrivarenhet
- Inställningar som endast kan anges via Web Image Monitor eller webbtjänst (exempelvis Bonjour, SSDP-inställning)

Obs

- Filformatet för export är CSV.

- Maskinen som informationsfilen med enhetsinställningar importeras till måste var inställd på samma sätt som maskinen varifrån informationsfilen med enhetsinställningar exporteras. Annars kan informationsfilen med enhetsinställningar inte importeras.
- Import och export mellan maskiner är endast möjligt om deras modeller, användningsregion samt följande enhetskonfiguration matchar.
  - Papperskassett
  - Utmatningsfack
  - Om de är utrustade med en efterbehandlare eller inte, samt typen av efterbehandlare
- Om enhetsinställningarna har ändrats exporterar du den uppdaterade informationsfilen med enhetsinställningar.
- Om det finns maskiner med samma enhetsinställningar kan du ställa in dem på exakt samma sätt genom att importera samma enhetsinställningsfil.
- Om det finns bildfiler i JPG-format på startskärmen exporteras de också.
- Medan en användare använder maskinen kan ingenting importeras eller exporteras förrän användaren slutför åtgärden.
- Under export och import kan maskinen inte utföra någon annan åtgärd.
- För detaljer om hantering av SD-kort, se Getting Started..
- Du kan även använda Web Image Monitor för att konfigurera inställningarna för import, export and server.

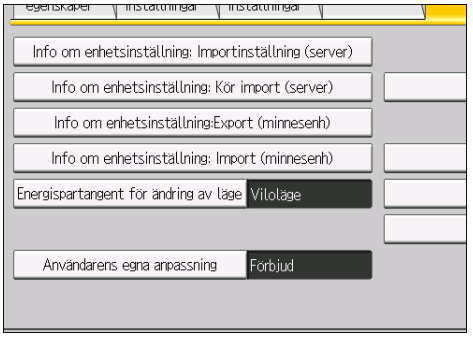
Exportera enhetsinformation

När enhetsinformation exporteras från kontrollpanelen sparas uppgifterna på ett SD-kort.

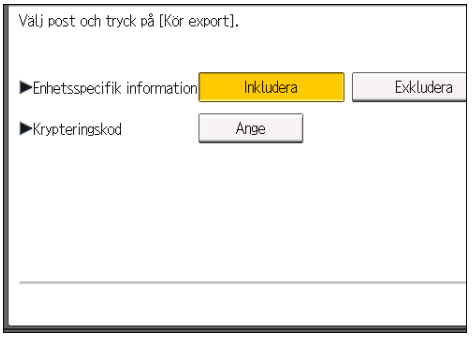
1. **Sätt in ett SD-kort i kortplatsen på sidan av kontrollpanelen.**

   För information om hur man ansluter SD-kortet, se handboken Getting Started (Komma igång).
2. **Logga in på kontrollpanelen som administratör med administratörs-, maskinadministratörs-, nätverksadministratörs- och filadministratörsbehörighet.**
3. **Tryck på [Systeminställning].**
4. **Tryck på [Admin.verktyg].**
5. **Tryck 3 gånger på [▼Nästa].**

6. **Tryck på [Info om enhetsinställning: Export (minnesenh)].**



7. **Ange villkoren för export.**



- Ange om du vill [Inkludera] eller [Exkludera] "Enhetsspecifik information". Enhetsspecifik information" omfattar IP-adress, värdnamn osv.
- Ange en krypteringskod.

8. **Tryck på [Kör export].**
9. **Tryck på [OK].**
10. **Tryck på [Avsluta].**
11. **Logga ut.**

Obs

- Om import eller export misslyckas kan du granska loggen efter fel. Loggen lagras på samma plats som den exporterade informationsfilen med enhetsinställningar.

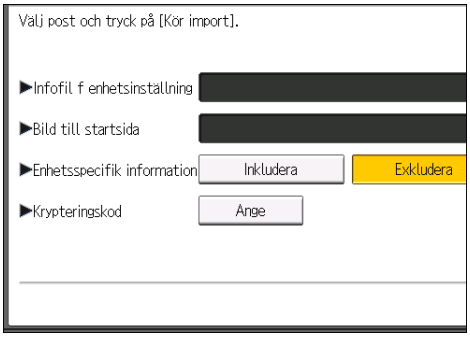
Importera enhetsinformation

Importera enhetsinformation som sparats på ett SD-kort.

1. **Sätt in ett SD-kort i kortplatsen på sidan av kontrollpanelen.**

   För information om hur man ansluter SD-kortet, se handboken Getting Started (Komma igång).

2. **Logga in på kontrollpanelen som administratör med administratörs-, maskinadministratörs-, nätverksadministratörs- och filadministratörsbehörighet.**
3. **Tryck på [Systeminställning].**
4. **Tryck på [Admin.verktyg].**
5. **Tryck 3 gånger på [▼Nästa].**
6. **Tryck på [Info om enhetsinställning: Importinställning (minnesenhet)].**
7. **Konfigurera importvillkoren.**



   - Tryck på [Välj] på "Infofil f enhetsinställning" för att välja de filer som ska importeras.
   - När du ska lägga till en bild på startsidan, tryck på [Välj] för "Bild till startsida" och välj sedan fil.
   - Ange om du vill [Inkludera] eller [Exkludera] "Enhetsspecifik information". Enhetsspecifik information" omfattar IP-adress, värdnamn osv.
   - Ange krypteringsnyckeln som skapades när filen exporterades.
8. **Tryck på [Kör import].**
9. **Tryck på [OK].**
10. **Tryck på [Avsluta].**

    Maskinen startas om.

Obs

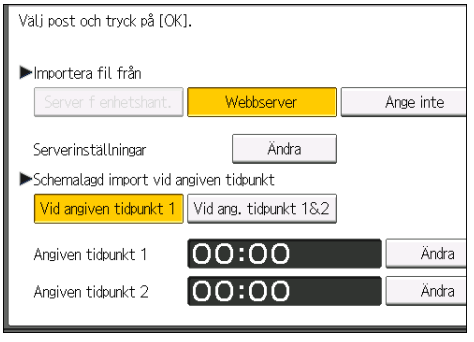
- Om import eller export misslyckas kan du granska loggen efter fel. Loggen lagras på samma plats som den exporterade informationsfilen med enhetsinställningar.

Regelbunden import av enhetsinformation

Denna inställning importerar automatiskt enhetsinformation som har lagrats på en server till maskinen.

1. **Logga in på kontrollpanelen som administratör med administratörs-, maskinadministratörs-, nätverksadministratörs- och filadministratörsbehörighet.**
2. **Tryck på [Systeminställning].**

3. **Tryck på [Admin.verktyg].**
4. **Tryck 3 gånger på [▼Nästa].**
5. **Tryck på [Info om enhetsinst: Importera inställning (server)]**
6. **Konfigurera importvillkoren.**



- Välj källa för import av filer. Konfigurera inställningar som t.ex. URL, användarnamn, lösenord osv, med hjälp av serverns detaljinställningar.
- Välj frekvens för import av infofiler för enhetsinställning och ställ in klockslag för regelbunden import.
- Välj om du vill importera en infofil för enhetsinställning om den är identisk med senast importerad fil.
- När den infofil för enhetsinställning som ska importeras är krypterad ska du konfigurera en krypteringsnyckel.
- Välj om du vill skicka ett e-postmeddelande till maskinadministratören när import misslyckas.

7. **Tryck på [OK].**
8. **Logga ut.**

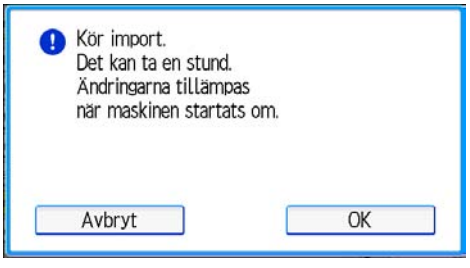
Obs

- Detta kan även konfigureras via Web Image Monitor. För mer information, se hjälpen till Web Image Monitor.
- När enhetsinställningsservern används kan mer detaljerade importinställningar göras. För mer information, se Handboken för enhetsinställningsservern.
- Om import eller export misslyckas kan du granska loggen efter fel. Loggen lagras på samma plats som den exporterade informationsfilen med enhetsinställningar.

Manuell import av en servers infofil för enhetsinställning

Manuell import av en servers infofil för enhetsinställning som angetts med [Info om enhetsinställning: Importinställning (server)].

1. **Logga in på kontrollpanelen som administratör med administratörs-, maskinadministratörs-, nätverksadministratörs- och filadministratörsbehörighet.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck 3 gånger på [▼Nästa].**
5. **Tryck på [Info om enhetsinställning: Kör import (server)].**
6. **Tryck på [OK].**



7. **Tryck på [Avsluta].**

   Maskinen startas om.

Obs

- Om import eller export misslyckas kan du granska loggen efter fel. Loggen lagras på samma plats som den exporterade informationsfilen med enhetsinställningar.

Felsökning

Om ett fel inträffar ska du först kontrollera loggens resultatkod. Andra värden än 0 indikerar att ett fel har inträffat. Resultatkoden visas i det inringade området nedan.

Exempel på en loggfil

CJD023

Om du inte kan lösa problemet eller inte vet hur du ska lösa det efter att du kontrollerat koden, skriv ner loggposten med felet och kontakta sedan din servicerepresentant.

ResultCode	Orsak	Lösningar
2 (INVALID REQUEST)	Det gjordes ett försök av filimport mellan olika modeller eller maskiner med olika enhetskonfigurationer.	Importera filer som exporterats från samma modell med samma enhetskonfiguration.
4 (INVALID OUTPUT DIR)	Kunde inte skriva enhetsinformationen till mottagarenheten.	Kontrollera om destinationsenheten fungerar normalt.
7(MODULE ERROR)	Ett oväntat fel inträffade under en import eller export.	Stäng av och slå på strömmen och försök sedan utföra åtgärden igen. Om felet kvarstår kontaktar du en servicetekniker.
8 (DISK FULL)	Det tillgängliga lagringsutrymmet på det externa mediet är otillräckligt.	Utför åtgärden igen efter att ha försäkrat dig om att det finns tillräckligt med lagringsutrymme.
9 (DEVICE ERROR)	Kunde inte skriva eller läsa loggfilen.	Kontrollera om sökvägen till mappen där filen ska lagras eller mappen i vilken filen lagras är otillgänglig.

ResultCode	Orsak	Lösningar
10 (LOG ERROR)	Misslyckades med att skriva ut loggfilen. Hårddisken är defekt.	Kontakta en servicetekniker.
20 (PART FAILED)	Kunde inte importera vissa inställningar.	Anledningen till felet registreras i "NgName". Kontrollera koden. **Orsak till felet (NgName)** 2 INVALID VALUE Det angivna värdet överstiger det tillåtna intervallet. 3 PERMISSION ERROR Behörighet för att ändra inställningen är otillgänglig. 4 NOT EXIST Inställningen existerar inte i systemet. 5 INTERLOCK ERROR Inställningen kan inte ändras på grund av systemets status eller sammankoppling med andra angivna inställningar. 6 OTHER ERROR Inställningen kan av något annat skäl inte ändras.
21 (INVALID FILE)	Kunde inte importera filen på grund av att den är i fel format i det externa mediet.	Kontrollera om filformatet är korrekt. Loggen är i form av en CSV-fil.
22 (INVALID KEY)	Krypteringsnyckeln är ogiltig.	Använd rätt krypteringsnyckel.

Hantera miljöanpassat räkneverk

När användarautentisering används visas information om miljöanpassat räkneverk vid inloggningen.

Det miljöanpassade räkneverket anger hur ofta färg-, duplex- och kombinerade utskrifter används i förhållande till det totala antalet utskrivna blad.

Det miljöindexet anger även hur mycket toner och papper som sparas. Ett högre miljöindex resulterar i ökad resursbesparing.

Obs

- När grundläggande, Windows- eller LDAP-autentisering används sammanställer maskinen all data och visar varje användares miljöanpassade räkneverk.
- När autentisering av användarkoden används för användarautentisering, eller när användarautentisering inte användas, sammanställs all data och visas i ett övergripande miljöanpassat räkneverk.

Konfigurera miljöanpassade räkneverk

Ställ in beräkningsperioden för det miljöanpassade räkneverkets uppgiftsinsamling och ange ett administratörsmeddelande.

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [Miljöanpassat räkenverksintervall/administratörsmeddelande].**
5. **Ändra inställningar.**
6. **Tryck på [OK].**
7. **Tryck på [Avsluta].**
8. **Logga ut.**

Räkneverksintervall

Ställ in beräkningsperioden för det miljöanpassade räkneverkets uppgiftsinsamling.

När [Ange dagar] har valts samlar det miljöanpassade räkneverket in data in under angivet antal dagar.

Standard: [**Räkna inte**]

Administratörsmeddelande

Välj ett meddelandet som ska visas när en användare loggar in.

Om du väljer "Fast meddelande 1" eller "Fast meddelande 2" visas ett standardmeddelande.

Om du väljer "Användarmeddelande" kan maskinadministratören ange ett meddelande som ska visas.

Standard: [Fast meddelande 1]

Visa informationsfönster

Ange om informationsskärmen ska visas vid inloggning.

Standard: [Av]

Visa tid

Ange när informationsskärmen visas.

Standard: [Logga in varje gång]

Återställa en maskins miljöanpassade räkneverk.

En maskins miljöanpassade räkneverk kan återställas.

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [Visa/Rensa miljöanpassat räkneverk].**
5. **Tryck på [Nollställ aktuellt värde] eller [Nollställ och tidigare värde].**
6. **Tryck på [OK].**
7. **Logga ut.**

Återställa användares miljöanpassade räkneverk

Genom att återställa användares miljöanpassade räkneverk, återställs alla användares miljöanpassade räkneverk.

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [Visa/Rensa miljöanpassat räkneverk per användare].**
5. **Tryck på [Nollställ aktuellt värde] eller [Nollställ och tidigare värde].**
6. **Tryck på [OK].**
7. **Logga ut.**

Hantera adressboken

Ange Radera användare automatiskt i adressboken

Ange hur maskinen hanterar en begäran om automatisk registrering när registrerade uppgifter i adressboken når sin maxgräns.

Om du anger detta till [På], läggs nya användarkonton till genom att automatiskt ta bort gamla användarkonton. Konton som inte har använts under längst tid raderas först.

Om du anger detta till [Av] raderas inte gamla användarkonton vilket betyder att nya användarkonton inte kan läggas till när maxgränsen för registrerade uppgifter har nåtts.

1. **Logga in som användaradministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [Radera användare automatiskt i adressboken].**
5. **Välj [På] och tryck på [OK].**
6. **Logga ut.**

Obs

- Uppgifterna raderas automatiskt endast när maskinen tar emot en begäran om registrering. Automatisk radering genomförs inte om användarkonton har lagts till manuellt.
- Endast användarkonton med användarkoder eller inloggade användarnamn och lösenord raderas automatiskt.

Radera alla uppgifter i adressboken

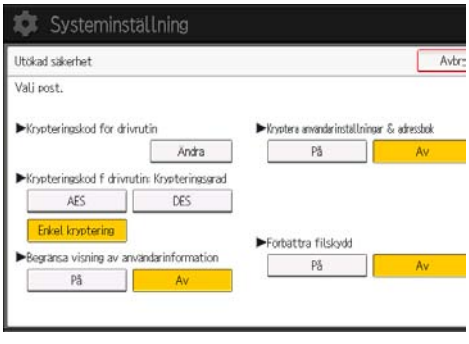
Du kan radera alla uppgifter som registrerats i adressboken.

1. **Logga in som användaradministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [Radera all data i Adressboken].**
5. **Tryck på [Ja] och tryck sedan på [Avsluta].**
6. **Logga ut.**

Ange Utökade säkerhetsfunktioner

Förutom den grundläggande säkerhet som fås genom användarautentisering och de åtkomstbegränsningar som varje administratör anger, kan säkerheten också höjas genom att kryptera överförd data och information i adressboken.

1. **Logga in från kontrollpanelen som administratör med privilegier.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa].**
5. **Tryck på [Utökad säkerhet].**
6. **Tryck på den inställning som du vill ändra och ändra inställningen.**



7. **Tryck på [OK].**
8. **Logga ut.**

Obs

- En administratörs behörighet varierar beroende på inställningen.

Krypteringskod för drivrutin

Nätverksadministratören kan ange detta.

Ange en textsträng för att dekryptera inloggnings- och fillösenord som skickas från drivrutinen när användarautentisering är PÅ.

Ange en krypteringskod för drivrutin genom att registrera den krypteringskod som anges i drivrutinen.

För mer information, se s. 132 "Ange en Krypteringskod för drivrutin".

Krypteringskod f drivrutin: Krypteringsgrad

Nätverksadministratören kan ange detta.

Ange krypteringsgrad för jobb som skickas från drivrutinen till maskinen.

Maskinen kontrollerar krypteringsgraden för det lösenord som har bifogats till ett jobb och bearbetar det.

Om [Enkel kryptering] har angetts accepteras alla jobb som har verifierats genom användarautentiseringen.

Om [DES] har angetts accepteras jobb som har krypterats med DES eller AES.

Om [AES] har angetts accepteras jobb som har krypterats med AES.

Om du väljer [AES] eller [DES] ska du ange krypteringsinställningen med hjälp av skrivardrivrutinen. För mer info om hur du anger skrivardrivrutin, se hjälpavsnittet för skrivardrivrutinen.

Standard: [**Enkel kryptering**]

Begränsa visning av användarinformation

Maskinadministratören kan ange detta om användarautentisering har angetts.

När jobbhistoriken kontrolleras med en nätverksanslutning där autentisering inte tillhandahålls, visas all personlig information som "*********". Eftersom information som identifierar registerade användare inte kan visas, hindras obehöriga användare från att få information i de registrerade filerna.

Standard: [**Av**]

Kryptera användarinställningar & adressbok

Användaradministratören kan ange detta.

Kryptera maskinanvändarnas individuella inställningar samt uppgifter i adressboken.

Även om maskinens interna information skaffas på olagligt vis, förhindrar krypteringen att individuella användarinställningar eller uppgifter i adressboken kan läsas.

För mer information, se s. 69 "Skydda adressboken".

Standard: [**Av**]

Förbättra filskydd

Filadministratören kan ange detta.

Genom att ange ett lösenord kan filadministratören begränsa åtgärder som utskrift och radering av filer. Filadministratören kan även förhindra att obehöriga användare får tillgång till filer. Det är fortfarande möjligt att förhindra att lösenord knäcks.

Genom att ange "Förbättra filskydd" blir filer låsta och otillgängliga om ett ogiltigt lösenord anges tio gånger. Detta kan skydda filer från obehöriga åtkomstförsök genom slumpvisa lösenord.

Om funktionen Förbättra filskydd är aktiverad visas ikonen längst ner i högra hörnet av skärmen.

De låsta filerna kan endast låsas upp av filadministratören.

Om filer låses är det inte möjligt att välja dem även om rätt lösenord anges.

Standard: [**Av**]

Inställningar via SNMPv1, v2

Nätverksadministratören kan ange detta.

Om SNMPv1- eller SNMPv2-protokoll används för att få åtkomst till maskinen kan inte autentisering utföras, vilket innebär att pappersinställningar eller andra inställningar som maskinadministratören anger kan ändras. Om du väljer [Förbjud] kan inställningen visas men inte anges med SNMPv1, v2.

Standard: [**Förbjud inte**]

Autentisera aktuellt jobb

Maskinadministratören kan ange detta.

Med den här inställningen kan du ange om autentisering krävs för sådan användning som att avbryta jobb under kopierings- och utskriftsfunktionerna.

Om du väljer [Inloggningspriv.] kan auktoriserade användare och maskinadministratören använda maskinen. När detta har valts krävs inte autentisering för användare som loggade in på skrivaren innan [Inloggningspriv.] valdes.

Om [Åtkomsträttigheter] är angivet kan alla användare avbryta ett kopierings- eller utskriftsjobb. Maskinadministratören kan också avbryta användarens utskriftsjobb.

Även om du väljer [Inloggningspriv.] och loggar in i skrivaren kan du inte avbryta ett pågående utskriftsjobb såvida du inte har behörighet att använda skrivarfunktionerna.

Du kan endast ange "Autentisera aktuellt jobb" om "Hantering av användarautentisering" har angivits.

Standard: [**Av**]

Lösenordspolicy

Användaradministratören kan ange detta.

Denna inställning låter dig ange [Komplexitetsinställning] och [Minimum antal tecken] för lösenordet. Genom att göra den här inställningen kan du endast använda lösenord som uppfyller de villkor som anges under "Komplexitetsinställning" och "Minimum antal tecken".

Om du väljer [Nivå 1], ange ett lösenord med en kombination av 2 slags tecken som väljs utifrån stora bokstäver, små bokstäver, decimaltal och symboler som #.

Om du väljer [Nivå 2], ange ett lösenord med en kombination av 3 slags tecken som väljs utifrån stora bokstäver, små bokstäver, decimaltal och symboler som #.

Standard: [**Av**]. Det finns inga begränsningar gällande antalet tecken, och typer av tecken är ej angivna.

Tjänsten @Remote

Maskinadministratören kan ange detta.

Kommunikation via HTTPS för Tjänsten @Remote avaktiveras om du väljer [Förhindra].

För inställning [Förbjud] ska du rådgöra med servicetekniker.

Om den är inställd på [Förbj. vissa tjänster] blir det omöjligt att ändra inställningar via en fjärranslutning, vilket ger en optimalt säker hantering.

Standard: [**Förbjud inte**]

Uppdatera firmware

Maskinadministratören kan ange detta.

Denna inställning är till för att ange om firmware-uppdateringar ska tillåtas på maskinen eller inte. En servicerepresentant uppdaterar firmware, eller så utförs firmware-uppdateringar via nätverket.

Om du väljer [Förbjud] kan maskinens firmware inte uppdateras.

Om du väljer [Förbjud inte] blir det inga begränsningar för uppdateringar av firmware.

Standard: [**Förbjud inte**]

Ändra firmware-struktur

Maskinadministratören kan ange detta.

Denna inställning är till för att ange om ändringar i maskinens firmware-struktur ska förhindras eller inte. Funktionen Ändra Firmware-struktur känner av maskinens status när SD-kortet sätts i, tas ut eller byts ut.

Om du väljer [Förbjud], stannar maskinen under uppstart om en firmware-struktur upptäcks, och ett meddelande visas där administratören ombeds logga in. Efter att maskinadministratören har loggat in, fullföljer maskinen uppstart med uppdaterad firmware.

Administratören kan kontrollera om den uppdaterade strukturen är tillåten eller inte genom att kontrollera firmware-versionen som visas på kontrollpanelens skärm. Om den inte är tillåten, kontakta din servicerepresentant innan inloggning.

När "Ändra firmware-struktur" är inställt på [Förbjud] måste administratörsautentisering aktiveras.

När du har ställt in [Förbjud] avaktiverar du administratörsautentiseringen. När administratörsautentiseringen är aktiverad igen kan du ställa tillbaka till [Förbjud inte].

Om du väljer [Förbjud inte] avaktiveras identifiering av ändringar i firmwarestrukturen.

Standard: [**Förbjud inte**]

Fel lösenord har angetts flera gånger

Maskinadministratören kan ange detta.

Om antalet autentiseringsförsök överstiger antalet som anges i inställningen uppfattar systemet åtkomsten som en lösenordsattack. Åtkomsten registreras i åtkomstloggen och informationen skickas till maskinadministratören via e-post.

Om "Max antal åtkomstförsök" är inställt på [0], identifieras inte lösenordsattacker.

- Max antal åtkomstförsök

  Ange max antal tillåtna autentiseringsförsök.

  Ange ett värde mellan "0" och "100" med siffertangenterna och tryck sedan på [#].

  Standard: [**30**]

- Avläsningstid

  Ange ett intervall mellan upprepade autentiseringsförsök som resulterar i misslyckade autentiseringar. När avläsningstiden har gått ut töms registret över autentiseringsförsök.

  Ange ett värde mellan "1" och "10" med siffertangenterna och tryck sedan på [#].

  Standard: [5]

Obs

- Beroende på de värden som angetts för inställningen för [Max antal åtkomstförsök] och [Avläsningstid] kan du vid upprepade tillfällen få e-post gällande identifierad åtkomstöverträdelse.
- Om du ofta får e-post gällande identifierad åtkomstöverträdelse ska du kontrollera innehållet och granska dina inställningsvärden.

Säkerhetsinst. för åtkomstöverträdelse

Maskinadministratören.

Om man loggar in på maskinen via ett nätverksprogram kan en användare blir utelåst av misstag pga att antalet autentiseringsförsök för den användaren inte stämmer överens med antalet försök som angivits på maskinen.

T.ex. åtkomst kanske nekas när ett utskriftsjobb med flera sidor skickas från ett program.

Om du väljer "[På]" under "Säkerhetsinst. för åtkomstöverträdelse", kan du förhindra den typen av autentiseringsfel.

- På
  - Varaktighet för åtkomstövertr.

    Ange hur många användaråtkomster som ska tillåtas.

    Ange ett värde mellan "0" och "60" med siffertangenterna och tryck sedan på [#].

    Standard: [15]
  - Värdbegr. för antal användare

    Ange hur många användarkonton som kan hanteras under "Säkerhetsinst. för åtkomstöverträdelse".

    Ange ett värde mellan "50" och "200" med siffertangenterna och tryck sedan på [#].

    Standard: [200]
  - Värdbegr. för antal lösenord

    Ange hur många lösenord som kan hanteras under "Säkerhetsinst. för åtkomstöverträdelse".

    Ange ett värde mellan "50" och "200" med siffertangenterna och tryck sedan på [#].

    Standard: [200]
  - Intervall för statusövervakare

Ange övervakningsintervallet för "Värdbegr. för antal användare" och "Värdbegr. för antal lösenord".

Ange ett värde mellan "1" och "10" med siffertangenterna och tryck sedan på [#].

Standard: [3]

- Av

Standard: [Av]

Enheten utsatt för åtkomstöverträdelse

Maskinadministratören kan ange detta.

Om antalet inloggningsförfrågningar överstiger antalet som anges av inställningen uppfattar systemet åtkomsten som en åtkomstöverträdelse. Åtkomsten registreras i åtkomstloggen och informationen skickas till maskinadministratören via e-post. Dessutom visas ett meddelande på kontrollpanelen och på Web Image Monitor.

Om "Max antal åtkomstförsök" är inställt på [0], identifieras inte åtkomstöverträdelser.

I "Fördröjn.tid för autentisering" kan du ange en fördröjningstid för inloggningsförfrågningar för att förhindra att systemet slutar att svara när en åtkomstöverträdelse identifieras.

Under "Värdbegr för samtidiga åtkomstförsök" kan du ange det maximala antalet värdar som kan få åtkomst till maskinen samtidigt. Om antalet samtidiga åtkomster överstiger antalet som anges av inställningen kommer övervakning att bli otillgängligt och maskinens övervakningsstatus registreras i loggen.

- Max antal åtkomstförsök

  Ange max antal tillåtna åtkomstförsök.

  Ange ett värde mellan "0" och "500" med siffertangenterna och tryck sedan på [#].

  Standard: [100]

- Avläsningstid

  Ange ett intervall mellan kraftigt upprepade åtkomster. När avläsningstiden har gått ut töms registret över kraftigt upprepade åtkomster.

  Ange ett värde mellan "10" och "30" med siffertangenterna och tryck sedan på [#].

  Standard: [10]

- Fördröjn.tid för autentisering

  Ange fördröjningstiden för autentisering då en åtkomstöverträdelse har identifierats.

  Ange ett värde mellan "0" och "9" med siffertangenterna och tryck sedan på [#].

  Standard: [3]

- Värdbegr för samtidiga åtkomstförsök

  Ange hur många autentiseringsförsök som ska tillåtas när autentisering är fördröjd pga en åtkomstöverträdelse.

  Ange ett värde mellan "50" och "200" med siffertangenterna och tryck sedan på [#].

Standard: [200]

Obs

- Beroende på angivna värden för inställningarna för [Max antal åtkomstförsök] och [Avläsningstid] kan du vid upprepade tillfällen få e-post gällande identifierad åtkomstöverträdelse.
- Om du vid ofta får e-post gällande identifierad åtkomstöverträdelse ska du kontrollera innehållet och granska inställningsvärden.

Andra säkerhetsfunktioner

Detta avsnitt beskriver inställningarna för att förhindra informationsläckage.

Systemstatus

Genom att klicka på [Kontrollera status] på kontrollpanelen kan du kontrollera maskinens aktuella status och inställningar. Om administratörsautentiseringen har angetts, visas endast [Info, maskinadress] i [Underh/kontaktinfo/mask.info] om du har loggat in på skrivaren som administratör.

Kontrollera giltighet på firmware

När maskinen startas används denna funktion för att kontrollera att firmware är giltigt.

Om ett fel inträffar under verifieringsprocessen visas ett verifieringsfel på kontrollpanelen.

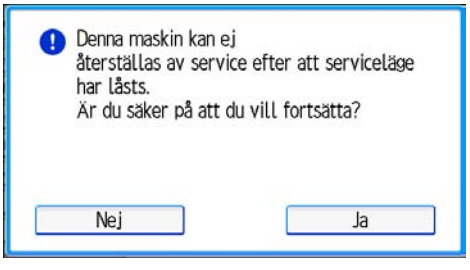
Observera att det även kan kontrolleras via Web Image Monitor efter maskinen startas. Om ett fel inträffar under verifieringsprocessen av Web Image Monitor kan Web Image Monitor inte användas. Kontrollera kontrollpanelen om detta händer.

Begränsar åtgärder av en kundtekniker

Du kan begränsa en kundteknikers tillgång till serviceläget.

En kundtekniker använder serviceläget för inspektion och reparation. Om "Servicelägeslås" har ställts in på [På] kan serviceläge inte användas om inte maskinadministratören loggar in på maskinen och annullerar Servicelägeslåset. Då kan kundteknikern inspektera och repararera maskinen. På så sätt säkerställs att inspektion och reparation kan utföras under maskinadministratörens uppsikt.

1. **Logga in som maskinadministratör via kontrollpanelen.**
2. **Tryck på [Systeminställning].**
3. **Tryck på [Admin.verktyg].**
4. **Tryck på [▼Nästa] två gånger.**
5. **Tryck på [Servicelägeslås].**
6. **Tryck på [På], följt av [OK].**
7. **Tryck på [Ja].**



8. **Logga ut.**

Mer information om utökad säkerhet

I det här avsnittet beskrivs inställningar som du kan konfigurera för att utöka maskinens säkerhet.

Inställningar som du kan konfigurera via kontrollpanelen

Använd kontrollpanelen för att konfigurera de säkerhetsinställningar som visas i följande tabell.

Systeminställningar

Flik	Post	Inställning
Timerinst.	Timer för automatisk utloggning	På: 180 sekunder eller mindre. Se s. 54 "Automatisk utloggning".
Administratörsverktyg	Hantering av användarautentisering	Välj [Grundl. autent.] och ställ in "Utskriftsjobbsautent." på [Hela]. Se s. 31 "Grundläggande autentisering".
Administratörsverktyg	Hantering av administratörsautentisering →Användarhantering	Välj [På] och sedan [Admin.verktyg] vid "Tillgängliga inst.. Se s. 11 "Konfigurera administratörsautentisering".
Administratörsverktyg	Hantering av administratörsautentisering →Användarhantering	Välj [På] och välj sedan alla "Tillgängliga inst.". Se s. 11 "Konfigurera administratörsautentisering".
Administratörsverktyg	Hantering av administratörsautentisering →Nätverkshantering	Välj [På] och sedan [Gränssnittsinst.], [Filöverföring] och [Admin.verktyg] för "Tillgängliga inst.". Se s. 11 "Konfigurera administratörsautentisering".
Administratörsverktyg	Hantering av administratörsautentisering →Filhantering	Välj [På] och sedan [Admin.verktyg] vid "Tillgängliga inst.. Se s. 11 "Konfigurera administratörsautentisering".
Administratörsverktyg	Utökad säkerhet→ Inställningar via SNMPv1, v2	Förbjud Se s. 193 "Ange Utökade säkerhetsfunktioner".

Flik	Post	Inställning
Administratörsverktyg	Utökad säkerhet→ Krypteringskod f drivrutin: Krypteringsgrad	AES Se s. 193 "Ange Utökade säkerhetsfunktioner".
Administratörsverktyg	Utökad säkerhet→ Autentisera aktuellt jobb	Åtkomsträttigheter Se s. 193 "Ange Utökade säkerhetsfunktioner".
Administratörsverktyg	Utökad säkerhet→ Lösenordspolicy	"Komplexitetsinställning": Nivå 1 eller högre, "Minimum antal tecken": 8 eller högre Se s. 193 "Ange Utökade säkerhetsfunktioner".
Administratörsverktyg	Säkerhetsnivå, nätverk	Nivå 2 Om du vill hämta maskinstatusen genom skrivardrivrutinen eller Web Image Monitor aktiverar du "SNMP" på Web Image Monitor. Se s. 94 "Ange Säkerhetsnivåer för nätverk".
Administratörsverktyg	Serviceläge slås	På Se s. 201 "Begränsar åtgärder av en kundtekniker".
Administratörsverktyg	Krypteringsinställningar för maskinens data	Välj [Kryptera] och sedan [All data] för "För enbart över alla data eller filsystemdata (utan att formatera) eller formatera alla.". Om [Kryptera] redan har valts krävs inga ytterligare krypteringsinställningar. Se s. 73 "Kryptera data på maskinen".

Obs

- SNMP-inställningen kan anges i [SNMP] under [Konfiguration] i Web Image Monitor.

Inställningar du kan konfigurera med Web Image Monitor

Använd Web Image Monitor till att konfigurera de säkerhetsinställningar som visas i följande tabell.

Enhetshantering→Konfiguration

Kategori	Post	Inställning
Enhetsinställningar →Loggar	Hämta Jobbloggar	Aktivt
Enhetsinställningar →Loggar	Hämta Åtkomstloggar	Aktivt
Säkerhet→Princip om utelåsning av användare	Utelåsning	Aktivt För mer information, se s. 52 "Funktion för utelåsning av användare".
Säkerhet→Princip om utelåsning av användare	Antal försök innan Utelåsning sker	5 gånger eller färre. För mer information, se s. 52 "Funktion för utelåsning av användare".
Säkerhet→Princip om utelåsning av användare	Timer för när utelåsningen ska upphöra	Ställ in på [Aktivt] eller [Ej aktivt]. Om du väljer [Aktivt], ställer du in timern på 60 minuter eller mer. För mer information, se s. 52 "Funktion för utelåsning av användare".
Säkerhet→Princip om utelåsning av användare	Lås användare ute i	När du ställer in "Lockout Release Timer" på [Active], ställer du in timern på 60 minuter eller mer. För mer information, se s. 52 "Funktion för utelåsning av användare".
Nätverk→ SNMPv3	Funktion SNMPv3	Ej aktivt För att använda SNMPv3-funktioner, ställ in "SNMPv3-funktion på [Active] och Tillåt SNMPv3-kommunikation på [Endast kryptering]. Eftersom SNMPv3 framtvingar autentisering för varje paket, avaktiveras inloggningsloggen när SNMPv3 är aktivt.
Säkerhet→ Nätverkssäkerhet	FTP	Ej aktivt Innan du anger den här inställningen ställer du in "Säkerhetsnivå för nätverk" på [Nivå 2] på kontrollpanelen.

Inställningar som du kan konfigurera när IPsec är tillgängligt/ej tillgängligt

All kommunikation till och från maskinen på vilka IPsec aktiveras krypteras.

Om nätverket hanterar IPsec rekommenderar vi att du aktiverar det.

Inställningar som du kan konfigurera när IPsec är tillgängligt

Om IPsec är tillgängligt, konfigurerar du inställningar som visas i följande tabell för att utöka säkerheten för de data som överförs på nätverket.

Kontrollpanelsinställningar

Systeminställningar

Flik	Post	Inställning
Gränssnittsinställningar	IPsec	Aktivt
Gränssnittsinställningar	Tillåt SSL/TLS-kommunikation	Endast chiffertext

Web Image Monitor-inställningar

Enhetshantering→Konfiguration

Kategori	Post	Inställning
Säkerhet→IPsec →Inställningar för automatiskt byte av krypteringsnycklar	Redigera→Säkerhetsnivå	Autentisering och hög krypteringsnivå

Inställningar som du kan konfigurera när IPsec inte är tillgängligt

Om IPsec inte är tillgängligt, konfigurerar du inställningar som visas i följande tabell för att utöka säkerheten för data som överförs på nätverket.

Kontrollpanelsinställningar

Systeminställningar

Flik	Post	Inställning
Gränssnittsinställningar	IPsec	Ej aktivt
Gränssnittsinställningar	Tillåt SSL/TLS-kommunikation	Endast chiffertext

Obs

- Du kan ställa in "IPsec" och "Tillåt SSL/TLS-kommunikation" med hjälp av Web Image Monitor.

Säkra data när IPsec inte är tillgängligt

Följande metod förbättrar säkerheten för användardata när IPsec inte är tillgängligt.

Administratörerna måste instruera användarna om att de måste utföra dessa metoder.

Skrivare

- Skriva ut med protokoll som stödjer kryptering:

  För att använda skrivarfunktionerna anger du SFTP som protokoll eller så anger du IPP och aktiverar SSL/TLS.

  För mer information om IPP-inställningar, se handboken Printer Driver Installation Guide (Handbok för installation av drivrutin.)

  För mer information om SSL/TLS-inställningar, se s. 104 "Konfigurera inställningar för SSL/TLS".

Obs

- För mer information om hur du aktiverar och inaktiverar IPsec via kontrollpanelen, se Connecting the Machine/ System Settings.
- För information om hur man anger IPsec-inställningarna via Web Image Monitor, se s. 110 "Konfigurera IPsec-inställningar".

8. Felsökning

I det här kapitlet beskrivs vad du kan göra om maskinen inte fungerar korrekt.

Om ett meddelande visas

Detta avsnitt beskriver hur du hanterar problem om ett meddelande visas på skärmen under användarautentisering.

Om ett meddelande annat än nedan visas, följ anvisningarna för att lösa problemet.

"Du har inte rättighet att använda den här funktionen."

Behörighet att använda funktionen har inte angetts.

Om detta visas när du använder en funktion:

- Funktionen är inte angiven i inställningarna Hantera adressboken.
- Användaradministratören måste besluta om tilldelning av behörighet för att använda funktionen.

Om detta visas när du anger en maskininställning:

- Vem som är administratör beror på vilka maskininställningar som användare vill ange.
- Genom att använda listan över inställningar måste administratören som är ansvarig för de maskininställningar som användaren vill ange bestämma om de ytterligare behörigheter som krävs för att använda funktionen ska tilldelas.

"Autentiseringen misslyckades."

Anledningar till misslyckade autentiseringar varierar och dessa indikeras genom felkoder.

För mer information, se s. 208 "Om en felkod visas".

"Administratörautentisering för användarhantering måste ställas in till på före detta val kan göras."

Användaradministratörens rättigheter har inte aktiverats i [Hantering av administratörsautentisering].

- Du måste först aktivera administratörens rättigheter i [Hantering av administratörsautentisering] för att ange Grundläggande autentisering, Windows-autentisering eller LDAP-autentisering.

För mer information, se s. 11 "Konfigurera administratörsautentisering".

"Vald(a) fil(er) innehåller fil(er) utan rättigheter. Endast fil(er) med rättigheter kommer att raderas."

Du har försökt radera filer utan att ha behörighet att göra det.

- Ägaren eller filadministratören kan radera filer. För att radera en fil som du inte har behörighet att radera, kontakta ägaren eller filadministratören.

Obs

- Om ett servicemeddelande visas kontaktar du service.

Om en felkod visas

När autentisering misslyckas visas meddelandet "Autentiseringen misslyckades." tillsammans med en felkod. Följande lista innehåller lösningar för varje felkod. Om en felkod inte finns med i listorna nedan, ska du anteckna koden och kontakta en servicerepresentant.

Visningsläge för felkod

SV CJD014

1. **Felkod**

   En felkod visas.

Grundläggande autentisering

B0104-000

Kunde inte dekryptera lösenordet.

- Ett lösenordsfel uppstod.

  Kontrollera att lösenordet är korrekt angivet.

- Antingen [DES] eller [AES] väljs för "Krypteringskod f drivrutin: Krypteringsgrad".

  Du får åtkomst genom att ange krypteringskoden för drivrutinen.

- Ett fel med krypteringskod för drivrutin uppstod.

  Kontrollera att krypteringskoden är korrekt angiven i drivrutinen.

B0206-002: Fall 1

Ett fel uppstod vid inloggning (användarnamn eller lösenord).

- Kontrollera att användarnamnet och lösenordet skrivs in korrekt och logga sedan in.

B0206-002: Fall 2

Användaren försökte göra en autentisering från ett program på skärmen "Systeminställningar" där endast administratören har autentiseringsbehörighet.

- Endast administratören har rättighet att logga in på den här skärmen.

- Logga in som allmän användare från programmets inloggningssida.

B0206-003

Ett autentiseringsfel inträffade eftersom användarnamnet innehåller ett mellanslag, kolon (:) eller citationstecken (").

- Skapa kontot på nytt om kontonamnet innehåller något av de här otillåtna tecknen.
- Om kontonamnet angavs felaktigt, skriv in det korrekta namnet och logga sedan in igen.

B0207-001

Ett autentiseringsfel inträffade eftersom adressboken används på en annan plats.

- Vänta några minuter och försök sedan igen.

B0208-000/B0208-002

Kontot är låst på grund av att antalet tillåtna autentiseringsförsök har nått max.

- Be användaradministratören låsa upp kontot.

Windows-autentisering

W0104-000

Kryptering av ett lösenord misslyckades.

- Ett lösenordsfel uppstod.

  Kontrollera att lösenordet är korrekt angivet.
- Antingen [DES] eller [AES] väljs för "Krypteringskod f drivrutin: Krypteringsgrad".

  Du får åtkomst genom att ange krypteringskoden för drivrutinen.
- Ett fel med krypteringskod för drivrutin uppstod.

  Kontrollera att krypteringskoden är korrekt angiven i drivrutinen.

W0206-002

Användaren försökte göra en autentisering från ett program på skärmen "Systeminställningar" där endast administratören har autentiseringsbehörighet.

- Endast administratören har rättighet att logga in på den här skärmen.
- Logga in som allmän användare från programmets inloggningssida.

W0206-003

Ett autentiseringsfel inträffade eftersom användarnamnet innehåller ett mellanslag, kolon (:) eller citationstecken (").

- Skapa kontot på nytt om kontonamnet innehåller något av de här otillåtna tecknen.
- Om kontonamnet angavs felaktigt, skriv in det korrekta namnet och logga sedan in igen.

W0207-001

Ett autentiseringsfel inträffade eftersom adressboken används på en annan plats.

- Vänta några minuter och försök sedan igen.

W0208-000/W0208-002

Kontot är låst på grund av att antalet tillåtna autentiseringsförsök har nått max.

- Be användaradministratören låsa upp kontot.

W0400-102

Kerberos-autentisering misslyckades eftersom servern inte fungerar korrekt.

- Kontrollera att servern fungerar korrekt.

W0400-200

På grund av det höga antalet autentiseringsförsök är alla resurser upptagna.

- Vänta några minuter och försök sedan igen.

W0400-202: Fall 1

SSL-inställningarna på autentiseringsservern och på maskinen överensstämmer inte.

- Kontrollera att SSL-inställningarna på autentiseringsservern och på maskinen överensstämmer.

W0400-202: Fall 2

Användaren angav sAMAccountName som användarnamn för att logga in.

- Om en användare anger sAMAccountName som användarnamn, misslyckas ldap_bind i en överordnad/underdomänmiljö. Använd istället UserPrincipleName för inloggning.

W0406-003

Ett autentiseringsfel inträffade eftersom användarnamnet innehåller ett mellanslag, kolon (:) eller citationstecken (").

- Skapa kontot på nytt om kontonamnet innehåller något av de här otillåtna tecknen.
- Om kontonamnet angavs felaktigt, ange det korrekt och logga sedan in igen.

W0406-101

Autentisering kan inte slutföras på grund av det höga antalet autentiseringsförsök.

- Vänta några minuter och försök sedan igen.
- Om situationen inte förbättras, kontrollera att det inte är fråga om en autentiseringsattack.
- Meddela administratören om skärmmeddelandet via e-post och kontrollera systemloggen för potentiella autentiseringsattacker.

W0406-107: Fall 1

Formen AnvändarePrincipNamn (användare@domännamn.xxx.com) används till användarnamnet.

- Användargrupp kan inte erhållas om formen AnvändarePrincipNamn (användare@domännamn.xxx.com)används.
- Använd "sAMKontonamn" (användare) för att logga in eftersom det här kontot tillåter att du erhåller användargruppen.

W0406-107: Fall 2

Aktuella inställningar tillåter inte grupphämtning.

- Kontrollera att användargruppens område är inställt på "Global grupp" och grupptyp är inställd på "Säkerhet" i gruppegenskaper.
- Kontrollera att kontot har lagts till användargruppen.
- Kontrollera att användargruppens namn som används på maskinen och gruppnamnet på DC (domänkontrollant) överensstämmer. DC är skiftlägeskänslig.
- Kontrollera att "Anv.autent.info vid inlogg." har angivits under "Aut.info" i det användarkonto som har registrerats på maskinen.
- Om det finns fler än en DC, kontrollera att en konfidentiell relation har konfigurerats mellan varje DC.

W0406-107: Fall 3

Domännamnet kan inte matchas.

- Kontrollera att DNS/WINS är angivet i domännamnet "Gränssnittsinst.".

W0406-107: Fall 4

Kan inte ansluta till autentiseringsservern.

- Kontrollera att det går att ansluta till autentiseringsservern.
- Använd "Ping-kommandot" i "Gränssnittsinst." för att kontrollera anslutningen.

W0406-107: Fall 5

Ett fel uppstod när användarnamn eller lösenord angavs.

- Kontrollera att användaren är registrerad på servern.
- Använd ett registrerat användarnamn och lösenord.

W0406-107 : Fall 6

Ett fel uppstod med domännamnet.

- Kontrollera att domännamnet för Windows-autentisering anges korrekt.

W0406-107: Fall 7

Kan inte matcha domännamnet.

- Ange IP-adressen i domännamnet och bekräfta att autentiseringen lyckades.

  Om autentiseringen lyckades:

- Om domännamnets toppnivå anges i domännamnet (som t.ex. domännamn.xxx.com), kontrollera att DNS anges i "Gränssnittsinst."
- Kontrollera att WINS är angivet i "Gränssnittsinst.", om ett NetBIOS-domännamn är angivet i domännamn (såsom DOMÄNNAMN).

Om autentisering misslyckades:

- Kontrollera att Begränsa LM/NTLM inte är inställt vare sig i "Domänkontrollantens säkerhetsprincip" eller "Domänsäkerhetsprincip".
- Kontrollera att portarna till domänkontrollantens brandvägg och brandväggen för anslutningsvägen från maskinen till domänkontrollanten är öppna.

- Om Windows brandvägg aktiveras skapar du en brandväggsregel under "Avancerade inställningar" för Windows brandvägg för att auktorisera portarna 137 och 139.
- I egenskapsfönstret för "Nätverksanslutningar", öppna egenskaper för TCP/IP. Klicka sedan på detaljinställningar, WINS, kontrollera rutan "Aktivera NetBIOS över TCP/IP" och ställ in talet 137 för att "Öppna".

W0406-107: Fall 8

Kerberos-autentisering misslyckades.

- Inställningarna för Kerberos-autentisering är inte korrekt konfigurerarde.

  Kontrollera att realmnamnet, namnet för KDC (Key Distribution Center) samt motsvarande domännamn har angivits korrekt.
- Timingen mellan KDC och maskinen överensstämmer inte.

  Autentiseringen kommer att misslyckas om skillnaden i timing mellan KDC och maskinen är större än fem minuter. Kontrollera att timingen matchar.
- Kerberos-autentiseringen kommer att misslyckas om realmnamnet anges med små bokstäver. Kontrollera att realmnamnet har angetts med versaler.
- Kerberos-autentisering kommer att misslyckas om automatisk hämtning för KDC misslyckas.

  Be servicerepresentanten kontrollera att hämtningsinställningarna är inställda på "automatisk hämtning".

  Om automatisk hämtning inte fungerar korrekt, växla till manuell hämtning.

W0409-000

Autentiseringen avbröts eftersom servern inte svarade.

- Kontrollera nätverkets konfiguration eller inställningarna på autentiseringsservern.

W0511-000 / W0517-000

Inloggningsnamnet för autentiseringsservern är detsamma som ett redan registrerat användarnamn på maskinen. (Namnen identifieras genom det unika attributet som anges i inställningarna för LDAP-autentisering.)

- Radera det gamla, kopierade namnet eller ändra inloggningsnamnet.

- Radera det gamla namnet på servern om autentiseringsservern nyligen bytts ut.

W0606-004

Autentiseringen misslyckades pp grund av att användarnamnet innehåller ord som inte kan användas av allmänna användare.

- Använd inte "other", "admin", "supervisor" eller "HIDE*" i allmänna användarkonton.

W0607-001

Ett autentiseringsfel inträffade eftersom adressboken används på en annan plats.

- Vänta några minuter och försök sedan igen.

W0612-005

Autentiseringen misslyckades eftersom inga fler användare kan registreras. (Antalet registrerade användare i adressboken har nått max.)

- Be administratören ta bort oanvända användarkonton i adressboken.

W0707-001

Ett autentiseringsfel inträffade eftersom adressboken används på en annan plats.

- Vänta några minuter och försök sedan igen.

W09XX-019

Den automatiska registreringen av användare på servern misslyckades när en åtkomst från klienten med hjälp av funktionen Central adressbokshantering autentiserades.

- Kontrollera nätverksanslutningen mellan klienten och servern.
- Användare kan inte registreras medan adressboken på servern redigeras.

LDAP-autentisering

L0104-000

Kryptering av ett lösenord misslyckades.

- Ett lösenordsfel uppstod.

  Kontrollera att lösenordet är korrekt angivet.
- Antingen [DES] eller [AES] väljs för "Krypteringskod f drivrutin: Krypteringsgrad".

  Du får åtkomst genom att ange krypteringskoden för drivrutinen.
- Ett fel med krypteringskod för drivrutin uppstod.

  Kontrollera att krypteringskoden är korrekt angiven i drivrutinen.

L0206-002

En användare försökte autentisera från ett program på skärmen "Systeminställningar" där endast administratören har autentiseringsbehörighet.

- Endast administratören har rättighet att logga in på den här skärmen.
- Logga in som allmän användare från programmets inloggningssida.

L0206-003

Ett autentiseringsfel inträffade eftersom användarnamnet innehåller ett mellanslag, kolon (:) eller citationstecken (").

- Skapa kontot på nytt om kontonamnet innehåller något av de här otillåtna tecknen.
- Om kontonamnet angavs felaktigt, skriv in det korrekta namnet och logga sedan in igen.

L0207-001

Ett autentiseringsfel inträffade eftersom adressboken används på en annan plats.

- Vänta några minuter och försök sedan igen.

L0208-000/L0208-002

Kontot är låst på grund av att antalet tillåtna autentiseringsförsök har nått max.

- Be användaradministratören låsa upp kontot.

L0307-001

Ett autentiseringsfel inträffade eftersom adressboken används på en annan plats.

- Vänta några minuter och försök sedan igen.

L0400-210

Kunde inte att hämta användarinformation vid LDAP-sökning.

- Sökförhållandena för attributet till inloggningsnamnet har eventuellt inte angetts, eller så är den angivna sökinformationen otillgänglig.
- Kontrollera att attributet till inloggningsnamnet angivits korrekt.

L0406-003

Ett autentiseringsfel inträffade eftersom användarnamnet innehåller ett mellanslag, kolon (:) eller citationstecken (").

- Skapa kontot på nytt om kontonamnet innehåller något av de här otillåtna tecknen.
- Om kontonamnet angavs felaktigt, skriv in det korrekta namnet och logga sedan in igen.

L0406-200

Autentisering kan inte slutföras på grund av det höga antalet autentiseringsförsök.

- Vänta några minuter och försök sedan igen.
- Om situationen inte förbättras, kontrollera att det inte är fråga om en autentiseringsattack.

- Meddela administratören om skärmmeddelandet via e-post och kontrollera systemloggen för potentiella autentiseringsattacker.

L0406-201

Autentisering är avaktiverad i LDAP-serverns inställningar.

- Ändra LDAP-serverns inställningar i administratörsverktyg i "Systeminställningar".

L0406-202/L0406-203: Fall 1

Det finns ett fel i inställningarna för LDAP-autentisering, LDAP-servern eller nätverkskonfigurationen.

- Kontrollera att LDAP-serverns inställningar är korrekta genom att göra ett anslutningstest.

  Om anslutningen inte lyckas kan ett fel i nätverksinställningarna ha inträffat.

  Kontrollera domännamnet eller DNS-inställningarna i "Gränssnittsinst.".
- Kontrollera att LDAP-servern har angetts korrekt i inställningarna för LDAP-autentisering.
- Kontrollera att användarnamnattributet har angetts korrekt i inställningarna för LDAP-autentisering.
- Kontrollera att SSL-inställningarna stöds av LDAP-servern.

L0406-202/L0406-203: Fall 2

Ett fel uppstod vid inloggning (användarnamn eller lösenord).

- Kontrollera att användarnamnet och lösenordet skrivs in korrekt.
- Kontrollera att ett användbart inloggningsnamn finns registrerat på maskinen.

  Autentisering kommer att misslyckas i följande fall:

  Om användarnamnet innehåller ett mellanslag, kolon (:) eller citationstecken (").

  Om användarnamnet överskrider 128 byte.

L0406-202/L0406-203: Fall 3

Det uppstod ett fel i den enkla krypteringen.

- Autentisering kommer att misslyckas om rutan för lösenord lämnas tom vid enkel autentisering.

  För att tillåta tomma lösenordsrutor, kontakta din servicerepresentant.
- Vid enkel autentisering hämtas inloggningsnamnet för DN från användarkontot.

  Autentisering kommer att misslyckas om inte DN kan hämtas.

  Kontrollera att det inte finns några fel i servernamnet, användarnamnet, lösenordet eller informationen som anges för sökfiltret.

L0406-204

Kerberos-autentisering misslyckades.

- Inställningarna för Kerberos-autentisering är inte korrekt konfigurerarde.

  Kontrollera att realmnamnet, KDC-namnet (Key Distribution Center) och det stödjande domännamnet angivits korrekt.

- Timingen mellan KDC och maskinen överensstämmer inte.

  Autentiseringen kommer att misslyckas om skillnaden i timing mellan KDC och maskinen är större än fem minuter. Kontrollera att timingen matchar.

- Kerberos-autentiseringen kommer att misslyckas om realmnamnet anges med små bokstäver. Kontrollera att realmnamnet har angetts med versaler.

L0409-000

Autentiseringen avbröts eftersom servern inte svarade.

- Kontakta server- eller nätverksadministratören.
- Om situationen inte förbättras, kontakta din servicerepresentant.

L0511-000

Inloggningsnamnet för autentiseringsservern är detsamma som ett redan registrerat användarnamn på maskinen. (Namnen identifieras genom det unika attributet som anges i inställningarna för LDAP-autentisering.)

- Radera det gamla, kopierade namnet eller ändra inloggningsnamnet.
- Radera det gamla namnet på servern om autentiseringsservern nyligen bytts ut.

L0606-004

Autentiseringen misslyckades pp grund av att användarnamnet innehåller ord som inte kan användas av allmänna användare.

- Använd inte "other", "admin", "supervisor" eller "HIDE*" i allmänna användarkonton.

L0607-001

Ett autentiseringsfel inträffade eftersom adressboken används på en annan plats.

- Vänta några minuter och försök sedan igen.

L0612-005

Autentiseringen misslyckades eftersom inga fler användare kan registreras. (Antalet registrerade användare i adressboken har nått max.)

- Be administratören ta bort oanvända användarkonton i adressboken.

L0707-001

Ett autentiseringsfel inträffade eftersom adressboken används på en annan plats.

- Vänta några minuter och försök sedan igen.

L09XX-019

Den automatiska registreringen av användare på servern misslyckades när en åtkomst från klienten med hjälp av funktionen Central adressbokshantering autentiserades.

- Kontrollera nätverksanslutningen mellan klienten och servern.

- Användare kan inte registreras medan adressboken på servern redigeras.

Om maskinen inte kan användas

Om följande inträffar när maskinen används ska du instruera användarna hur de ska hantera detta.

Problem	Orsak	Lösning
Kan inte utföra följande: • Skriv ut med skrivardrivrutinen	Användarautentisering har nekats.	Kontrollera användarnamn och inloggningsnamn med administratören för det nätverk som används om du använder Windows-autentisering eller LDAP-autentisering. Bekräfta med användaradministratören om du använder grundläggande autentisering.
Kan inte utföra följande: • Skriv ut med skrivardrivrutinen	Den krypteringskod som angivits i drivrutinen överensstämmer inte med krypteringskoden för maskinens drivrutin.	Ange den krypteringskod för drivrutin som finns registrerad i maskinen. För mer information, se s. 132 "Ange en Krypteringskod för drivrutin".
När "Adressbok" har öppnats i Device Manager NX och du har angett korrekt användarnamn och lösenord visas ett meddelande om att ett felaktigt lösenord har angivits.	"Krypteringskod f drivrutin: Krypteringsgrad" är inte korrekt inställd. Alternativt har "SSL/TLS" aktiverats trots att det certifikat som krävs inte finns installerat på datorn.	Ställ in "Krypteringskod f drivrutin: Krypteringsgrad" på [Enkel kryptering]. Alternativt kan du aktivera "SSL/TLS", installera servercertifikatet på maskinen och sedan installera certifikatet på datorn. För mer information, se s. 193 "Ange Utökade säkerhetsfunktioner" och s. 104 "Konfigurera inställningar för SSL/TLS".

Problem	Orsak	Lösning
Användarautentisering aktiveras men arkiverade utskriftsfiler visas inte.	Användarautentiseringen kan ha avaktiverats utan "Alla användare" valdes för användaråtkomst för lagrade utskriftsfiler.	Aktivera användarautentisering igen och välj [Alla användare] som inställning för åtkomstbehörigheten för de filer du vill visa. För mer information, se hjälpen till Web Image Monitor.
Användarautentisering är avaktiverad, men användare registrerade i adressboken visas ändå inte.	Användarautentisering kan ha avaktiverats utan att "Alla användare" har valts för "Skydda mottagare".	Aktivera användarautentisering igen och välj [Alla användare] som inställning för åtkomstbehörigheten för de användare du vill visa. För mer information, se s. 69 "Skydda adressboken".
Kan inte skriva ut när användarautentisering har specificerats.	Användarautentisering kanske inte har specificerats i skrivardrivrutinen.	Ange användarautentisering i skrivardrivrutinen. För mer information, se skrivardrivrutinens hjälp.
[Slutför jobb & begr forts anv] har valts i "Maskinåtgärd när begränsning är nådd", men det aktuella jobbet avbryts innan det har bearbetats.	Beroende på vilket program du använder kanske maskinen inte känner igen ett jobb som ett multipelt jobb, och avbryter därför jobbet innan det har bearbetats.	Återställ inställningen för utskriftsvolym för användaren genom att t.ex. nollställa användarräkneverket för utskriftsvolym och gör sedan om utskriften igen. För mer information, se s. 66 "Återställa användarräkneverk för utskriftsvolym".
När körningen av Kryptera användarinställningar & adressbok har slutförts, visas inte meddelandet Avsluta trots att du väntar länge på det.	Autentisering kan ta tid eftersom ett stort antal poster har registrerats i adressboken. Alternativt kan en fil vara skadad eller så kan det vara fel på hårddisken.	Om skärmen fortfaranden inte har uppdaterats även om tiden som angetts i "Endast filsystems data" i enlighet med s. 73 "Kryptera data på maskinen" har gått ut så kontakta ditt serviceombud.

9. Lista över inställningsbehörigheter

I detta kapitel listas administratörens och användarens inställningsbehörigheter då administratörautentisering eller användarautentisering är aktiverat.

Så här läser du

Tyda rubriker

- Användare

  Användaradministratören har behörighet att utföra denna åtgärd.

- Mask

  Maskinadministratören har behörighet att utföra denna åtgärd.

- N/V

  Nätverksadministratören har behörighet att utföra denna åtgärd.

- Fil

  Filadministratören har behörighet att utföra denna åtgärd.

- Inga inst.

  Den inloggade användaren har behörighet att utföra denna åtgärd.

  I de fall då inga inställningar har gjorts i "Tillgängliga inst." i [Hantering av administratörsautentisering].

- Inst.

  Den inloggade användaren har behörighet att utföra denna åtgärd.

  Status när inställningar har valts i "Tillgänliga inst." för [Hantering av administratörsautentisering].

- Nv.1

  I de fall då [Menyskydd] har ställts in på [Nivå 1].

- Nv.2

  I de fall då [Menyskydd] har ställts in på [Nivå 2].

Tyda symbolerna

R/W: Möjligt att verkställa, ändra samt läsa.

R: Möjligt att läsa.

-: Ej möjligt att verkställa, ändra samt läsa.

Systeminställningar

När administratörsautentisering har angetts varierar restriktionerna för användaråtgärder beroende på konfigurationerna i "Tillgängliga inst.".

[Normalegenskaper]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Programmera/Ändra/Radera användartext]	R	R/W	R	R	R/W	R
[Panelsignal]	R	R/W	R	R	R/W	R
[Klarsignal]	R	R/W	R	R	R/W	R
[Funktionsprioritet]	R	R/W	R	R	R/W	R
[Fördelning av funktionstangent]	R	R/W	R	R	R/W	R
[Inställning för skärmfärg]	R	R/W	R	R	R/W	R
[Utskrift: Skrivare]	R	R/W	R	R	R/W	R
[Inställning för utmatningsfack]	R	R/W	R	R	R/W	R
[Kassettprioritet: Skrivare]	R	R/W	R	R	R/W	R
[Tangentrepetition]	R	R/W	R	R	R/W	R
[Visningstid för Systemstatus/Jobblista]	R	R/W	R	R	R/W	R
[Statusindikator]	R	R/W	R	R	R/W	R
[Z-vikningsläge]	R	R/W	R	R	R/W	R
[Läge för: Parallellfals 4-sidig folder]	R	R/W	R	R	R/W	R
[Läge för: Parallellfals 6-sidig folder/ dragspel]	R	R/W	R	R	R/W	R
[Läge för: Parallellfals 6-sidig folder/flik in]	R	R/W	R	R	R/W	R
[Läge för: Dubbel parallellfals 8-sidig folder]	R	R/W	R	R	R/W	R
[Läge för: Altarfals]	R	R/W	R	R	R/W	R
[Externt tangentbord]	R	R/W	R	R	R/W	R

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Progr./Ändra USB-lista]	R	R/W	R	R	R/W	R
[Finjustering av beskärning vid limbindning.]	R	R/W	R	R	R/W	R
[Kompatibelt ID]	R	R/W	R	R	R/W	R

[Timerinställningar]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Timer för viloläge]	R	R/W	R	R	R/W	R
[Timer för energisparläge]	R	R/W	R	R	R/W	R
[System för auto-återgång av timer]	R	R/W	R	R	R/W	R
[Auto-återgång timer, skrivare]	R	R/W	R	R	R/W	R
[Ange datum]	R	R/W	R	R	R/W	R
[Ange tid]	R	R/W	R	R	R/W	R
[Timer för automatisk utloggning]	R	R/W	R	R	R/W	R
[Fixeringsenhet i läge Av (Energibsp) På/Av]	R	R/W	R	R	R/W	R
[Veckotimer]	R	R/W	R	R	R/W	R
[Auto-av tim. på uppv. av bind.lim]	R	R/W	R	R	R/W	R

[Gränssnittsinställningar]

[Nätverk]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Maskinens IPv4-adress]*1	R	R	R/W	R	R/W	R
[IPv4 Gateway-adress]	R	R	R/W	R	R/W	R
[Maskinens IPv6-adress]	R	R	R	R	R	R
[IPv6 Gateway-adress]	R	R	R	R	R	R

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Autokonfiguration IPv6 Stateless-adress]	R	R	R/W	R	R/W	R
[DHCPv6-konfiguration]	R	R	R/W	R	R/W	R
[DNS-konfiguration]*2	R	R	R/W	R	R/W	R
[DDNS-konfiguration]	R	R	R/W	R	R/W	R
[IPsec]	R	R	R/W	R	R/W	R
[Domännamn]*1	R	R	R/W	R	R/W	R
[WINS-konfiguration]	R	R	R/W	R	R/W	R
[Aktivt protokoll]	R	R	R/W	R	R/W	R
[NW frametype]	R	R	R/W	R	R/W	R
[SMB-datornamn]	R	R	R/W	R	R/W	R
[SMB-arbetsgrupp]	R	R	R/W	R	R/W	R
[Ethernethastighet]	R	R	R/W	R	R/W	R
[Ping-kommando]	–	–	R/W	–	R/W	R
[Tillåt SNMPv3-kommunikation]	R	R	R/W	R	R/W	R
[Tillåt SSL/TLS-kommunikation]	R	R	R/W	R	R/W	R
[Värdnamn]	R	R	R/W	R	R/W	R
[Maskinnamn]	R	R	R/W	R	R/W	R
[IEEE 802.1X-autentisering för Ethernet]	R	R	R/W	R	R/W	R
[Återställ IEEE 802.1X-autentisering till standard]	–	–	R/W	–	R/W	–

*1 När automatisk hämtning är inställd, är uppgifterna skrivskyddade.

*2 Alla administratörer och användare kan köra anslutningstest.

[Skriv ut lista]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Skriv ut lista]	–	–	R/W	–	R/W	–

[Filöverföring]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[SMTP-server]	R	R	R/W	R	R/W	R
[SMTP-autentisering]*3	R	R/W	R	R	R/W	R
[POP före SMTP]	R	R/W	R	R	R/W	R
[Mottagningsprotokoll]	R	R/W	R	R	R/W	R
[Inställningar för POP3/IMAP4]	R	R/W	R	R	R/W	R
[E-postadress för administratör]	R	R/W	R	R	R/W	R
[Port för e-postkommunikation]	R	R	R/W	R	R/W	R
[Intervall för e-postmottagning]	R	R	R/W	R	R/W	R
[E-postlagring i server]	R	R	R/W	R	R/W	R
[Automatisk e-postavisering]	–	R/W	–	–	R/W	–

*3 Lösenord kan inte läsas.

[Admin.verktyg]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Hantera adressboken]	R/W	R/W *4	R/W *4	R/W *4	R/W*5	R*5
[Adressbok: Programmera/Ändra/Radera grupp]	R/W	R/W *4	R/W *4	R/W *4	R/W*5	R*5
[Adressbok: Ändra ordning]	R/W	–	–	–	R/W	–
[Adressbok: Redigera titel]	R/W	–	–	–	R/W	–

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Adressbok: Byt titel]	R/W	–	–	–	R/W	R
[Säkerhetskopiera/återställ: Användarinst. & adressbok]	R/W	–	–	–	R/W	–
[Radera användare automatiskt i adressboken]	R/W	–	–	–	R/W	–
[Radera all data i Adressboken]	R/W	–	–	–	R/W	–
[Visa/skriv ut räkneverk]	R	R/W	R	R	R/W	R/W
[Visa/rensa/skriv ut räkneverk per användare]	R/W*6	R/W*7	R	R	R/W	–
[Visa/nollställ miljöanpassat räkneverk]	–	R/W	–	–	–	–
[Visa/nollställ miljöanpassat räkneverk per användare]	–	R/W	–	–	–	–
[Miljöanpassad räkneverksperiod/ administratörsmeddelande]	R	R/W	R	R	R	R
[Maskinåtgärd när begränsning är nådd]	R	R/W	R	R	R	R
[Begränsad utskriftsvolym: räkneverksinställning]	R	R/W	R	R	R	R
[Utökad begränsad utskriftsvolym]	R	R/W	R	R	R	R
[Begränsad utskriftsvolym: standardvärde]	R/W	R	R	R	R	R
[Använd Mediaanslutning]	R	R/W	R	R	R	R
[Hantering av användarautentisering]	R	R/W	R	R	R/W	R
[Förbättrad hantering av autentisering]	R	R/W	R	R	R/W	R
[Hantering av administratörsautentisering]	R/W*8*9	R/W*9	R/W*9	R/W*9	R/W	–
[Programmera/Ändra administratör]	R/W*10	R/W*10	R/W*10	R/W*10	–	–
[Räkneverkshantering]	R	R/W	R	R	R/W	R

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Hantering av extern avgiftsenhet]	R	R/W	R	R	R/W	R
[Förbättrad hantering av extern avgiftsenhet]	R	R/W	R	R	R/W	R
[Utökad säkerhet]						
• [Krypteringskod för drivrutin]	–	–	R/W	–	R/W	–
• [Krypteringskod f drivrutin: Krypteringsgrad]	R	R	R/W	R	R/W	R
• [Begränsa visning av användarinformation]	R	R/W	R	R	R/W	R
• [Kryptera användarinställningar & adressbok]	R/W	R	R	R	R	R
• [Förhöjt filskydd]	R	R	R	R/W	R	R
• [Inställningar via SNMPv1, v2]	R	R	R/W	R	R/W	R
• [Autentisera aktuellt jobb]	R	R/W	R	R	R/W	R
• [Lösenordspolicy]	R/W	–	–	–	–	–
• [Tjänsten @Remote]	R	R/W	R	R	R/W	R
• [Uppdatera Firmware]	R	R/W	R	R	–	–
• [Ändra firmware-struktur]	R	R/W	R	R	–	–
• [Fel lösenord har angetts flera gånger]	–	R/W	–	–	–	–
• [Säkerhetsinställning för åtkomstöverträdelse]	–	R/W	–	–	–	–
• [Enhet utsatt för åtkomstöverträdelse]	–	R/W	–	–	–	–
[Programmera/Ändra/Radera LDAP-server]*3	–	R/W	–	–	R/W	R
[I viloläge genom Timer för viloläge]	R	R/W	R	R	R/W	R
[Testservicesamtal]	–	R/W	–	–	R/W	–
[Meddela maskinstatus]	–	R/W	–	–	R/W	–

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Serviceläges lås]	R	R/W	R	R	R/W	R
[Firmware-version]	R	R	R	R	R	R
[Säkerhetsnivå för nätverk]	R	R	R/W	R	R	R
[Radera minnesinställning automatiskt]	R	R/W	R	R	R	R
[Radera allt minne]	–	R/W	–	–	–	–
[Radera alla loggar]	–	R/W	–	–	R/W	–
[Överför logginställning]*11	R	R/W	R	R	R/W	R
[Skydd mot obehörig kopieutskrift: Skrivare]	R	R/W	R	R	R/W	R
[Programmera/Ändra/Ta bort realm]	–	R/W	–	–	R/W	R
[Krypteringsinställningar för maskinens data]	–	R/W	–	–	–	–
[Programmera/ändra enhetscertifikat]	–	–	R/W	–	–	–
[Klarläge efter utskrift]	R	R/W	R	R	R/W	R
[Info om enhetsinställning: Importinställning (server)]*12	–	–	–	–	–	–
[Info om enhetsinställning: Kör import (server)] *12	–	–	–	–	–	–
[Info om enhetsinställning:Export (minnesenh)]*12	–	–	–	–	–	–
[Info om enhetsinställning: Import (minnesenh)]*12	–	–	–	–	–	–
[Energispartangent för ändring av läge]	R	R/W	R	R	R/W	R
[Användarens egna startsida]	R	R/W	R	R	R/W	R
[Räkneverk f utskr.volym: Schemalagd/ang återställn.inst.]	R	R/W	R	R	R	R
[Välj valbart språk]	–	R/W	–	–	R/W	–
[Samla in loggar]	R	R/W	R	R	R/W	R

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Central adressbokshantering]						
• [Central adressbokshantering]	R	R/W	R	R	R	R
• [Klientsynkronisering]*13	R/W	R/W	R	R	R	R
• [Synka mot server]*14	R/W	R/W	R	R	R	R

*3 Lösenord kan inte läsas.

*4 Endast rubrikändringar och användarsökningar är möjliga.

*5 Poster som kan utföras, ändras och läsas varierar beroende på åtkomstbehörighet.

*6 Kan endast rensas.

*7 Kan endast skrivas ut.

*8 Kan inte ändras när den individuella autentiseringsfunktionen används.

*9 Endast inställningarna för administratörsrättigheter kan ändras.

*10 Administratörer kan endast ändra sina egna konton.

*11 Kan endast ändras till [Av].

*12 R/W kan utföras av en administratör med alla de rättigheter som användaradministratören, maskinadministratören, nätverksadministratören och filadministratören har

*13 Detta visas om du använder maskinen som server.

*14 Detta visas om du använder maskinen som klient.

Papperskassettinställning

I det här avsnittet visas inställningarna som visas när du trycker på [Pappersinställning] på kontrollpanelen.

När administratörsautentisering har ställts in varierar restriktionerna för användaråtgärder beroende på konfigurationerna i "Tillgängliga inst.".

[Kassettpprinställningar]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Papperskassett]	R	R/W	R	R	R/W	R
[Redigera anpassat format]	–	R/W	–	–	R/W	–

Redigera startsida

När administratörsautentisering har ställts in varierar restriktionerna för användaråtgärder beroende på konfigurationerna i "Tillgängliga inst.".

[Redigera startsida]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Flytta ikon]	R	R/W	R	R	R/W	R
[Radera ikon]	R	R/W	R	R	R/W	R
[Lägg till ikon]	–	R/W	–	–	R/W	–
[Återställ standardikoner]	–	R/W	–	–	R/W	–
[Infoga bild på startsida]	–	R/W	–	–	R/W	–

Justeringsinställningar för användare

Inställningar	Använ dare	Mask	N/V	Fil	Inga inst.	Inst.
[Justeringsinställingar för användare]	R/W	R/W	R/W	R/W	R/W	R/W

Justeringsinställningar för kvalificerade användare

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Justeringsinställningar för kvalificerade användare]	–	R/W	–	–	–	–

Skrivarfunktioner

I det här avsnittet listas de skrivarfunktioner som visas när du trycker på [Skrivare] på Startsidan.

När administratörautentisering har ställts in skiljer sig restriktionerna för användaråtgärder åt beroende på inställningarna för "Skydda meny".

Skrivarfunktioner

Inställningar	Användare	Mask	N/V	Fil	Nv.1	Nv.2
[Jobblist]	R	R	R	R	R	R
[Utskriftsjobb]	R	R	R	R/W	R/W	R/W
[Skriv ut från minnesenhet]	–	–	–	–	R/W	R/W
[Återställ jobb]	R/W	R/W	R/W	R/W	R/W	R/W
[Jobbåtgärd]	R/W	R/W	R/W	R/W	R/W	R/W
[Sidmatning]	R/W	R/W	R/W	R/W	R/W	R/W
[Jobblista, spoolutskr]	R	R/W	R	R	R	R
[Fellogg]	–	R	–	–	R	R

Skrivarinställningar

När administratörautentisering har ställts in skiljer sig restriktionerna för användaråtgärder åt beroende på inställningarna för "Skydda meny".

[Lista/Provutskrift]

Inställningar	Användare	Mask	N/V	Fil	Nv.1	Nv.2
[Flera listor]	–	R/W	–	–	R/W	R/W
[Konfigurationssida]	–	R/W	–	–	R/W	R/W
[Fellogg]	–	R/W	–	–	R/W	R/W
[PCL konfiguration/fontsida]	–	R/W	–	–	R/W	R/W
[PS konfiguration/fontsida]	–	R/W	–	–	R/W	R/W
[PDF konfiguration/fontsida]	–	R/W	–	–	R/W	R/W
[Hexdump]	–	R/W	–	–	R/W	R/W

[Datahantering]

Inställningar	Användare	Mask	N/V	Fil	Nv.1	Nv.2
[Skydda meny]	R	R/W	R	R	R	R
[Lås Lista/Provutskrift]	R	R/W	R	R	R	R
[Ta bort alla tillfälliga utskriftsjobb]	–	–	–	R/W	–	–
[Ta bort alla lagrade utskriftsjobb]	–	–	–	R/W	–	–
[Ta bort tillf. utskr.jobb automatiskt]	R	R	R	R/W	R	R
[Ta bort lagrade utskr.jobb automat.]	R	R	R	R/W	R	R
[Fyrfärgs grafikläge]	R	R	R	R/W	R	R
[Färgkalibrering]	R	R	R	R/W	R	R

[System]

Inställningar	Användare	Mask	N/V	Fil	Nv.1	Nv.2
[Skriv ut felrapport]	R	R/W	R	R	R	R
[Auto fortsätt]	R	R/W	R	R	R	R
[Lagra & hoppa över felaktiga jobb]	R	R/W	R	R	R	R
[Minnesspill]	R	R/W	R	R	R	R
[Autobekr. för Avbryt jobb vid PDL-fel]	R	R/W	R	R	R	R
[Avbryt utskriftsjobb automatiskt vid fel]	R	R/W	R	R	R	R
[Jobbdelning]	R	R/W	R	R	R	R
[Rotera 180 grader]	R	R/W	R	R	R	R
[Skriv ut komprimerad data]	R	R/W	R/W	R	R	R
[Duplex]	R	R/W	R	R	R	R
[Kopior]	R	R/W	R	R	R	R
[Skriv ut tom sida]	R	R/W	R	R	R	R
[Spoolarea]	R	R/W	R	R	R	R
[Skrivarspråk]	R	R/W	R	R	R	R
[Subpappersformat]	R	R/W	R	R	R	R
[Sidformat]	R/W	R/W	R	R	R	R
[Brevhuvudsinställning]	R	R/W	R	R	R	R
[Prioritetet för inst. av ppr.kassett]	R	R/W	R	R	R	R
[Kant-till-kantutskrift]	R	R/W	R	R	R	R
[Standardspråk för skrivare]	R	R/W	R	R	R	R
[Kassettbyte]	R	R/W	R	R	R	R
[Utöka autom. kassettbyte]	R	R/W	R	R	R	R
[Det finns outskrivna jobb pga avst. maskin.]	R	R/W	R	R	R	R

Inställningar	Användare	Mask	N/V	Fil	Nv.1	Nv.2
[Begränsa direktutskriftsjobb]	R	R/W	R	R	R	R
[Byt startskärm]	R	R/W	R	R	R	R

[Värdgränssnitt]

Inställningar	Användare	Mask	N/V	Fil	Nv.1	Nv.2
[I/O-buffert]	R	R/W	R	R	R	R
[I/O-Timeout]	R	R/W	R	R	R	R

[PCL-meny]

Inställningar	Användare	Mask	N/V	Fil	Nv.1	Nv.2
[Riktning]	R	R/W	R	R	R	R
[Rader per sida]	R	R/W	R	R	R	R
[Fontkälla]	R	R/W	R	R	R	R
[Fontnummer]	R	R/W	R	R	R	R
[Punkstorlek]	R	R/W	R	R	R	R
[Breddsteg]	R	R/W	R	R	R	R
[Symbolval]	R	R/W	R	R	R	R
[Courier-font]	R	R/W	R	R	R	R
[Utöka A4-bredd]	R	R/W	R	R	R	R
[Bifoga CR till LF]	R	R/W	R	R	R	R
[Upplösning]	R	R/W	R	R	R	R

[PS-meny]

Inställningar	Användare	Mask	N/V	Fil	Nv.1	Nv.2
[Jobb-timeout]	R	R/W	R	R	R	R
[Vänte-timeout]	R	R/W	R	R	R	R
[Metod för pappersval]	R	R/W	R	R	R	R
[Växla mellan 1- och 2-sidig utskriftsfunktion]	R	R/W	R	R	R	R
[Dataformat]	R	R/W	R	R	R	R
[Upplösning]	R	R/W	R	R	R	R
[Tonerbesparing]	R	R/W	R	R	R	R
[Färginställning]	R	R/W	R	R	R	R
[Färgprofil]	R	R/W	R	R	R	R
[Bearbeta färgmodell]	R	R/W	R	R	R	R
[Auto avkänning: riktning]	R	R/W	R	R	R	R
[Gråskaleåtergivning]	R	R/W	R	R	R	R

[PDF-meny]

Inställningar	Användare	Mask	N/V	Fil	Nv.1	Nv.2
[Byt PDF-lösenord]	R	R/W	R	R	R	R
[PDF-lösenord för grupp]	R	R/W	R	R	R	R
[Omvänd utskriftsordning]	R	R/W	R	R	R	R
[Upplösning]	R	R/W	R	R	R	R
[Tonerbesparing]	R	R/W	R	R	R	R
[Färginställning]	R	R/W	R	R	R	R
[Färgprofil]	R	R/W	R	R	R	R
[Bearbeta färgmodell]	R	R/W	R	R	R	R

Inställningar	Användare	Mask	N/V	Fil	Nv.1	Nv.2
[Auto avkänning: riktning]	R	R/W	R	R	R	R

Inställningar för utökade funktioner

[Inställn. för utökade funktioner]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Startinställning]	R	R/W	R	R	R	R
[Installera]	R	R/W	R	R	R	R
[Avinstallera]	R	R/W	R	R	R	R
[Information om utökad funktion]	R	R/W	R	R	R	R
[Admin.verktyg]	–	R/W	–	–	–	–
[Tilläggsprogram Startinställning]	R	R/W	R	R	R	R
[Installera tilläggsprog.]	R	R/W	R	R	R	R
[Avinstallera tilläggsprog.]	R	R/W	R	R	R	R
[Tilläggsprog. info]	R	R/W	R	R	R	R

Underhåll

När administratörsautentisering har ställts in varierar restriktionerna för användaråtgärder beroende på konfigurationen i "Tillgängliga inst.".

[Underhåll]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Färgregistrering]	–	R/W	–	–	R/W	–

Web Image Monitor: Visa miljöanpassat räkneverk

Dessa inställningar finns i [Status/information].

En användare kan endast granska sitt eget räkneverk.

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Hämta]	–	R/W	–	–	–	–
[Total räkeverksställning för enhet]	–	R	–	–	–	–
[Räkneverk per användare]	–	R	–	–	R	R

Web Image Monitor: Jobb

Dessa inställningar finns i [Status/information].

Användare kan bara ändra jobb som de själva har verkställt.

[Jobblista]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Aktuella/Väntande jobb]: [Ta bort reservation]	–	R/W	–	–	–	R/W
[Aktuella/Väntande jobb]: [Pausa utskrift]/ [Fortsätt utskrift]	–	R/W	–	–	–	–
[Aktuella/Väntande jobb]: [Ändra ordning]	–	R/W	–	–	–	–
[Jobbhistorik]	–	R	–	–	R	R*1

*1 Kan granskas när användarkodautentisering är aktiverat som användarautentiseringsmetod.

[Skrivare]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Spoolutskrift]: [Radera]	R	R/W	R	R	R	R
[Jobbhistorik]	R	R/W	R	R	R	R
[Fellogg]	–	R	–	–	R	R

Web Image Monitor: Enhetsinställningar

Dessa inställningar finns i [Konfiguration] i [Enhetshantering].

När administratörsautentisering har ställts in varierar restriktionerna för användaråtgärder beroende på konfigurationen i "Tillgängliga inst.".

[System]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Enhetsnamn]	R	R	R/W	R	R/W	R
[Kommentar]	R	R	R/W	R	R/W	R
[Plats]	R	R	R/W	R	R/W	R
[Displayspråk]	R	R/W	R	R	R/W	R
[Spoolutskrift]	R	R/W	R	R	R/W	R
[Energispartangent för att ändra läge]	R	R/W	R	R	R/W	R
[Visa IP-adress på enhetens display]	R	R/W	R	R	–	–
[Använd Mediaanslutning]	R	R/W	R	R	R	R
[Kompatibelt ID]	R	R/W	R	R	R/W	R
[Förhindra att lagrade filer skrivs ut från Web Image Monitor]	R	R/W	R	R	R	R
[Utmatningsfack]	R	R/W	R	R	R/W	R
[Kassettprioritet]	R	R/W	R	R	R/W	R

[Fördelning av funktionstangent/funktionsprioritet]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Fördelning av funktionstangent]	R	R/W	R	R	R/W	R
[Funktionsprioritet]	R	R/W	R	R	R/W	R

[Papper]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Kassett 1-8]	R	R/W	R	R	R/W	R
[Kassett A]	R	R/W	R	R	R/W	R
[Mellanarksfackets övre fack]	R	R/W	R	R	R/W	R
[Mellanarksfackets nedre fack]	R	R/W	R	R	R/W	R
[Mellanarksfack för limbindare: övre kassett]	R	R/W	R	R	R/W	R
[Mellanarksfack för limbindare: nedre kassett]	R	R/W	R	R	R/W	R
[Svag pappersidentifiering]	R	R/W	R	R	R	R

[Anpassat pappersformat]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Programmera/ändra]	–	R/W	–	–	R/W	–
[Radera]	–	R/W	–	–	R/W	–
[Återkalla papperskatalog]	–	R/W	–	–	R/W	–

[Datum/Tid]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Ange datum]	R	R/W	R	R	R/W	R
[Ange tid]	R	R/W	R	R	R/W	R
[SNTP-servernamn]	R	R/W	R	R	R/W	R
[SNTP-pollingintervall]	R	R/W	R	R	R/W	R
[Tidszon]	R	R/W	R	R	R/W	R

[Timer]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Timer för viloläge]	R	R/W	R	R	R/W	R
[Timer för energisparläge]	R	R/W	R	R	R/W	R
[Timer för automatisk återställning av systemet]	R	R/W	R	R	R/W	R
[Timer för automatisk återställning av skrivare]	R	R/W	R	R	R/W	R
[Timer för automatisk utloggning]	R	R/W	R	R	R/W	R
[Avstängt läge, fixeringsenhet På/Av]	R	R/W	R	R	R/W	R
[Veckotimer]	R	R/W	R	R	R/W	R

[Loggar]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Jobblogg]	R	R/W	R	R	R/W	R
[Åtkomstlogg]	R	R/W	R	R	R/W	R
[Miljöanpassade loggar]	R	R/W	R	R	R/W	R
[Överför loggar]*2	R	R/W	R	R	R/W	R
[Klassificeringskod]	R	R/W	R	R	R/W	R
[Radera alla loggar]	–	R/W	–	–	R/W	–

*2 Kan endast ändras till [Ej aktivt].

[Ladda ner loggar]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Loggar att hämta]	–	R/W	–	–	–	–
[Hämta]	–	R/W	–	–	–	–

[E-post]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Administratörens e-postadress]	–	R/W	–	–	R/W	R
[Mottagningsprotokoll]	–	R/W	–	–	R/W	R
[Intervall för e-postmottagning]	–	–	R/W	–	R/W	R
[E-postlagring i server]	–	–	R/W	–	R/W	R
[SMTP-servernamn]	–	–	R/W	–	R/W	R
[SMTP-portnummer]	–	–	R/W	–	R/W	R
[Använd säker anslutning (SSL)]	–	–	R/W	–	R/W	R
[SMTP-autentisering]	–	R/W	–	–	R/W	R
[SMTP-autentisering]	–	R/W	–	–	R/W	R
[Användarnamn för SMTP-autentisering]	–	R/W	–	–	R/W	–
[Lösenord för SMTP-autentisering]*3	–	R/W	–	–	R/W	–
[Kryptering av SMTP-autententisering]	–	R/W	–	–	R/W	R
[POP före SMTP]	–	R/W	–	–	R/W	R
[E-postadress för POP]	–	R/W	–	–	R/W	R
[POP-användarnamn]	–	R/W	–	–	R/W	–
[POP-lösenord]*3	–	R/W	–	–	R/W	–
[Timeout-inställningar efter POP-autentisering]	–	R/W	–	–	R/W	R
[POP3/IMAP4-servernamn]	–	R/W	–	–	R/W	R
[POP3/IMAP4-kryptering]	–	R/W	–	–	R/W	R
[Portnummer för POP3-mottagning]	–	–	R/W	–	R/W	R
[Portnummer för IMAP4-mottagning]	–	–	R/W	–	R/W	R
[E-postadress för e-postavisering]	–	R/W	–	–	R/W	R
[Ta emot e-postavisering]	–	R/W	–	–	R/W	–

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Användarnamn för e-postavisering]	–	R/W	–	–	R/W	–
[Lösenord för e-postavisering]*3	–	R/W	–	–	R/W	–

*3 Lösenord kan inte läsas.

[Automatisk e-postavisering]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Aviseringsmeddelande]	R	R/W	R	R	R/W	R
[Grupper som ska meddelas]	R	R/W	R	R	R/W	R
[Välj grupper/poster som ska meddelas]	R	R/W	R	R	R/W	R
[Detaljerade inställningar för varje post]	R	R/W	R	R	R/W	R

[E-postavisering på begäran]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Ämne för meddelande]	R	R/W	R	R	R/W	R
[Aviseringsmeddelande]	R	R/W	R	R	R/W	R
[Åtkomstbegränsning till information]	R	R/W	R	R	R/W	R
[Mottagbara inställningar för e-postadress/ domännamn]	R	R/W	R	R	R/W	R

[Hantering av användarautentisering]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Hantering av användarautentisering]	R	R/W	R	R	R/W	R
[Inställningar för autentisering av utskriftsjobb]	R	R/W	R	R	R/W	R
[Autentiseringsinställningar för användarkod]	R	R/W	R	R	R/W	R

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Grundläggande autentiseringsinställningar]	R	R/W	R	R	R/W	R
[Inställningar för Windows-autentisering]	R	R/W	R	R	R/W	R
[Gruppinställningar för Windows-autentisering]	R	R/W	R	R	R/W	R
[Inställningar för LDAP-autentisering]	R	R/W	R	R	R/W	R

[Hantering av administratörsautentisering]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Autentisering av användaradministratör]	R/W	R	R	R	R	R
[Autentisering av maskinadministratör]	R	R/W	R	R	R	R
[Autentisering av nätverksadministratör]	R	R	R/W	R	R	R
[Autentisering av filadministratör]	R	R	R	R/W	R	R

[Programmera/ändra administratör]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Användaradministratör]	R/W	R	R	R	–	–
[Maskinadministratör]	R	R/W	R	R	–	–
[Nätverksadministratör]	R	R	R/W	R	–	–
[Filadministratör]	R	R	R	R/W	–	–
[Användarnamn]*4	R/W	R/W	R/W	R/W	–	–
[Lösenord]*4	R/W	R/W	R/W	R/W	–	–
[Krypteringslösen]*4	R/W	R/W	R/W	R/W	–	–

*4 Administratörer kan endast ändra sina egna konton.

[Begränsad utskriftsvolym]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Maskinåtgärd när begränsning är nådd]	R	R/W	R	R	R	R
[Begränsad utskriftsvolym: räkneverksinställning]	R	R/W	R	R	R	R
[Räkneverk för utskriftsvolym: Inställning för schemalagd/angiven återställning]	R	R/W	R	R	R	R

[LDAP-server]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Ändra]	–	R/W	–	–	R/W	–
[Radera]	–	R/W	–	–	R/W	–

[Uppdatering av firmware]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Uppdatera]	–	R/W	–	–	–	–
[Firmware-version]	–	R	–	–	–	–

[Kerberos-autentisering]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Krypteringsalgoritm]	–	R/W	–	–	–	–
[Realm 1-5]	–	R/W	–	–	–	–

[Info om enhetsinställning: Importinställning (server)]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Importera fil från]*5	–	–	–	–	–	–
[Schemalagd import vid angiven tidpunkt]*5	–	–	–	–	–	–
[Jämför ny fil med senast importerad fil]*5	–	–	–	–	–	–
[E-postavisering vid fel]*5	–	–	–	–	–	–
[Antal försök]*5	–	–	–	–	–	–
[Försöksintervall]*5	–	–	–	–	–	–
[Krypteringskod]*5	–	–	–	–	–	–

*5 R/W är en administratör med alla de rättigheter som användaradministratören, maskinadministratören, nätverksadministratören och filadministratören har.

[Importera test]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Start]*5	–	–	–	–	–	–

*5 R/W är en administratör med alla de rättigheter som användaradministratören, maskinadministratören, nätverksadministratören och filadministratören har.

[Importera/exportera info om enhetsinställning]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Exportera info om enhetsinställning]*5	–	–	–	–	–	–
[Importera info om enhetsinställning]*5	–	–	–	–	–	–
[Användares egna startsida]*5	–	–	–	–	–	–

*5 R/W är en administratör med alla de rättigheter som användaradministratören, maskinadministratören, nätverksadministratören och filadministratören har.

[Miljöanpassad räkneverksperiod/administratörsmeddelande]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Visa informationsskärm]	R	R/W	R	R	R/W	R
[Visa tid]	R	R/W	R	R	R/W	R
[Beräkningsperiod]	R	R/W	R	R	R/W	R
[Beräkningsperiod (dagar)]	R	R/W	R	R	R/W	R
[Administratörsmeddelande]	R	R/W	R	R	R/W	R

[Skydd mot obehörig kopiering: Skrivare]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Inställning för skydd mot obehörig kopiering]	R	R/W	R	R	R	R
[Obligatoriskt skydd mot obehörig kopiering]	R	R/W	R	R	R	R
[Typ av skydd mot obehörig kopiering]	R	R/W	R	R	R	R
[Masktyp för mönster/densitet/effekt]	R	R/W	R	R	R	R
[Inställning för skyddstext]	R	R/W	R	R	R	R

[Program/Change USB Device List]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Device 1]	R	R/W	R	R	R/W	R
[Device 2]	R	R/W	R	R	R/W	R

Web Image Monitor: Skrivare

Dessa inställningar finns i [Konfiguration] i [Enhetshantering].

När administratörautentisering har ställts in skiljer sig restriktionerna för användaråtgärder åt beroende på inställningarna för "Skydda meny".

[Grundinställningar]

Inställningar	Användare	Mask	N/V	Fil	Nv.1	Nv.2
[Rapport för skrivarfel]	R	R/W	R	R	R	R
[Fortsätt automatiskt]	R	R/W	R	R	R	R
[Minnesspill]	R	R/W	R	R	R	R
[Bekräftelse för autoavbryt jobb vid skrivarspråksfel]	R	R/W	R	R	R	R
[Autoavbryt för utskriftsjobb vid fel]	R	R/W	R	R	R	R
[Jobbdelning]	R	R/W	R	R	R	R
[Ta bort tillfälliga utskriftsjobb automatiskt]	R	R	R	R/W	R	R
[Ta bort lagrade filer automatiskt]	R	R	R	R/W	R	R
[Jobb ej utskrivna pga avslagen maskin]	R	R/W	R	R	R	R
[Rotera 180 grader]	R	R/W	R	R	R	R
[Skriv ut komprimerad data]	R	R/W	R/W	R	R	R
[Duplex]	R	R/W	R	R	R	R
[Kopior]	R	R/W	R	R	R	R
[Skriv ut tom sida]	R	R/W	R	R	R	R
[Spoolarea]	R	R/W	R	R	R	R
[Skrivarspråk]	R	R/W	R	R	R	R
[Subpappersformat]	R	R/W	R	R	R	R
[Sidformat]	R	R/W	R	R	R/W	R
[Brevhuvudsinställning]	R	R/W	R	R	R	R

Inställningar	Användare	Mask	N/V	Fil	Nv.1	Nv.2
[Prioritet för inställning av kassett]	R	R/W	R	R	R	R
[Lagra & hoppa över felaktiga jobb]	R	R/W	R	R	R	R
[Kant-till-kantutskrift]	R	R/W	R	R	R	R
[Standardskrivarspråk]	R	R/W	R	R	R	R
[Kassettbyte]	R	R/W	R	R	R	R
[Lås på Lista/Provutskrift]	R	R/W	R	R	R	R
[Utökat automatiskt kassettskifte]	R	R/W	R	R	R	R
[Virtuell skrivare]	R	R/W	R	R	R	R
[Begränsa direktutskriftsjobb]	R	R/W	R	R	R	R
[Inställning för byte av startskärm]	R	R/W	R	R	R	R
[Värdgränssnitt]	R	R/W	R	R	R	R
[PCL-meny]	R	R/W	R	R	R	R
[PS-meny]	R	R/W	R	R	R	R
[PDF-meny]	R	R/W	R	R	R	R

[Kassettparametrar (PCL)]

Inställningar	Användare	Mask	N/V	Fil	Nv.1	Nv.2
[Kassettparametrar (PCL)]	–	R/W	–	–	–	–

[Kassettparametrar (PS)]

Inställningar	Användare	Mask	N/V	Fil	Nv.1	Nv.2
[Kassettparametrar (PS)]	–	R/W	–	–	–	–

[Tillfälligt PDF-lösenord]

Inställningar	Användare	Mask	N/V	Fil	Nv.1	Nv.2
[Tillfälligt PDF-lösenord]	–	–	–	–	R/W	R/W

[PDF-grupplösenord]

Inställningar	Användare	Mask	N/V	Fil	Nv.1	Nv.2
[PDF-grupplösenord]	–	R/W	–	–	–	–

[Fast PDF-lösenord]

Inställningar	Användare	Mask	N/V	Fil	Nv.1	Nv.2
[Fast PDF-lösenord]	–	R/W	–	–	–	–

[Inställningar för virtuell skrivare]

Inställningar	Användare	Mask	N/V	Fil	Nv.1	Nv.2
[Virtuellt skrivarnamn]	R	R/W	R	R	R	R
[Protokoll]	R	R/W	R	R	R	R
[Rapport för skrivarfel]	R	R/W	R	R	R	R
[Jobbdelning]	R	R/W	R	R	R	R
[Rotera 180 grader]	R	R/W	R	R	R	R
[Duplex]	R	R/W	R	R	R	R
[Kopior]	R	R/W	R	R	R	R
[Skriv ut tom sida]	R	R/W	R	R	R	R
[Subpappersformat]	R	R/W	R	R	R	R
[Kassett]	R	R/W	R	R	R/W	R/W
[Sidformat]	R	R/W	R	R	R/W	R

Inställningar	Användare	Mask	N/V	Fil	Nv.1	Nv.2
[Papperstyp]	R	R/W	R	R	R/W	R/W
[Utmatningsfack]	R	R/W	R	R	R/W	R/W
[Brevhuvudsinställning]	R	R/W	R	R	R	R
[Kant-till-kantutskrift]	R	R/W	R	R	R	R
[PCL-meny]	R	R/W	R	R	R	R
[PS-meny]	R	R/W	R	R	R	R
[PDF-meny]	R	R/W	R	R	R	R
[RHPP-inställningar]	R	R/W	R	R	R/W	R/W

[Tillstånd för skrivarspråk att bearbeta filsystem]

Inställningar	Användare	Mask	N/V	Fil	Nv.1	Nv.2
[PJL]	R	R/W	R	R	R	R
[PDF, PostScript]	R	R/W	R	R	R	R

Web Image Monitor: Gränssnitt

Dessa inställningar finns i [Konfiguration] i [Enhetshantering].

När administratörsautentisering har ställts in varierar restriktionerna för användaråtgärder beroende på konfigurationen i "Tillgängliga inst.".

[Gränssnittsinställningar]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Nätverk]	R	R	R	R	R	R
[MAC-adress]	R	R	R	R	R	R
[Ethernetsäkerhet]	R	R	R/W	R	R/W	R
[Ethernethastighet]	R	R	R/W	R	R/W	R
[USB-värd]	R	R/W	R	R	R/W	R

Web Image Monitor: Nätverk

Dessa inställningar finns i [Konfiguration] i [Enhetshantering].

När administratörsautentisering har ställts in varierar restriktionerna för användaråtgärder beroende på konfigurationen i "Tillgängliga inst.".

[IPv4]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[IPv4]	R	R	R/W*1	R	R/W*1	R
[Värdnamn]	R	R	R/W	R	R/W	R
[DHCP]	R	R	R/W	R	R/W	R
[Domännamn]	R	R	R/W	R	R/W	R
[IPv4-adress]	R	R	R/W	R	R/W	R
[Subnätmask]	R	R	R/W	R	R/W	R
[DDNS]	R	R	R/W	R	R/W	R
[WINS]	R	R	R/W	R	R/W	R
[Primär WINS-server]	R	R	R/W	R	R/W	R
[Sekundär WINS-server]	R	R	R/W	R	R/W	R
[LLMNR]	R	R	R/W	R	R/W	R
[Scope-ID]	R	R	R/W	R	R/W	R
[Detaljer]	R	R	R/W	R	R/W	R

*1 Du kan inte inaktivera IPv4 när du använder Web Image Monitor genom en IPv4-anslutning.

[IPv6]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[IPv6]	R	R	R/W*2	R	R/W*2	R

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Värdnamn]	R	R	R/W	R	R/W	R
[Domännamn]	R	R	R/W	R	R/W	R
[Link-localadress]	R	R	R	R	R	R
[Stateless-adress]	R	R	R/W	R	R/W	R
[Manuell konfigurationsadress]	R	R	R/W	R	R/W	R
[DHCPv6]	R	R	R/W	R	R/W	R
[DHCPv6-adress]	R	R	R	R	R	R
[DDNS]	R	R	R/W	R	R/W	R
[LLMNR]	R	R	R/W	R	R/W	R
[Detaljer]	R	R	R/W	R	R/W	R

*2 Du kan inte inaktivera IPv6 när du använder Web Image Monitor genom en IPv6-anslutning.

[NetWare]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[NetWare]	R	R	R/W	R	R/W	R
[NetWare-utskriftsinställningar]	R	R	R/W	R	R/W	R
[NCP-leverans]	R	R	R/W	R	R/W	R

[SMB]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[SMB]	R	R	R/W	R	R/W	R
[Protokoll]	R	R	R	R	R	R
[Arbetsgruppnamn]	R	R	R/W	R	R/W	R
[Datornamn]	R	R	R/W	R	R/W	R

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Kommentar]	R	R	R/W	R	R/W	R
[Delningsnamn]	R	R	R	R	R	R
[Meddela när utskrift är klar]	R	R	R/W	R	R/W	R

[SNMP]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[SNMP]	–	–	R/W	–	–	–
[Protokoll]	–	–	R/W	–	–	–
[Inställning SNMPv1, v2]	–	–	R/W	–	–	–
[Grupp]	–	–	R/W	–	–	–

[SNMPv3]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[SNMP]	–	–	R/W	–	–	–
[Protokoll]	–	–	R/W	–	–	–
[SNMPv3-inställning]	–	–	R/W	–	–	–
[SNMPv3 Trap Communication Setting]	–	–	R/W	–	–	–
[Konto (Användare)]	–	–	R/W	–	–	–
[Konto (Nätverksadministratör)]	–	–	R/W	–	–	–
[Konto (Maskinadministratör)]	–	R/W	–	–	–	–

[SSDP]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[SSDP]	–	–	R/W	–	–	–

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[UUID]	–	–	R	–	–	–
[Profil gäller till]	–	–	R/W	–	–	–
[TTL]	–	–	R/W	–	–	–

[Bonjour]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Bonjour]	R	R	R/W	R	R/W	R
[Lokalt värdnamn]	R	R	R	R	R	R
[Detaljer]	R	R	R/W	R	R/W	R
[Prioritetsordning för utskrift]	R	R	R/W	R	R/W	R

[Systemlogg]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Systemlogg]	R	R	R	R	R	–

Web Image Monitor: Säkerhet

Dessa inställningar finns i [Konfiguration] i [Enhetshantering].

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Nätverkssäkerhet]	–	–	R/W	–	–	–
[Åtkomstkontroll]	–	–	R/W	–	–	–
[IPP-autentisering]	–	–	R/W	–	–	–
[SSL/TLS]	–	–	R/W	–	–	–
[ssh]	–	–	R/W	–	R	R
[Webbplatscertifikat]	–	–	R/W	–	–	–
[Enhetscertifikat]	–	–	R/W	–	–	–
[IPsec]	–	–	R/W	–	–	–
[Princip om utelåsning av användare]	–	R/W	–	–	–	–
[IEEE 802. 1X]	–	–	R/W	–	–	–
[Extended Security]						
• [Krypteringskod för drivrutin]	–	–	R/W	–	R/W	–
• [Driver Encryption Key: Encryption Strength]	R	R	R/W	R	R/W	R
• [Restrict Display of User Information]	R	R/W	R	R	R/W	R
• [Encrypt User Custom Settings & Address Book]	R/W	R	R	R	R	R
• [Enhance File Protection]	R	R	R	R/W	R	R
• [Authenticate Current Job]	R	R/W	R	R	R/W	R
• [@Remote Service]	R	R/W	R	R	R/W	R
• [Update Firmware]	R	R/W	R	R	–	–
• [Change Firmware Structure]	R	R/W	R	R	–	–

Inställningar	Använ dare	Mask	N/V	Fil	Inga inst.	Inst.
• [Password Policy]	R/W	–	–	–	–	–
• [Settings by SNMPv1, v2]	R	R	R/W	R	R/W	R
• [Security Setting for Access Violation]	–	R/W	–	–	–	–
• [Fel lösenord har angetts flera gånger]	–	R/W	–	–	–	–
• [Enhet utsatt för åtkomstöverträdelse]	–	R/W	–	–	–	–

Web Image Monitor: @Remote

Dessa inställningar finns i [Konfiguration] i [Enhetshantering].

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Inställningar för RC Gate]	–	R/W	–	–	–	–
[Uppdatera firmware för RC Gate]	–	R/W	–	–	–	–
[Proxyserver för RC Gate]	–	R/W	–	–	–	–
[Meddela enhets funktionsproblem]	–	R/W	–	–	–	–

Web Image Monitor: Webbsida

Dessa inställningar finns i [Konfiguration] i [Enhetshantering].

När administratörsautentisering har ställts in varierar restriktionerna för användaråtgärder beroende på konfigurationen i "Tillgängliga inst.".

[Webbsida]

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Webbsidans språk]	R	R	R/W	R	R/W	R
[Automatisk utloggning från Web Image Monitor]	R	R	R/W	R	R/W	R
[Ange URL-adress till länkad sida]	R	R	R/W	R	R/W	R
[Ange URL-adress för Hjälp]	R	R	R/W	R	R/W	R
[WSD/UPnP-inställning]	R	R	R/W	R	R/W	R
[Ladda ner Hjälpfil]	R/W	R/W	R/W	R/W	R/W	R/W

Web Image Monitor: Inställn. för utökade funktioner

Dessa inställningar finns i [Konfiguration] i [Enhetshantering].

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Startinställning]	–	R/W	–	–	–	–
[Information om utökade funktioner]	R	R	R	R	R	R
[Installera]	–	R/W	–	–	–	–
[Avinstallera]	–	R/W	–	–	–	–
[Administratörsverktyg]	–	R/W	–	–	–	–
[Startinställning för tilläggsprogram]	–	R/W	–	–	–	–
[Installera tilläggsprogram]	–	R/W	–	–	–	–
[Avinstallera tilläggsprogram]	–	R/W	–	–	–	–
[Kopiera utökade funktioner]	–	R/W	–	–	–	–
[Kopiera kort för datasparing]	–	R/W	–	–	–	–

Web Image Monitor: Adressbok

Dessa inställningar finns i [Enhetshantering].

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Lägg till användare]	R/W	–	–	–	R/W	R/W
[Ändra]	R/W	–	–	–	R/W	R/W
[Radera]	R/W	–	–	–	R/W	R/W
[Lägg till grupp]	R/W	–	–	–	R/W	R/W
[Underhåll]	R/W	–	–	–	–	–
[Central adressbokshantering]	R/W	–	–	–	–	–

Web Image Monitor: Central adressbokshantering

Dessa inställningar finns i [Enhetshantering].

Detta visas inte om du har administratörsrättigheter. Ange i så fall detta i [Enhetshantering] > [Adressbok].

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Central adressbokshantering]	–	R/W	–	–	–	–

Web Image Monitor: Huvudströmbrytare av

Dessa inställningar finns i [Enhetshantering].

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Huvudströmbrytare av]	–	R/W	–	–	–	–
[OK]	–	R/W	–	–	–	–

Web Image Monitor: Återställ skrivarjobb

Dessa inställningar finns i [Enhetshantering].

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Återställ aktuellt jobb]	–	R/W	–	–	–	–
[Återställ alla jobb]	–	R/W	–	–	–	–

Web Image Monitor: Återställ maskinen

Dessa inställningar finns i [Enhetshantering].

När administratörsautentisering har ställts in varierar restriktionerna för användaråtgärder beroende på konfigurationen i "Tillgängliga inst.".

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Återställ maskinen]	–	R/W	–	–	R/W	–

Web Image Monitor: Hantering av startsida

Dessa inställningar finns i [Enhetshantering].

När administratörsautentisering har ställts in varierar restriktionerna för användaråtgärder beroende på konfigurationen i "Tillgängliga inst.".

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Redigera ikoner]	R	R/W	R	R	R/W	R
[Återställ standardikoner]	–	R/W	–	–	R/W	–
[Inställningar för startsida]	R	R/W	R	R	R/W	R

Web Image Monitor: Skärmövervakning

Dessa inställningar finns i [Enhetshantering].

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Visa enhetens skärm]	–	R/W	–	–	–	–

Web Image Monitor: Anpassa skärm efter användare

Det visas om [Användares egna inställningar] är inställd på [Tillåt].

Användare kan endast ändra sina egna inställningar.

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Redigera ikoner]	–	–	–	–	–	R/W
[Återställ standardikoner]	–	–	–	–	–	R/W
[Funktionsprioritet per användare]	–	–	–	–	–	R/W

Web Image Monitor: Skrivare: Utskriftsjobb

Dessa inställningar finns i [Utskriftsjobb/lagrad fil].

De skrivardokument som användare kan hantera är de dokument som användare själva har lagrat eller alla om användarautentisering inte är aktiverat.

Skrivardokument som har lagrats av andra användare visas inte.

Inställningar	Användare	Mask	N/V	Fil	Inga inst.	Inst.
[Skriv ut]	–	–	–	–	R/W*1	R/W*1
[Radera]	–	–	–	R/W	R/W*1	R/W*1
[Redigera detaljerad information]	–	–	–	R/W	R/W*1	R/W*1
[Lås upp jobb]	–	–	–	R/W	–	–

*1 Åtkomst till lagrade dokument kan vara begränsad beroende på användarens privilegier.

Lista över åtkomsträttigheter för lagrade filer

Tyda rubriker

- Läs

  Användare som tilldelats behörigheter för att läsa.

- Redigera

  Användare som tilldelats behörigheter för att redigera.

- R/T

  Användare som tilldelats behörigheter att redigera/radera.

- Fullst.

  Användare som tilldelats fulla rättigheter.

- Ägare

  Indikerar antingen användaren som registrerade ett dokument eller en användare som angetts som ägare.

- Fil

  Indikerar filadministratören.

Tyda symbolerna

R/W: Kan verkställa

–: Kan inte verkställa

I denna tabell listas åtkomsträttigheterna till Web Image Monitor.

Inställningar	Läs	Redigera	R/T	Fullst.	Ägare	Fil
[Skriver ut]	R/W	R/W	R/W	R/W	R/W	–
[Detaljer]	R/W	R/W	R/W	R/W	R/W	R/W
Ändra ägare	–	–	–	–	–	R/W
[Åtkomstbehörighet]: [Behörighet för användare/grupper]	–	–	–	R/W	R/W*1	R/W
[Ändra filnamn]	–	R/W	R/W	R/W	R/W*1	–
[Ändra lösenord]	–	–	–	–	R/W	R/W
[Lås upp filer]	–	–	–	–	–	R/W
[Ta bort fil]	–	–	R/W	R/W	R/W*1	R/W

*1 Ägaren kan ändra åtgärdsrättigheter.

Lista över åtkomsträttigheter för adressböcker

Tyda rubriker

- Läs

  Användare som tilldelats behörigheter för att läsa.

- Redigera

  Användare som tilldelats behörigheter för att redigera.

- R/T

  Användare som tilldelats behörigheter att redigera/radera.

- Fullst.

  Användare som tilldelats fulla rättigheter.

- Post

  Indikerar en användare vars personuppgifter har registrerats i adressboken. Det indikerar även användare som känner till sitt användarnamn och lösenord.

- Användare

  Indikerar användaradministratören.

Tyda symbolerna

R/W: Det är möjligt att verkställa, ändra och läsa.

R: Möjligt att läsa.

–: Det är ej möjligt att verkställa, ändra och läsa.

[Namn]

Inställningar	Läs	Redigera	R/T	Fullst.	Post	Användare
[Namn]	R	R/W	R/W	R/W	R/W	R/W
[Tangentnamn]	R	R/W	R/W	R/W	R/W	R/W
[Registreringsnr]	R	R/W	R/W	R/W	R/W	R/W
[Visa prioritet]	R	R/W	R/W	R/W	R/W	R/W
[Välj titel]	R	R/W	R/W	R/W	R/W	R/W

[Aut.info]

Inställningar	Läs	Redigera	R/T	Fullst.	Post	Användare
[Användarkod]	–	–	–	–	–	R/W
[Användarnamn]	–	–	–	–	R	R/W
[Lösenord]	–	–	–	–	R/W*1	R/W*1
[Tillgängliga funktioner]	–	–	–	–	R	R/W
[Begränsad utskriftsvolym]	–	–	–	–	R	R/W

*1 Lösenord kan inte läsas.

[Skydd]

Inställningar	Läs	Redigera	R/T	Fullst.	Post	Användare
[Skydda mottagare]: [Rättigheter för anv./grupp]	–	–	–	R/W	R/W	R/W

[Lägg till grupp]

Inställningar	Läs	Redigera	R/T	Fullst.	Post	Användare
[Registreringsnr]	R	R/W	R/W	R/W	R/W	R/W
[Sök]	R	R/W	R/W	R/W	R/W	R/W
[Byt titel]	R/W	R/W	R/W	R/W	R/W	R/W

INDEX

S

T

U

W

Å

Ä

Ö

MEMO

MEMO

