

WorkForce Enterprise 2- og AM-serien

Kontorskrivere

Sikre løsninger



EPSON®

Beskytt nettverkssikkerhet uansett hvor utskrift skjer

Det er enkelt å overse viktige sikkerhetstiltak med nettverkstilkoblede enheter i virksomheten din. Og selv om du kanskje ikke har tatt det i betraktning, kan flerfunksjonsskrivere (MFP-er), skannere og andre tilkoblede eller nettverkstilkoblede enheter være åpne for sikkerhetssvakheter.

Fremveksten av hjemme- og hybridarbeid har forsterket denne risikoen. En studie utført av Quocirca¹ fant at 56 % av organisasjonene hadde lidd minst ett tap av data på grunn av et utskriftsrelatert sikkerhetsbrudd, der 83 % forventet å øke utgiftene sine for utskriftssikkerhet i løpet av det kommende året. De viktigste bekymringene for organisasjoner er å sikre

hjemmeutskrift (28 %), beskytte konfidensielle eller sensitive dokumenter fra å bli skrevet ut (28 %) og forstå typen trusler og sårbarheter i utskriftsinfrastrukturen deres (25 %).

Da den gjennomsnittlige kostnaden for et utskriftsrelatert databrudd er € 953 000*, er det ikke noe du har råd til å ta lett på.

Takket være Epsons tilnærming til skriversikkerhet er det imidlertid en risiko du kan redusere, uansett hvor utskriften for virksomheten din skjer.

Topp 3 utfordringer innen utskriftssikkerhet

28 %

Sikre utskrift i et eksternt miljø/
hjemmemiljø

28 %

Beskytte sensitive eller konfidensielle dokumenter fra å bli skrevet ut

25 %

Forstå typene trusler og sårbarheter i utskriftsinfrastrukturen vår



* Basert på £ 820 000 som sitert av Quocirca og konvertert til € 953 000 ved bruk av valutakurs fra xe.com per 07/07/2025.

Epsons sikkerhetserklæring

Å styrke nettverksfunksjonene til enhetene er nøkkelen til vår tilnærming til sikkerhet. Hver eneste Epson WorkForce-skriver er bygd på tre kjerneprinsipper for å sørge for sikkerheten til Epson-enhetene gjennom hele livssyklusen deres:

1. Produktsikkerhet er grunnlaget for kvalitet
2. Informasjon og kunnskap om sikkerhet blir delt aktivt, slik at du alltid er oppdatert
3. Sårbarheter vurderes hele tiden for å sikre maksimal beskyttelse av enheten

Trygg etter design

Beskyttede data og sikre nettverk leveres som standard med Epsons MFP-er, ved hjelp av funksjoner som kan bidra til å overholde EUs personvernforordning (GDPR) og bedriftens sosiale ansvar (CSR). Disse sikkerhetstiltakene, integrert direkte i produktene våre, gir deg forsikringen om at virksomheten din oppfyller sikkerhetskravene dine.

Enhetene våre er uavhengig testet og sikkerhetsvalidert av Keypoint Intelligence. Epsons proprietære skriver/skanner-teknologi for SoC og fastvareplattform beskytter kundeinformasjon og produkter mot sikkerhetstrusler.



Sikker utskrift og skanning

Sikre dokumentpersonvern og forhindre at uautoriserte personer ser uovervåkede utdata ved enheten, ved å sende inn dokumentene dine som en «konfidensiell jobb» fra utskriftsdriveren.

Begrensning av tilgang til funksjoner på enheten kan gjøres ved hjelp av frontpanellåsen.

Sikker kommunikasjon

Filtrer IP-adresser, tjenester og mottaks- og overføringsportnumre som har tilgang til Epson-enheter. Du kan også kryptere all nettverkskommunikasjon ved hjelp av IPSec-funksjonen.

På enheten

Med Epson Device Admin (EDA) blir sikkerheten på enheten enklere å administrere. Funksjonen er kompatibel med et bredt utvalg av de nettverkstilkoblede skriverne våre og lar brukere styre alt via et smart og intuitivt grensesnitt.

PDF-beskyttelse

Legg passordbeskyttelsesfunksjonalitet³ til skannede PDF-filer for å beskytte mot uautoriserte seere og forhindre dokumentredigering og -utskrift.

Dokumentbehandling og databehandling

Administrer flere oppgaver sentralt, fra skannejobbprofiler til brukertilgangsrettigheter. Administratorer kan håndtere en rekke oppgaver sentralt, fra skannejobbprofiler til brukertilgangsrettigheter. IT-administratorer har muligheten til å styre tilgangsrettigheter til jobber på flere måter, inkludert ID-kort, pålogginger/passord og PIN-koder.

Sømløs integrering i IT-infrastruktur med den lokale brukerdatabasen eller katalogtjenester som Microsoft Entra ID og Google Cloud Directory.

Hvis du vil ha mer informasjon om Epsons sikkerhet eller løsninger, kan du skanne kodene eller gå til koblingene nedenfor.

Epson
Solutions Suite



[Epson Solutions Suite](#)



[Produktsikkerhet](#)

Sikkerhet anerkjent over hele verden

Hos Epson gir vi sikkerheten vår referanseverdi på en global skala. Vi oppfyller ISO/IEC 15408³, også kalt Common Criteria (CC), som er en internasjonal standard for sikkerhetstiltak i IT-produkter og systemer, og CCRA-sertifisering, som demonstrerer at produktet er sertifisert i samsvar med Japan Information Technology Security Evaluation and Certification Scheme (JISEC).



Nettverkssikkerhet

Med nettverkssikkerhet som hovedprioritet kan administratorer sette opp individuelle tillatelser og begrensninger for et bredt spekter av nettverksoppgaver. Med WorkForce Enterprise 2-skriverne våre kan administratorer også filtrere IP-adresser, tjenestetyper, mottaks- og overføringsportnumre ved hjelp av IP Sec/IP-filtreringsfunksjonen. Mens de bestemmer seg for om de vil godta eller blokkere bestemte IP-adresser. Vi støtter også SNMPv3 e-postkryptering og TLS1.3.



Beskytte alt-i-ett-skriveren din

For ekstra beskyttelse av skriverne dine kan du velge å blokkere tilgang fra en datamaskin via USB og deaktivere minnekort- og USB-minnegrensesnittene. Du kan også bruke anti-kopi-vannmerking⁵ for å forhindre uautorisert duplisering av originaldokumenter og PDF-kryptering⁵ for å sikre at digitale dokumenter forblir trygge.



Sikker utskrift/skanning

Alternativet «konfidensiell jobb» betyr at du kan beskytte dokumentpersonvern og forhindre uønsket visning av uovervåket utgang.



WPA3

Epsons nyeste MFP-er støtter WPA3⁵, som er den nyeste autentiserings- og krypteringsteknologien for Wi-Fi (trådløst lokalt nett), noe som gir virksomheter mer robust og sterkere beskyttelse for dataene deres over det trådløse nettverket.



Dokumentbeskyttelse

Øk produktivitet og overvåk bruk med sikker utskrift, skanning og kopiering gjennom brukerautentisering.



Tilgangskontroll

Brukerautentisering og funksjonsbegrensninger.



Enhetsbeskyttelse

Verifisering av fastvaresignatur, sikker oppstart og inntrengningsoppdagelse av kjøretid for skadelig programvare.



Sabotasjesikkert blekk

DURABrite™ Pro-blekket vårt trenger fast inn i fibre i papiret, noe som beskytter viktige dokumenter mot manipulering og er i samsvar med ISO 11798:2023.



Brukerdatabeskyttelse

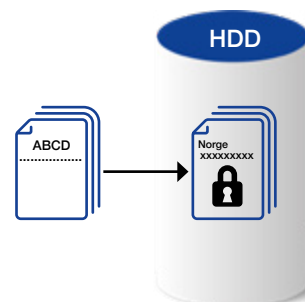
Du kan også angi unike passord for delte bokser⁵, dokumenter og adressebøker på Epson-skriverne dine. For fullstendig sikkerhet slettes data fra skriveren når jobber er fullført eller strømmen er slått av. Hvis enheten har en harddisk, krypteres alle data, og data slettes etter hver utskriftsjobb. For ytterligere beskyttelse kan administratoren også overskrive harddisken. Les mer i [sikkerhetshåndboken vår](#).

Personvern

HDD-kryptering, HDD-sikker datasletting, Trusted Platform Module (TPM) og passordkryptering.

Kryptering av lagrede data i HDD

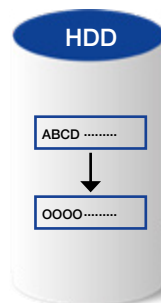
Vi beskytter alltid kundedata med kryptering når man lagrer data på en intern harddisk på en alt-i-ett-skriver. Kryptering av dataene forhindrer uautorisert tilgang eller ondsinnet angrep på personopplysninger hvis harddisken blir stjålet. HDD-en leveres med en selvkrypterende stasjon, og dokumentdataene krypteres med AES-256.



Sekvensiell sletting av jobbdataba

Når det er aktivert, overskrives de slettede dataene på harddisken⁵ på følgende måter for å forhindre gjenoppretting. Det finnes flere alternativer:

1. Rask sletting: Krypteringsnøkkelen endres for å forhindre at slettede data gjenopprettes.
2. Sikker sekvensiell sletting: Krypteringsnøkkelen endres, og de slettede dataene på harddisken overskrives med «0» for å sikre at de slettede dataene ikke kan gjenopprettes.



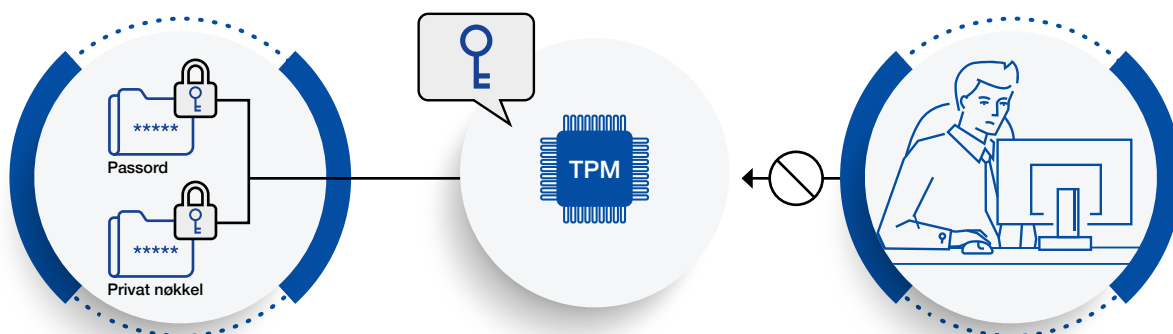
Referer til brukerhåndboken for produktet ditt for en detaljert forklaring av sletting av jobbdataba.

TPM

I modeller med TPM (Trusted Platform Module) forbedres sikkerhetsnivået på følgende måte:

- Krypteringsnøkklene for gjenoppretting av krypterte passord og privat nøkkelinformasjon er lagret på TPM-brikken.
- TPM-brikken kan beskyttes mot uautorisert analyse på maskinvarenivået, da TPM-brikken ikke kan nås fra utenfor skriveren.
- TPMs sanne tilfeldige tall brukes som øktnøkler for kommunikasjon med nettleseren (Web Config).
- TPMs sanne tilfeldige tall brukes til å generere autentiseringsnøkler for den krypterte HDD-en.

Flerfunksjonsskriverne har en TPM 2.0-brikke.



	WorkForce Enterprise	WorkForce Enterprise AM	
Produktnavn	WF-C21000/C20600/C20750	AM-C4000/C5000/ C6000 og AM- M5500	AM-C400/C550/ C550z
Type	A3	A3	A4
Nettverkssikkerhet			
TLS-kommunikasjon	✓	✓	✓
TLS1.1, TLS1.2, TLS1.3	✓	✓	✓
Kontrollere protokolltillatelser og -eksklusjoner	✓	✓	✓
IPsec/IP-filtrering	✓	✓	✓
IKEv1, IKEv2	✓	✓	✓
ESP:AES-CBC-128/AES-CBC-192/AES-CBC-256/3DES	✓	✓	✓
ESP:AES-GCM-128/AES-GCM-192/AES-GCM-256	✓	✓	✓
ESP/AH:SHA-1/MD5	✓	✓	✓
ESP/AH:SHA-256/SHA-384/SHA-512	✓	✓	✓
IEEE802.1X-autentisering	✓	✓	✓
EAP-TLS, PEAP-TLS	✓	✓	✓
PEAP/MSCHAPv2	✓	✓	✓
EAP-TTLS	✓	✓	✓
AES128/AES256/3DES/RC4	✓	✓	✓
SNMPv3	✓	✓	✓
WPA3	✓	✓	✓
Separasjon mellom grensesnitt	✓	✓	✓
Beskytte alt-i-ett-skrivervaren din			
Blokker USB-tilkobling fra datamaskin	✓	✓	✓
Deaktivere det eksterne grensesnittet	✓	✓	✓
Håndtering av virus introdusert av USB-minne	✓	✓	✓
Utskrifts-/skannesikkerhet			
Konfidensielle jobber	✓*6	✓	✓
Antikopieringsmønster ⁶	✓	✓	✓
Vannmerke ⁶	✓	✓	✓
PDF-kryptering	✓	✓	✓
S/MIME	✓	✓	✓
AES-128/AES-192/AES-256/3DES	✓	✓	✓
SHA-1/SHA-256/SHA-384/SHA-512/MD5	✓	✓	✓
Domenebegrensninger	✓*7	✓	✓
Autorisasjonspassord for skanning til nettverksmappe/FTP, skanning til e-post og e-postvarsling	–	✓*7	✓
Støtte for lange autentiseringspassord	–	–	✓*8
Standard deaktivering av filtilgang fra PDL	✓*7	✓	✓
Sikker utskrift	✓	✓	✓
Fakssikkerhet⁹			
Begrensninger for direkte oppringing	✓	✓	✓
Bekreftelse av adresseliste	✓	✓	✓
Gjenkjenning av summetone	✓	✓	✓
Tiltak mot forlatte fakser	✓	✓	✓
Bekreftelsesrapport for overføring	✓	✓	✓
Slette sikkerhetskopieringsdataene for mottatte fakser	✓	✓	✓
Begrens sending til flere mottakere	✓	✓	✓
Skriversikkerhet			
Automatiske fastvareoppdateringer	✓	✓	✓
Beskyttelse mot ulovlige fastvareoppdateringer	–	✓	✓
Sikker oppstart	–	✓	✓
Deteksjon av infiltrering av skadelig programvare	✓*7	✓	✓
Sikkerhetstiltak når du avhender skrivervaren			
Gjenopprett fabrikkstandard	✓	✓	✓
Sikkerhetssertifisering og -standards			
ISO15408/IEEE2600.2™	✓	✓	✓

	WorkForce Enterprise	WorkForce Enterprise AM	
Produktnavn	WF-C21000/C20600/C20750	AM-C4000/C5000/ C6000 og AM-M5500	AM-C400/C550/ C550z
Type	A3	A3	A4
Sikkerhetsfunksjoner gjennom kompatibilitet med tredjepartsprogramvare			
Åpen plattform-samsvarende modell	✓	✓	✓
Epson Print Admin (EPA) / EPA Serverless			
Brukerautentisering via ID-kort/påloggingsinformasjon/PIN-kode	✓	✓	✓
Fullstendig kontroll over enhetens handlinger per enkeltperson	✓	✓	✓
Tilpasning av MFP-menyen	✓	✓	✓
Trekk-utskrift og direkte utskrift	✓	✓	✓
Skann og send til meg (e-post, mappe)	✓	✓	✓
Skann til nettskytjenester (OneDrive for Business, SharePoint Online, Teams og Google Drive) ¹⁰	✓	✓	✓
Skann til passordbeskyttede PDF-filer	✓	✓	✓
Avanserte innstillinger for skannearbeidsflyt ¹¹	✓	✓	✓
Driverløs utskrift fra nettskytjenester (OneDrive for Business, SharePoint Online og Teams) ¹⁰	✓	✓	✓
Synkronisering med katalogtjeneste (LDAP, Open LDAP, Microsoft EntraID, Microsoft Entra DS, Google Secure LDAP og Google Cloud-katalog) ¹⁰	✓	✓	✓
Rapporter – brukerbeskyttelsesinnstilling – skjul filnavn	✓	✓	✓
Retningslinjer for passord, kontolåsing ¹¹	✓	✓	✓
Regler og retningslinjer for utskrift ¹¹	✓	✓	✓
Sporing og rapportering	✓	✓	✓
Kvote ¹⁰	✓	✓	✓
Sikker mobil utskrift (AirPrint og Mopria) ¹²	–	✓	✓
Brukerdatabeskyttelse			
Bokssikkerhet	✓	✓	✓
Beskytte adresseboken din	✓	✓	✓
Datahåndtering behandlet av en alt-i-ett-skriver	✓	✓	✓
Kryptering av lagrede data i harddisk	✓	✓	✓
Sekvensiell sletting av jobbdataba	✓	✓	✓
Kryptering av passord	✓	✓	✓
TPM	✓* ¹³	✓	✓
Speiling av harddisken	–	✓	–
Driftsbegrensning			
Panellås	✓	✓	✓
Tilgangskontroll	✓	✓	✓
Autentisert utskrift/skanning ⁸	✓	✓	✓
Retningslinjer for passord	✓	✓	✓
Overvåkingslogg	✓	✓	✓

Kontakt Epson-salgsrepresentanten din for mer informasjon.

Navn:

Telefon:

E-post:

1. Print Security Landscape, 2025 - Identity, AI, and Quantum: Navigating the New Threat Landscape¹, Quocirca, July 2025.
2. Keypoint Intelligence Security Validation Testing Seal 2024-2026 gjelder for AM-C400 og AM-C550.
3. ISO/IEC 15408 leveres ikke med standard konfigurasjon. Spesiell fastvare og spesiell oppsettsprosess kreves.
4. CCRA-sertifiseringslogoen viser at produktet ble evaluert og sertifisert i samsvar med Japan Information Technology Security Evaluation and Certification Scheme (JISEC). Det innebærer ingen garanti for at produktet er helt fritt for sårbarhet. Det innebærer heller ikke at produktet er utstyrt med alle nødvendige sikkerhetsfunksjoner under alle driftsmiljøer.
5. For en fullstendig liste over modellspesifikasjoner gå til support.epson.net/security/en
6. Støttet bare Windows-skriverdriveren.
7. For å bruke denne funksjonen, oppdater skriverens fastvare til den nyeste versjonen.
8. Krever autentisert utskriftsmetode.
9. Bare tilgjengelig når det alternative faks-kortet er installert.
10. Gjelder Epson Print Admin og bare for spesifikke produkter på Epson Print Admin Serverless.
11. Gjelder bare Epson Print Admin.
12. Gjelder bare Epson Print Admin Serverless.
13. Vil kanskje ikke støttes avhengig av regionen. Kontakt det lokale salgskontoret for tilgjengelighet i landet ditt.



Resirkuler på en ansvarlig måte

Epson Norge
Salgskontor: 67 11 37 70
Support/Service: 21 93 95 04
www.epson.no/contactus

Fjordveien 3
1363 Hovik



@epsonnorge
epson-norge

Varemerker og registrerte varemerker eies av Seiko Epson Corporation eller deres respektive innehavere. Produktopplysningene kan endres uten varsel.

EPSON[®]