WorkForce Enterprise 2 og AM-sortimentet

Erhvervsprintere

Sikre løsninger

EPSON®

Beskyt netværkssikkerheden, uanset hvor udskrivningen sker

Det er nemt at overse vigtige sikkerhedsforanstaltninger med alle netværksenheder i din virksomhed. Selvom du måske ikke har overvejet det, kan multifunktionsprintere (MFP'er), scannere og enhver anden tilsluttet eller netværksforbundet enhed være sårbare over for sikkerhedsrisici.

Stigningen af hjemmearbejde og hybridarbejde har øget denne risiko. En undersøgelse foretaget af Quocirca[1] viste, at 56% af organisationerne havde lidt mindst ét datatab på grund af et udskriftsrelateret sikkerhedsbrud, og 83% forventede at øge deres udgifter til printsikkerhed i det kommende år. De største bekymringer for organisationer er at sikre hjemmeprint (28%), beskytte fortrolige eller følsomme dokumenter mod at blive udskrevet (28%) og forstå typen af trusler og sårbarheder i deres printinfrastruktur (25%).

De gennemsnitlige omkostninger ved et printrelateret databrud er på € 953.000*, så det ikke noget, du har råd til at tage let på.

Takket være Epsons tilgang til printersikkerhed er det dog en risiko, du kan mindske, uanset hvor din virksomheds udskrivning sker.

Top 3 udfordringer med printsikkerhed

28%

Sikring af print i et fjern-/hjemmemiljø

28%

Beskyttelse af følsomme eller fortrolige dokumenter mod print

25%

Forstå typerne af trusler og sårbarheder i vores printinfrastruktur

* Baseret på £ 820.000 som citeret af Quocirca og konverteret til € 953.000 med FX-pris fra xe.com pr. 07/07/2025.

Epsons sikkerhedserklæring

Styrkelse af dine enheders netværksfunktioner er nøglen til vores tilgang til sikkerhed. For at sikre sikkerheden for Epsons enheder i hele deres livscyklus er hver Epson WorkForce-printer bygget på tre kerneprincipper:

1. Produktsikkerhed er grundlaget for kvalitet
2. Information og viden om sikkerhed deles aktivt, så du altid er opdateret
3. Sårbarheder gennemgås konstant for at maksimere beskyttelsen af enheder

Sikker ved design

Databeskyttelse og netværkssikkerhed følger som standard med Epsons MFP'er sammen med funktioner, der kan hjælpe med virksomhedens persondataforordning (GDPR) og Corporate Social Responsibility (CSR). Disse sikkerhedsforanstaltninger, der er integreret direkte i vores produkter, giver dig sikkerhed for, at din virksomhed opfylder dine sikkerhedskrav.

Vores enheder testes uafhængigt og er sikkerhedsvalideret af Keypoint Intelligence. Epsons proprietære printer/scanner SoC og firmwareplatformsteknologi beskytter kundeoplysninger og produkter mod sikkerhedstrusler.

[2]

Sikker print og scanning

Du kan sikre dokumentfortrolighed og forhindre uautoriserede personer i at se ubemandet output på enheden ved at indsende dine dokumenter som et "fortroligt job" fra print-/scanningsdriveren.

Begrænsning af adgang til funktioner på enheden kan gøres ved hjælp af frontpanellåsen.

Sikker kommunikation

Filtrér IP-adresser, tjenester, modtagelses- og transmissionsportnumre osv., der har adgang til Epson enheder. Du kan også kryptere al netværkskommunikation ved brug af IPSec-funktionen.

På enhed

Med Epson Device Admin (EDA) bliver sikkerhed på enheden nemmere at administrere. Det er kompatibelt med et stort udvalg af netværksprintere og gør det muligt for brugerne at styre alt via et smart og intuitivt interface.

PDF-beskyttelse

Tilføj adgangskodebeskyttelsesfunktionalitet[3] til scannede PDF-filer for at beskytte mod uautoriserede brugere og forhindre dokumentredigering og -print.

Dokumentbehandling og datastyring

Administrer flere opgaver centralt fra scanning af jobprofiler til brugeradgangsrettigheder. Administratorer kan styre en lang række opgaver centralt fra scanning af jobprofiler til brugeradgangsrettigheder. IT-administratorer har mulighed for at kontrollere adgangsrettigheder til jobs på en række forskellige måder, herunder ID-kort, login/adgangskode og PIN-koder.

Problemfri integration i IT-infrastruktur med den lokale brugerdatabase eller Directory-tjenester såsom Microsoft Entra ID og Google Cloud Directory.

Du kan få mere at vide om Epsons sikkerhed eller løsninger ved at scanne koderne eller besøge linkene nedenfor.

Epson Solutions Suite

Epson Solutions Suite

Produktsikkerhed

Sikkerhed anerkendt over hele verden

Hos Epson benchmarker vi vores sikkerhed på globalt plan. Vi opfylder ISO/IEC 15408[3], også kaldet Common Criteria (CC), som er en international standard for sikkerhedsforanstaltninger i it-produkter og -systemer, og CCRA-certificering, som viser, at produktet er blevet certificeret i overensstemmelse med Japan Information Technology Security Evaluation and Certification Scheme (JISEC).

Netværkssikkerhed
Med netværkssikkerhed som en vigtig prioritet kan administratorer konfigurere individuelle tilladelser og begrænsninger på en lang række netværksopgaver. Med vores WorkForce Enterprise 2-printere kan administratorer også filtrere IP-adresser, servicetyper, modtagelses- og transmissionsportnumre ved hjælp af funktionen IP Sec/IP-filtrering. Samtidig beslutter du, om du vil acceptere eller blokere specifikke IP-adresser. Vi understøtter også SNMPv3 e-mailkryptering og TLS1.3.

Beskyttelse af din All-in-One-printer
For at få ekstra beskyttelse af dine printere kan du vælge at blokere adgangen fra en computer via USB og deaktivere hukommelseskortet og USB-hukommelsesgrænsefladerne. Du kan også bruge vandmærkning med kopibeskyttelse[5] til at forhindre uautoriseret duplikering af originale dokumenter og PDF-kryptering[5] for at sikre, at digitale dokumenter forbliver sikre.

Sikker udskrivning/scanning
Indstillingen "Fortroligt job" betyder at du kan beskytte dine dokumenter fra at blive set af andre. Løsningen betyder at du på printeren skal indtaste en selvvalgt kode for at dit dokument bliver printet.

WPA3
Epsons nyeste MFP'er understøtter WPA3[5], som er den nyeste godkendelses- og krypteringsteknologi til WiFi (trådløst LAN), hvilket giver virksomheder en mere robust og stærkere beskyttelse af deres data via det trådløse netværk.

Dokumentbeskyttelse
Øg produktiviteten, og overvåg brugen med sikker print, scanning og kopiering gennem brugergodkendelse.

Adgangskontrol
Brugergodkendelse og funktionsbegrænsninger.

Beskyttelse af enheden
Bekræftelse af firmwaresignatur, sikker opstart og registrering af indtrængen af malware-runtime.

Manipuleringssikkert blæk
Vores DURABrite™ Pro-blæk trænger godt ind i papirets fibre, hvilket beskytter vigtige dokumenter mod manipulation og er i overensstemmelse med ISO 11798:2023.

Beskyttelse af brugerdata

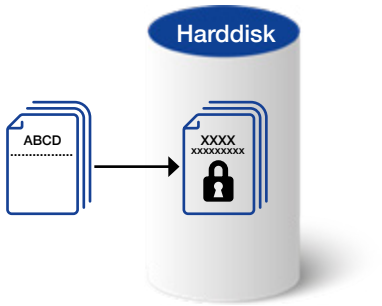
Du kan også indstille unikke adgangskoder til delte felter[5], dokumenter og adressebøger på dine Epson printere. Af hensyn til fuldstændig sikkerhed ryddes data fra printeren, når opgaverne er fuldført, eller strømmen er slukket. Hvis enheden har en harddisk, krypteres alle data, og data slettes efter hvert printjob. For at få ekstra beskyttelse kan administratoren også overskrive harddisken.
Læs mere i vores sikkerhedsguidebog.

Databeskyttelse

HDD-kryptering, sletning af sikre data i HDD, Trusted Platform Module (TPM) og adgangskodekryptering.

Kryptering af gemte data i HDD

Vi beskytter altid kundedata med kryptering, når vi gemmer data på en intern HDD på en alt-i-en-printer. Kryptering af dataene forhindrer uautoriseret adgang eller ondsindet angreb på personlige data, hvis HDD'en bliver stjålet. HDD leveres med et selvkrypterende drev, og dokumentdataene krypteres med AES-256.

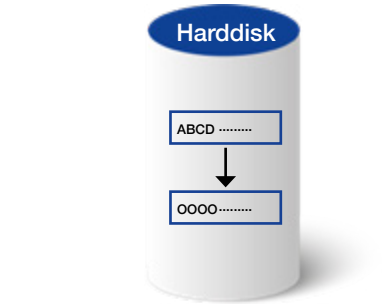


Sekventiel sletning af jobdata

Når den er aktiveret, overskrives de slettede data på harddisk[5] på følgende måder for at forhindre gendannelse. Der er flere muligheder:

1. Hurtig sletning: Krypteringsnøglen ændres for at forhindre, at slettede data gendannes.
2. Sikker sekventiel sletning: Krypteringsnøglen ændres, og de slettede data på harddisken overskrives med "0'er" for yderligere at sikre, at de slettede data ikke kan gendannes.

For en detaljeret forklaring på sletning af jobdata, henvises der til produktets brugervejledning.

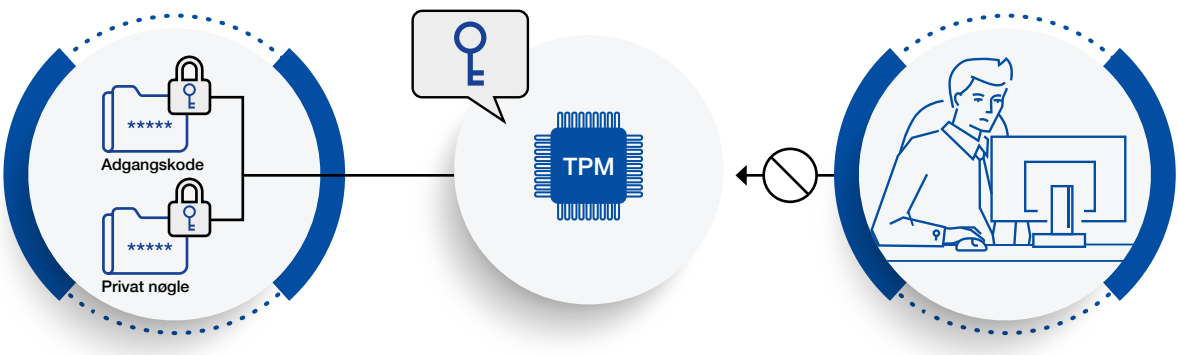


TPM

I modeller med TPM (Trusted Platform Module) forbedres sikkerhedsniveauet som følger:

- Krypteringsnøglerne til gendannelse af krypterede adgangskoder og private nøgleoplysninger gemmes på TPM-chippen.
- TPM-chippen kan beskyttes mod uautoriseret analyse på hardwareniveau, da der ikke kan opnås adgang til TPM-chippen uden for printeren.
- TMP'ernes sande tilfældige tal bruges som sessionsnøgler til kommunikation med browseren (Web Config).
- TMP'ernes ægte tilfældige tal bruges til at generere godkendelsesnøgler til den krypterede harddisk.

Multifunktionsprinterne har en TPM 2.0-chip.



	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
Netværkssikkerhed			
TLS-kommunikation	✔	✔	✔
TLS1.1, TLS1.2, TLS1.3	✔	✔	✔
Kontrol af protokoltilladelser og -eksklusioner	✔	✔	✔
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-godkendelse	✔	✔	✔
EAP-TLS, PEAP-TLS	✔	✔	✔
PEAP/MSCHAPv2	✔	✔	✔
EAP-TTLS	✔	✔	✔
AES128/AES256/3DES/RC4	✔	✔	✔
SNMPv3	✔	✔	✔
WPA3	✔	✔	✔
Adskillelse mellem grænseflader	✔	✔	✔
Beskyttelse af din All-in-One-printer			
Bloker USB-forbindelse fra computer	✔	✔	✔
Deaktivering af det eksterne interface	✔	✔	✔
Håndtering af virus indført via USB-hukommelse	✔	✔	✔
Print-/scanningssikkerhed			
Fortrolige jobs	✔*6	✔	✔
Antikopieringsmønster[6]	✔	✔	✔
Vandmærke[6]	✔	✔	✔
PDF-kryptering	✔	✔	✔
S/MIME	✔	✔	✔
AES-128/AES-192/AES-256/3DES	✔	✔	✔
SHA-1/SHA-256/SHA-384/SHA-512/MD5	✔	✔	✔
Domænebegrænsninger	✔*7	✔	✔
Autorisationsadgangskode til scanning til netværksmappe/FTP, scanning til e-mail og e-mail besked	–	✔ *7	✔
Understøttelse af lange godkendelsesadgangskoder	–	–	✔ *8
Standard deaktivering af filadgang fra PDL	✔*7	✔	✔
Sikker udskrivning	✔	✔	✔
Faxsikkerhed[9]			
Restriktioner for direkte opkald	✔	✔	✔
Bekræftelse af adresseliste	✔	✔	✔
Genkendelse af ringetone	✔	✔	✔
Foranstaltninger mod efterladte fax	✔	✔	✔
Bekræftelsesrapport for transmission	✔	✔	✔
Sletning af backup-data for modtagne fax	✔	✔	✔
Begræns afsendelse til flere modtagere	✔	✔	✔
Printersikkerhed			
Automatiske firmwareopdateringer	✔	✔	✔
Beskyttelse mod ulovlige firmwareopdateringer	–	✔	✔
Sikker opstart	–	✔	✔
Registrering af malware-infiltration	✔*7	✔	✔
Sikkerhedsforanstaltninger, når du bortskaffer printeren			
Gendan fabriksstandard	✔	✔	✔
Sikkerhedscertificering og -standarder			
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
Sikkerhedsfunktioner gennem kompatibilitet med tredjepartssoftware			
Åben platformkompatibel model	✔	✔	✔
Epson Print Admin Serverless (EPAS)			
Brugergodkendelse via ID-kort/loginoplysninger/pinkode	✔	✔	✔
Fuld kontrol over enheders handlinger pr. person	✔	✔	✔
Tilpasning af MFP-menu	✔	✔	✔
Pull-print og direkte print	✔	✔	✔
Scan og send til mig (e-mail, mappe)	✔	✔	✔
Scan til cloud-tjenester (OneDrive for Business, SharePoint online, Google Drive)[10]	✔	✔	✔
Scan til adgangskodebeskyttede PDF-filer	✔	✔	✔
Avancerede indstillinger for scanningsarbejdsgange[11]	✔	✔	✔
Print fra Cloud Services (OneDrive for Business, SharePoint On-line og Teams) uden brug af driver[10]	✔	✔	✔
Synkronisering med mappetjeneste (LDAP, åben LDAP, Microsoft EntraID, Microsoft Entra DS, Google sikker LDAP og Google Cloud-mappe)[10]	✔	✔	✔
Rapporter - Brugerbeskyttelsesindstilling - Skjul filnavn	✔	✔	✔
Politik for adgangskode, kontospærring[11]	✔	✔	✔
Printregler og -politikker[11]	✔	✔	✔
Sporing og rapportering	✔	✔	✔
Quota[10]	✔	✔	✔
Sikker mobil print (AirPrint og Mopria)[12]	–	✔	✔
Beskyttelse af brugerdata			
Bokssikkerhed	✔	✔	✔
Beskyttelse af din adressebog	✔	✔	✔
Datahåndtering behandlet af en all-in-one-printer	✔	✔	✔
Kryptering af gemte data i harddisk	✔	✔	✔
Sekventiel sletning af jobdata	✔	✔	✔
Kryptering af adgangskode	✔	✔	✔
TPM	✔*13	✔	✔
Spejling af harddisken	–	✔	–
Driftsmæssig begrænsning			
Panellås	✔	✔	✔
Adgangskontrol	✔	✔	✔
Godkendt print/scanning[8]	✔	✔	✔
Politik for adgangskode	✔	✔	✔
Overvågningslogfil	✔	✔	✔

Kontakt din Epson salgsrepræsentant, hvis du vil have flere oplysninger.

Navn:

Telefon:

Mail:

1. Print Security Landscape, 2025 - Identitet, AI og Quantum: Navigating the New Threat Landscape', Quocirca, July 2025.
2. Keypoint Intelligence Security Validation Testing Seal 2024-2026 gælder for AM-C400 og AM-C550.
3. ISO/IEC 15408 leveres ikke med standardkonfiguration. Speciel firmware og særlig opsætningsproces påkrævet.
4. CCRA-certificeringslogoet viser, at produktet blev evalueret og certificeret i overensstemmelse med Japan Information Technology Security Evaluation and Certification Scheme (JISEC). Det indebærer ikke nogen garanti for, at produktet er helt fri for sårbarheder. Det betyder heller ikke, at produktet er udstyret med alle nødvendige sikkerhedsfunktioner under alle driftsmiljøer.
5. Du kan finde en komplet liste over modelspecifikationer på support.epson.net/security/en
6. Understøtter kun Windows-printerdriveren.
7. For at bruge denne funktion skal du opdatere printerfirmwaren til den nyeste version.
8. Kræver godkendt printmetode.
9. Kun tilgængelig efter installation af faxboard.
10. Gælder for Epson Print Admin og kun for specifikke produkter på Epson Print Admin Serverless.
11. Gælder kun for Epson Print Admin.
12. Gælder kun for Epson Print Admin Serverless.
13. Understøttes muligvis ikke afhængigt af region. Kontakt dit lokale salgskontor for at få oplysninger om tilgængelighed i dit land.

Genbrug ansvarligt

Epson Danmark
Tlf.: 44 50 85 85
Hotline: 32 72 92 10
www.epson.dk/contactus

Epson Danmark
Vibeholms Allé 15
2605 Brøndby

@EpsonDenmark
epson-denmark

A21406-da-DK 10/25

EPSON®