Epsons sikkerhedsløsninger

Sikkerhedsløsninger til professionel billedbehandling

WorkForce Enterprise 2
og AM-C-serie

EPSON®

Beskyt netværkssikkerheden, uanset hvor udskrivningen sker

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

Stigningen af hjemmearbejde og hybridarbejde har øget denne risiko. En undersøgelse foretaget af Quocirca[1] viste, at mens 70% af it-beslutningstagere mener, at udskrivning er kritisk eller meget vigtig for deres virksomhed, er 31% bekymret over de sikkerhedsrisici, der er forbundet med fjernudskrivning/ hjemmeprint, og kun 19% føler sig helt sikre på, at deres infrastruktur for print er sikker.

Når de gennemsnitlige omkostninger ved et printrelateret databrud er på kr. 6.449.000*, er det ikke noget, du har råd til at tage let på.

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

70%

af it-beslutningstagere mener, at udskrivning er afgørende eller meget vigtig for deres forretning

31%

er bekymret over de sikkerhedsrisici, der er forbundet med fjernudskrivning/ hjemmeprint

19%

føler sig helt sikre på, at deres infrastruktur for print er sikker

* Baseret på £ 743.000 som citeret af Quocirca og konverteret til kr. 6.449.000 med FX-pris fra xe.com pr. 09/01/2024.

Epsons tilgang til sikkerhed

Styrkelse af dine enheders netværksfunktioner er nøglen til vores tilgang til sikkerhed. For at sikre sikkerheden for Epsons enheder i hele deres livscyklus, bygger Epson WorkForce 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

Sikkerhedsfunktioner designet til dig

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.

Sikker udskrivning og scanning

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

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

På enhed

Med Epson Device Admin bliver det nemmere at administrere sikkerhed, indstillinger og lignende på jeres netværks-opkoblede Epson enheder. Ved hjælp af et intuitivt interface er det muligt at overvåge, implementere og opsætte alarmer og rapporter.

Sikker kommunikation

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

PDF-beskyttelse

Tilføj adgangskode-beskyttelsesfunktionalitet[3] til scannede PDF-filer for at beskytte mod uautoriserede fremvisere 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 bruger-ID og din adgangskode, LDAP-Active Directory, login med ID-kort og pinkode.

Besøg **www.epson.eu/bi-security-solutions**
for yderligere oplysninger om tilgængelige løsninger

Sikkerhed anerkendt i 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).

4

5

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 antikopi vandmærkning[2] til at forhindre uautoriseret duplikering af originale dokumenter og PDF-kryptering[2] 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[2], 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
Godkendelsesbeskyttet print scan og joblog.

Adgangskontrol
Brugergodkendelse og funktionsbegrænsninger.

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

Beskyttelse af brugerdata

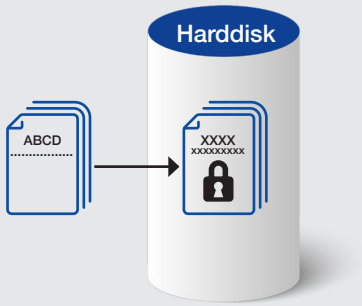
Du kan også indstille unikke adgangskoder til delte felter[2], dokumenter og adressebøger på dine Epson printere. Af hensyn til fuldstændig sikkerhed ryddes data fra printeren, når opgaverne er fuldført, eller strømmen er slukket. Hvis enheden har en harddisk, krypteres alle data, og data slettes efter hvert printjob. For at få ekstra beskyttelse kan administratoren også overskrive harddisken.
Læs mere i vores sikkerhedsvejledning på **epson.eu/bi-security-solutions**

Databeskyttelse

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

Kryptering af gemt data i HDD

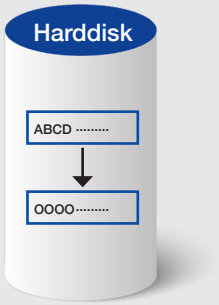
Vi beskytter altid kundedata med kryptering, når vi gemmer data på en intern HDD på en alt-i-en-printer. Kryptering af dataene forhindrer uautoriseret adgang eller ondsindet angreb på personlige data, hvis HDD'en bliver stjålet. HDD leveres med et selvkrypterende drev, og dokumentdataene krypteres med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



Sekventiel sletning af jobdata

Når den er aktiveret, overskrives de slettede data på harddisken[2] 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.



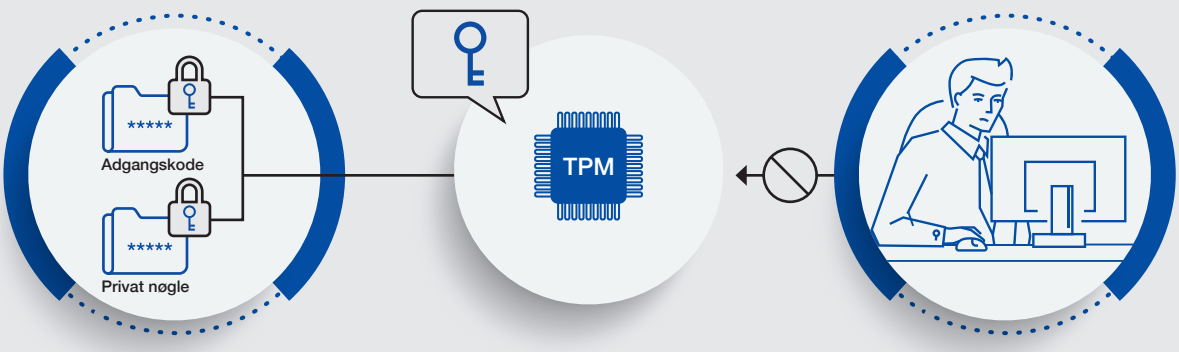
For en detaljeret forklaring på sletning af jobdata, henvises der til produktets brugervejledning.

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 uvilkårlige tal bruges som sessionsnøgler til kommunikation med browseren (Web Config).
- TMP'ernes uvilkårlige tal bruges til at generere godkendelsesnøgler til den krypterede harddisk.

All-in-One-printeren har en TPM 2.0-chip.



	WorkForce Enterprise			AM-C		
Produktnavn	**WF-C21000**	**WF-C20600**	**WF-C20750**	**AM-C6000**	**AM-C5000**	**AM-C4000**
Type	A3	A3	A3	A3	A3	A3
Netværkssikkerhed						
TLS-kommunikation	✔	✔	✔	✔	✔	✔
TLS1.1	✔	✔	✔	✔	✔	✔
TLS1.2	✔	✔	✔	✔	✔	✔
TLS1.3	✔*1	✔*1	✔*1	✔	✔	✔
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	✔*2	✔*2	✔*2	✔	✔	✔
Antikopieringsmønster	✔*2	✔*2	✔*2	✔*2	✔*2	✔*2
Vandmærke	✔*2	✔*2	✔*2	✔*2	✔*2	✔*2
PDF-kryptering	✔	✔	✔	✔	✔	✔
S/MIME	✔	✔	✔	✔	✔	✔
AES-128/AES-192/AES-256/3DES	✔	✔	✔	✔	✔	✔
SHA-1/SHA-256/SHA-384/SHA-512/MD5	✔	✔	✔	✔	✔	✔
Faxsikkerhed	✔	✔	✔	✔	✔	✔
Faxsikkerhed						
Domænebegrænsninger	✔*1	✔*1	✔*1	✔	✔	✔
Autorisationsadgangskode til scanning til netværksmappe/FTP, scanning til e-mail og e-mail besked	–	–	–	✔*1	✔*1	✔*1
Sikker print	✔	✔	✔	✔	✔	✔
Standard deaktivering af filadgang fra PDL	✔*1	✔*1	✔*1	✔	✔	✔
Restriktioner for direkte opkald	✔*3	✔*3	✔*3	✔*3	✔*3	✔*3
Bekræftelse af adresseliste	✔*3	✔*3	✔*3	✔*3	✔*3	✔*3
Genkendelse af ringetone	✔*3	✔*3	✔*3	✔*3	✔*3	✔*3
Foranstaltninger mod forladte fax	✔*3	✔*3	✔*3	✔*3	✔*3	✔*3
Bekræftelsesrapport for transmission	✔*3	✔*3	✔*3	✔*3	✔*3	✔*3
Sletning af backup-data for modtagne fax	✔*3	✔*3	✔*3	✔*3	✔*3	✔*3
Begræns afsendelse til flere modtagere	✔*3	✔*3	✔*3	✔*3	✔*3	✔*3

*1. For at bruge denne funktion skal du opdatere printerfirmwaren til den nyeste version.
*2. Understøtter kun Windows-printerdriveren.
*3. Kun tilgængelig efter installation af faxboard.

	WorkForce Enterprise			AM-C		
Produktnavn	WF-C21000	WF-C20600	WF-C20750	AM-C6000	AM-C5000	AM-C4000
Type	A3	A3	A3	A3	A3	A3
Sikkerhedsfunktioner gennem kompatibilitet med tredjepartssoftware						
Åben platformkompatibel model	✔	✔	✔	✔	✔	✔
Epson Print Admin						
Quota, printregler og -politikker	✔	✔	✔	✔	✔	✔
Brugergodkendelse via ID-kort/loginoplysninger/pinkode	✔	✔	✔	✔	✔	✔
Adgang til de funktioner, der er tildelt rollen eller afdelingen	✔	✔	✔	✔	✔	✔
Personliggørelse af MFP-menu pr. gruppe eller person	✔	✔	✔	✔	✔	✔
Pull-print	✔	✔	✔	✔	✔	✔
Direkte print	✔	✔	✔	✔	✔	✔
Scan og send til mig (e-mail, mappe)	✔	✔	✔	✔	✔	✔
Scan til cloud-tjenester (OneDrive for Business, SharePoint online, Google Drive)	✔	✔	✔	✔	✔	✔
Avancerede indstillinger for scanningsarbejdsgange	✔	✔	✔	✔	✔	✔
Synkronisering med mappetjeneste (LDAP, åben LDAP, Azure AD, Azure AD DS, Google Secure LDAP og Google Cloud-bibliotek)	✔	✔	✔	✔	✔	✔
Scan til adgangskodebeskyttede PDF-filer	✔	✔	✔	✔	✔	✔
Epson Print Admin Serverless						
Brugergodkendelse via ID-kort/loginoplysninger/pinkode	✔	✔	✔	✔	✔	✔
Fuld kontrol over enheders handlinger pr. person	✔	✔	✔	✔	✔	✔
Pull-print	✔	✔	✔	✔	✔	✔
Direkte print	✔	✔	✔	✔	✔	✔
Scan og send til mig (e-mail, mappe)	✔	✔	✔	✔	✔	✔
Sporing og rapportering	✔	✔	✔	✔	✔	✔
Synkronisering med Directory Service (LDAP og Open LDAP)	✔	✔	✔	✔	✔	✔
Support til printkvote	✔	✔	✔	✔	✔	✔
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	✔*4	✔*4	✔*4	✔	✔	✔
Driftsmæssig begrænsning						
Panellås	✔	✔	✔	✔	✔	✔
Adgangskontrol	✔	✔	✔	✔	✔	✔
Godkendt print	✔*5	✔*5	✔*5	✔*5	✔*5	✔*5
Politik for adgangskode	✔	✔	✔	✔	✔	✔
Overvågningslogfil	✔	✔	✔	✔	✔	✔
Printersikkerhed						
Automatiske firmwareopdateringer	✔	✔	✔	✔	✔	✔
Sikkerhedsforanstaltninger, når du bortskaffer printeren						
Gendan fabriksstandard	✔	✔	✔	✔	✔	✔
Sikkerhedscertificering og -standarder						
ISO15408/IEEE2600.2™	✔	✔	✔	✔*6	✔*6	✔*6

*4. Understøttes muligvis ikke, afhængigt af land. Kontakt dit lokale salgskontor for at få oplysninger om tilgængelighed i dit land.
*5. Kræver godkendt printmetode.
*6. Tilgængeligt i Q4 2023.

Kontakt din Epson sælger, hvis du ønsker flere oplysninger.

Navn:

Telefon:

Mail:

1. "The Print Security Landscape, 2023 - Sikring af printinfrastrukturen midt i et voksende trusselslandskab", Quocirca, maj 2023.
2. Du kan finde en komplet liste over modelspecifikationer på www.epson.eu/bi-security-solutions.
3. ISO/IEC 15408 leveres ikke med standardkonfiguration. Speciel firmware og særlig opsætningsproces påkrævet.
4. Gælder for WorkForce Enterprise 2
5. Gælder for AM-C-serien

Genbrug venligst 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

A13981-brochure-hires-da-DK-business-printing-security-solutions.pdf

EPSON®