

WorkForce Enterprise 2 un AM klāsts

Biroja printeri

Droši risinājumi



EPSON®

Aizsargājiet tīkla drošību neatkarīgi no drukāšanas vietas

Jūsu uzņēmumā ir viegli nepamanīt svarīgus drošības pasākumus, lietojot jebkuras tīkla ierīces. Un, lai gan jūs to neesat apsvēris, daudzfunkciju printeri (MFP), skeneri un jebkura cita savienota vai tīklā savienota ierīce var būt atvērta drošības vājībām.

Mājas un hibrīda darba pieaugums ir palielinājis šo risku. Quocirca¹ pētījumā tika konstatēts, ka ar drukāšanu saistīta drošības pārkāpuma dēļ 56 % organizāciju vismaz vienreiz ir zaudējušas datus, un 83 % plāno palielināt drukāšanas drošības izdevumus nākamajā gadā. Organizāciju galvenās bažas saistītas ar mājas drukāšanas drošības nodrošināšanu (28 %), konfidencialu vai sensitīvu dokumentu aizsardzību

pret nesankcionētu drukāšanu (28 %) un izpratnes radīšanu par drukas infrastruktūras apdraudējumiem un ievainojamību (25 %).

Tā kā ar drukāšanu saistīta datu noplūde vidēji izmaksā 953 000 €*, to nevar uzvert vieglprātīgi.

Tomēr, pateicoties Epson pieejai printeru drošībai, tas ir risks, ko varat mazināt neatkarīgi no tā, kur jūsu uzņēmums drukā.

3 galvenie drukas drošības izaicinājumi

28 %

drukāšanas nodrošināšana attālinātā/mājas vidē

28 %

sensitīvu vai konfidencialu dokumentu aizsardzība pret drukāšanu

25 %

izpratne par mūsu drukas infrastruktūras apdraudējumu un ievainojamību veidiem



* Pamatojoties uz Quocirca norādīto 820 000 £ vērtību, kas konvertēta 953 000 €, izmantojot xe.com valūtas kursu uz 2025. gada 7. jūliju.

Epson drošības paziņojums

Jūsu ierīču tīkla iespēju stiprināšana ir mūsu drošības pieejas pamatā. Lai nodrošinātu Epson ierīču drošību visā to dzīves ciklā, katrs Epson WorkForce printeris ir veidots, pamatojoties uz trim turpmāk minētajiem pamatprincipiem.

1. Produkta drošība ir kvalitātes pamats
2. Informācija un zināšanas par drošību tiek aktīvi koplietotas, lai jūs vienmēr būtu informēti
3. Lai maksimāli palielinātu ierīces aizsardzību, ievainojamības tiek pastāvīgi pārskatītas

Droša uzbūve

Aizsargāti dati un droši tīkli ir Epson daudzfunkcionālo printeru standarts, izmantojot funkcijas, kuras var palīdzēt ievērot Vispārīgo datu aizsardzības regulu (VDAR) un korporatīvo sociālo atbildību (KSA). Šie drošības pasākumi, kuri ir tieši integrēti mūsu produktos, sniedz jums pārliecību, ka jūsu uzņēmums atbilst jūsu drošības prasībām.

Mūsu ierīces ir neatkarīgi testētas un drošības validāciju veic Keypoint Intelligence. Epson patentētā printeru/skenēru SoC un programmaparatūras platformas tehnoloģija aizsargā klientu informāciju un produktus no drošības apdraudējumiem.



Droša drukāšana un skenēšana

Nodrošiniet dokumentu privātumu un neļaujiēt nepilnvarotām personām skatīt bez uzraudzības atstātu izdruku ierīcē, iesniedzot dokumentus kā "Konfidencialu darbu" no printera draivera.

Piekļuvi ierīces funkcijām var ierobežot, izmantojot priekšējā paneļa bloķēšanas funkciju.

Droša saziņa

Filtrējiet IP adreses, pakalpojumus, uztveršanas un pārraides portu numurus, kuriem ir piekļuve Epson ierīcēm. Varat arī šifrēt visu tīkla saziņu, izmantojot IPSec funkciju.

Ierīcē

Izmantojot Epson Device Admin (EDA), ierīces drošības pārvaldība kļūst vienkāršāka. Tā ir saderīga ar plašu mūsu tīkla printeru klāstu un ļauj lietotājiem visu kontrolēt, izmantojot viedu un intuitīvu saskarni.

PDF aizsardzība

Pievienojiet paroli aizsardzības funkcionalitāti³ skenētajiem PDF failiem, lai aizsargātu tos pret neatļautiem skatītājiem un novērstu dokumentu rediģēšanu un drukāšanu.

Dokumentu apstrāde un datu pārvaldība

Centralizēti pārvaldiet vairākus uzdevumus, sākot no skenēšanas uzdevumu profiliem līdz lietotāju piekļuves tiesībām. Administratori var centralizēti pārvaldīt dažādus uzdevumus, sākot no skenēšanas uzdevumu profiliem līdz lietotāju piekļuves tiesībām. IT administratoriem ir iespēja kontrolēt piekļuves tiesības uzdevumiem vairākos veidos, tostarp ar ID kartēm, pieteikšanās vārdiem/parolēm un PIN kodiem.

Nemanāma integrācija IT infrastruktūrā ar lokālo lietotāju datu bāzi vai direktoriju pakalpojumiem, piemēram, Microsoft EntraID un Google Cloud Directory.

Lai iegūtu papildinformāciju par Epson drošību vai risinājumiem, lūdzu, skenējiet kodus vai apmeklējiet tālāk norādītās saites.

Epson
Solutions Suite



[Epson risinājumu komplekts](#)



[Produktu drošība](#)

Drošība, kas atzīta visā pasaulē

Uzņēmumā Epson mēs augstu vērtējam savu drošību globālā mērogā. Mēs ievērojam atbilstību standartam ISO/IEC 15408³, ko sauc arī par kopējiem kritērijiem (Common Criteria jeb CC), kas ir starptautisks standarts drošības pasākumiem IT produktos un sistēmās, un CCRA sertifikācijai, kas apliecina, ka produkts ir sertificēts saskaņā ar Japānas Informācijas tehnoloģiju drošības novērtēšanas un sertifikācijas shēmu (Japan Information Technology Security Evaluation and Certification Scheme jeb JISEC).



Tikla drošība

Tā kā tīkla drošība ir galvenā prioritāte, administratori var iestatīt individuālas atļaujas un ierobežojumus plašam tīkla uzdevumu klāstam. Izmantojot mūsu WorkForce Enterprise 2 printerus, administratori var arī filtrēt IP adreses, pakalpojumu veidus, saņemšanas un pārraides portu numurus, izmantojot IP Sec/IP filtrēšanas funkciju. Vienlaikus viņi var izlemt, pieņemt vai bloķēt konkrētas IP adreses. Mēs atbalstām arī SNMPv3 e-pasta šifrēšanu un TLS1.3.



Daudzfunkciju printera aizsardzība

Lai nodrošinātu papildu aizsardzību printeriem, varat izvēlēties bloķēt piekļuvi no datora, izmantojot USB, un atspējot atmiņas kartes un USB atmiņas saskarnes. Varat arī izmantot pretkopēšanas ūdenszīmes⁵, lai novērstu oriģinālo dokumentu neatļautu kopēšanu, un PDF šifrēšanu⁵, nodrošinot digitālo dokumentu drošību.



Droša drukāšana/skenēšana

Opcija "Konfidenciāls darbs" nozīmē, ka varat aizsargāt dokumentu privātumu un novērst nevēlamu neuzraudzītas izvades apskati.



WPA3

Epson jaunākie MFP atbalsta WPA3⁵, kas ir jaunākā autentifikācijas un šifrēšanas tehnoloģija WiFi (bezvadu LAN), nodrošinot uzņēmumiem stabilāku un spēcīgāku datu aizsardzību bezvadu tīklā.



Dokumentu aizsardzība

Uzlabojiet produktivitāti un uzraugiet lietošanu ar drošu drukāšanu, skenēšanu un kopēšanu, izmantojot lietotāja autentifikāciju.



Piekļuves kontrole

Lietotāja autentifikācija un funkciju ierobežojumi.



Ierīces aizsardzība

Programmaparatūras paraksta verifikācija, droša palaišana un jaunprogrammatūras darbības ilguma ielaušanās noteikšana.



Aizsardzība pret viltojumiem

Mūsu DURABrite™ Pro tinte stingri iesūcas papīra šķiedrās, tādējādi aizsargājot svarīgus dokumentus no viltošanas un atbilstot standartam ISO 11798:2023.



Lietotāja datu aizsardzība

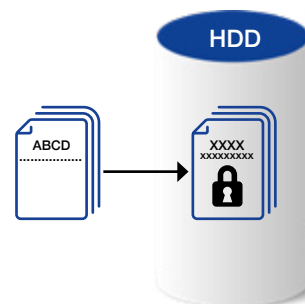
Varat arī iestatīt unikālas paroles koplietojamām pastkastēm⁵, dokumentiem un adrešu grāmatām Epson printeros. Pilnīgai drošībai dati tiek dzēsti no printera pēc darbu pabeigšanas vai izslēgšanas. Ja ierīcei ir cietais disks, visi dati tiek šifrēti un dati tiek dzēsti pēc katra drukas darba. Papildu aizsardzībai administrators var arī pārrakstīt cieto disku. Lasiet vairāk mūsu [drošības rokasgrāmatā](#).

Datu aizsardzība

HDD šifrēšana, HDD droša datu dzēšana, uzticams platformas modulis (TPM – Trusted Platform Module) un parolu šifrēšana.

Saglabāto datu šifrēšana cietajā diskā

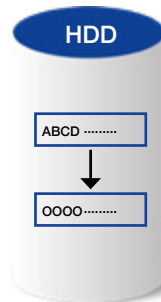
Saglabājot datus iekšējā cietajā diskā daudzfunkcionālā printerī, mēs vienmēr aizsargājam klientu datus ar šifrēšanu. Datu šifrēšana novērš nesankcionētu piekļuvi vai ļaunprātīgu uzbrukumu personiskajai informācijai, ja cietais disks tiek nozagts. Cietajam diskam ir paššifrējošs disks, un dokumentu dati tiek šifrēti ar AES-256.



Darba datu secīga dzēšana

Ja šis iestatījums ir iespējots, izdzēstie dati cietajā diskā⁵ tiek pārrakstīti tālāk norādītajos veidos, lai novērstu atjaunošanu. Ir vairākas iespējas.

1. Ātra dzēšana: šifrēšanas atslēga tiek mainīta, lai novērstu dzēsto datu atjaunošanu.
2. Droša secīga dzēšana: šifrēšanas atslēga tiek mainīta, un izdzēstie dati cietajā diskā tiek pārrakstīti ar "0", lai turpmāk nodrošinātu, ka izdzēstos datus nevar atgūt.



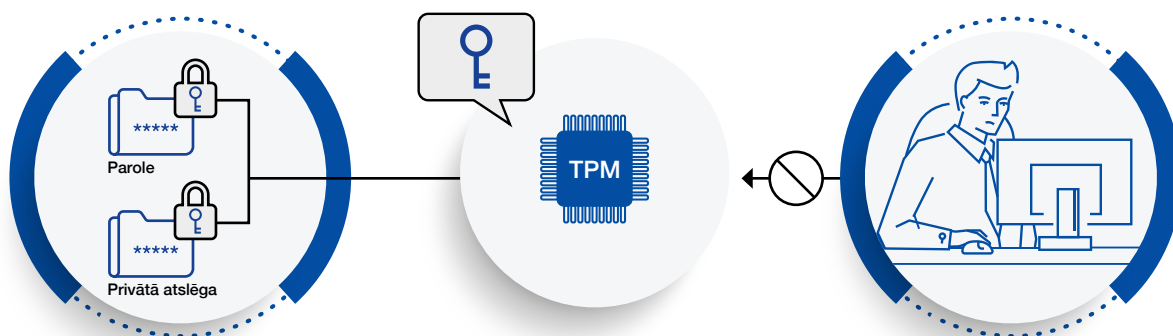
Detalizētu skaidrojumu par darba datu dzēšanu skatiet sava produkta lietotāja rokasgrāmatā.

TPM

Modeļiem ar uzticamas platformas moduli (Trusted Platform Module jeb TPM) drošības līmenis uzlabojas, kā norādīts turpmāk.

- Šifrēšanas atslēgas šifrētu paroli un privātās atslēgas informācijas atjaunošanai tiek glabātas TPM mikroshēmā.
- TPM mikroshēmu var aizsargāt no nesankcionētas analīzes aparatūras līmenī, jo TPM mikroshēmai nevar piekļūt no ārpusē, ārpus printera.
- TPM patiesie nejaušie skaitļi tiek izmantoti kā sesijas atslēgas saziņai ar pārlūkprogrammu (tīmekļa konfigurācija).
- TPM patiesie nejaušie skaitļi tiek izmantoti autentifikācijas atslēgu ģenerēšanai šifrētajam cietajam diskam.

Daudzfunkciju printeriem ir TPM 2.0 mikroshēma.



	WorkForce Enterprise	WorkForce Enterprise AM	
Produkta nosaukums	WF-C21000/C20600/C20750	AM-C4000/C5000/ C6000 un AM-M5500	AM-C400/C550/ C550z
Tips	A3	A3	A4
Tīkla drošība			
TLS saziņa	✓	✓	✓
TLS1.1, TLS1.2, TLS1.3	✓	✓	✓
Protokolu atļauju un izslēgšanas kontrole	✓	✓	✓
IPsec/IP filtrēšana	✓	✓	✓
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 autentifikācija	✓	✓	✓
EAP-TLS, PEAP-TLS	✓	✓	✓
PEAP/MSCHAPv2	✓	✓	✓
EAP-TTLS	✓	✓	✓
AES128/AES256/3DES/RC4	✓	✓	✓
SNMPv3	✓	✓	✓
WPA3	✓	✓	✓
Saskarņu atdalīšana	✓	✓	✓
Daudzfunkciju printera aizsardzība			
USB savienojuma bloķēšana no datora	✓	✓	✓
Ārējās saskarnes atspējošana	✓	✓	✓
USB atmiņas ievadīto vīrusu apstrāde	✓	✓	✓
Drukāšanas/skenēšanas drošība			
Konfidencialitāte darbi	✓ ^{*6}	✓	✓
Pretkopēšanas modelis ⁶	✓	✓	✓
Ūdenszīme ⁶	✓	✓	✓
PDF šifrēšana	✓	✓	✓
S/MIME	✓	✓	✓
AES-128/AES-192/AES-256/3DES	✓	✓	✓
SHA-1/SHA-256/SHA-384/SHA-512/MD5	✓	✓	✓
Domēnu ierobežojumi	✓ ^{*7}	✓	✓
Autorizācijas parole skenēšanai uz tīkla mapi/FTP, skenēšanai uz e-pastu un e-pasta paziņojumiem	–	✓ ^{*7}	✓
Atbalsts garām autentifikācijas parolēm	–	–	✓ ^{*8}
Noklusējuma failu piekļuves atspējošana no PDL	✓ ^{*7}	✓	✓
Droša drukāšana	✓	✓	✓
Faksa drošība⁹			
Tiešās zvanišanas ierobežojumi	✓	✓	✓
Adrešu saraksta apstiprināšana	✓	✓	✓
Zvana toņa noteikšana	✓	✓	✓
Pasākumi pret atmestiem faksiem	✓	✓	✓
Pārbaudes apstiprinājuma ziņojums	✓	✓	✓
Saņemto faksu dublējuma datu dzēšana	✓	✓	✓
Sūtīšanas ierobežošana vairākiem adresātiem	✓	✓	✓
Printera drošība			
Automātiski programmaparatūras atjauninājumi	✓	✓	✓
Aizsardzība pret nelegāliem programmaparatūras atjauninājumiem	–	✓	✓
Droša sāknēšana	–	✓	✓
Ļaunprogrammatūras infiltrācijas noteikšana	✓ ^{*7}	✓	✓
Drošības pasākumi, izmantojot printeri			
Rūpnīcas noklusējuma iestatījumu atjaunošana	✓	✓	✓
Drošības sertifikācija un standarti			
ISO15408/IEEE2600.2™	✓	✓	✓

	WorkForce Enterprise	WorkForce Enterprise AM	
Produkta nosaukums	WF-C21000/C20600/C20750	AM-C4000/C5000/ C6000 un AM-M5500	AM-C400/C550/ C550z
Tips	A3	A3	A4
Drošības funkcijas, pateicoties saderībai ar trešo personu programmatūru			
Ar atvērto platformu saderīgs modelis	✓	✓	✓
Epson Print Admin (EPA) / EPA Serverless			
Lietotāja autentifikācija, izmantojot ID kartes/pieteikšanās datus/ PIN kodu	✓	✓	✓
Pilnīga ierīces darbību kontrole katram lietotājam	✓	✓	✓
MFP izvēlnes personalizēšana	✓	✓	✓
Drukāšana pēc pieprasījuma un tiešā drukāšana	✓	✓	✓
Skenēšana un nosūtīšana man (e-pasts, mape)	✓	✓	✓
Skenēšana uz mākoņpakalpojumiem (OneDrive for Business, SharePoint Online, Teams un Google Drive) ¹⁰	✓	✓	✓
Skenēšana uz ar paroli aizsargātiem PDF failiem	✓	✓	✓
Uzlaboti skenēšanas darbplūsmas iestatījumi ¹¹	✓	✓	✓
Drukāšana bez draivera no mākoņpakalpojumiem (OneDrive darbam, SharePoint Online un Teams) ¹⁰	✓	✓	✓
Sinhronizācija ar direktoriju pakalpojumu (LDAP, Open LDAP, Microsoft EntraID, Microsoft Entra DS, Google secure LDAP un Google Cloud directory) ¹⁰	✓	✓	✓
Atskaites – lietotāja aizsardzības iestatījums – faila nosaukuma slēpšana	✓	✓	✓
Paroles politika, konta bloķēšana ¹¹	✓	✓	✓
Drukāšanas noteikumi un politikas ¹¹	✓	✓	✓
Izsekošana un ziņošana	✓	✓	✓
Kvota ¹⁰	✓	✓	✓
Droša mobilā drukāšana (AirPrint un Mopria) ¹²	–	✓	✓
Lietotāja datu aizsardzība			
Pastkastes drošība	✓	✓	✓
Jūsu adrešu grāmatas aizsardzība	✓	✓	✓
Daudzfunkcionālā printera apstrādātā datu apstrāde	✓	✓	✓
Saglabāto datu šifrēšana cietajā diskā	✓	✓	✓
Darba datu secīga dzēšana	✓	✓	✓
Paroles šifrēšana	✓	✓	✓
TPM	✓ ^{*13}	✓	✓
Cietā diska spoguļošana	–	✓	–
Darbības ierobežojumi			
Paneļa bloķēšana	✓	✓	✓
Piekļuves kontrole	✓	✓	✓
Autentificēta drukāšana/skenēšana ⁸	✓	✓	✓
Paroles politika	✓	✓	✓
Audita žurnāls	✓	✓	✓

Lai iegūtu plašāku informāciju, sazinieties ar savu Epson pārdošanas pārstāvi.

Vārds:

Tālrunis:

E-pasta
adrese:

1. Print Security Landscape, 2025 - Identity, AI, and Quantum: Navigating the New Threat Landscape', Quocirca, July 2025.
2. Keypoint Intelligence drošības validācijas testēšanas ziņojums 2024.–2026. gadam attiecas uz AM-C400 un AM-C550.
3. ISO/IEC 15408 nav standarta konfigurācijas. Nepieciešama īpaša programmaparatūra un īpaši iestatīšanas process.
4. CCRA sertifikācijas logotips norāda, ka produkts ir novērtēts un sertificēts saskaņā ar Japānas Informācijas tehnoloģiju drošības novērtēšanas un sertifikācijas shēmu (Japan Information Technology Security Evaluation and Certification Scheme jeb JISEC). Tas negarantē, ka produkts ir pilnībā brīvs no ievainojamībām. Tas arī nenozīmē, ka produkts ir aprīkots ar visām nepieciešamajām drošības funkcijām katrā darbības vidē.
5. Pilnu modeļa specifikāciju sarakstu skatiet vietnē support.epson.net/security/en
6. Atbalsta tikai Windows printera draiveri.
7. Lai izmantotu šo funkciju, atjauniniet printera programmaparatūru uz jaunāko versiju.
8. Nepieciešama autentificēta drukāšanas metode.
9. Pieejams tikai tad, ja ir uzstādīta izvēles faksa plate.
10. Attiecas uz Epson Print Admin un tikai uz noteiktiem produktiem, kas darbojas ar Epson Print Admin Serverless.
11. Attiecas tikai uz Epson Print Admin.
12. Attiecas tikai uz Epson Print Admin Serverless.
13. Var netikt atbalstīts atkarībā no reģiona. Lūdzu, sazinieties ar vietējo pārdošanas biroju, lai uzzinātu par pieejamību jūsu valstī.



Lūdzu, utilizējiet atbildīgi

Epson Europe B.V.
Azle Building,
Atlas Arena Amsterdam
Hoogoordreed 5

www.epson.eu/contact-us



@Epson.baltics
Epson Baltics

Preču zīmes un reģistrētās preču zīmes pieder Seiko Epson Corporation vai tās attiecīgajiem īpašniekiem.
Informācija par produktiem var tikt mainīta bez iepriekšēja paziņojuma.

EPSON®