

WorkForce Enterprise 2- ja AM-mallisto

Yritystulostimet

Turvalliset ratkaisut



EPSON®

Suojaa verkon turvallisuus missä tahansa tulostatkin

Verkossa oleviin yrityksesi laitteisiin liittyvät tärkeät tietoturvatimet on helppo jättää huomiotta. Ja vaikket et ehkä ole ajatellut sitä, monitoimitulostimet, skannerit ja muut yhdistetyt tai verkossa olevat laitteet voivat altistaa tietoturvauhille.

Etä- ja hybridityöskentelyn lisääntyminen on lisännyt tätä riskiä. Quocircan¹ tutkimuksessa havaittiin, että 56 % organisaatioista oli kärsinyt vähintään yhden tietojen menetyksen tulostukseen liittyvän tietoturvarikkomuksen vuoksi. 83 % organisaatioista odotti tulostusturvallisuuden kustannusten kasvavan tulevan vuoden aikana. Organisaatioiden suurimmat huolenaiheet ovat kotitulostuksen suojaaminen (28 %), luottamuksellisten tai

arkaluonteisten asiakirjojen suojaaminen tulostamiselta (28 %) sekä tulostusjärjestelmän uhka- ja haavoittuvuustyyppien ymmärtäminen (25 %).

Tulostukseen liittyvien tietoturvarikkomusten keskimääräiset kustannukset ovat 953 000 €* , joten asiaan ei kannata suhtautua kevyesti.

Epsonin tulostinturvallisuuteen panostavan lähestymistavan ansiosta kyseinen riski on kuitenkin mahdollista minimoida riippumatta siitä, missä yrityksesi tulostaminen tapahtuu.

Kolme suurinta tulostusturvallisuuteen liittyvää haastetta

28 %

Tulostuksen suojaaminen etä-/kotiympäristössä

28 %

Arkaluonteisten tai luottamuksellisten asiakirjojen suojaaminen tulostamiselta

25 %

Tulostusjärjestelmämme uhka- ja haavoittuvuustyyppien ymmärtäminen



* Perustuu Quocircan mainitsemaan 820 000 puntaan (~953 000 euroa käyttäen xe.comin valuuttakurssia 7.7.2025).

Epsonin turvallisuusperiaatteet

Laitteiden verkko-ominaisuuksien vahvistaminen on tietoturvaa koskevassa lähestymistavassamme keskeisellä sijalla. Epsonin laitteiden tietoturvan varmistamiseksi niiden elinkaaren aikana jokaisen Epson WorkForce -tulostimen toiminta perustuu kolmeen keskeiseen periaatteeseen:

1. Laadun perustana on tuoteturvallisuus.
2. Tietoturvaa koskevia tietoja jaetaan aktiivisesti, jotta olet aina ajan tasalla.
3. Haavoittuvuuksia arvioidaan ja korjataan jatkuvasti laitteen mahdollisimman tehokkaan suojauksen varmistamiseksi.

Turvallisuus sisäänrakennettuna

Epsonin monitoimitulostimissa tietosuoja ja verkkojen turvallisuus ovat vakiona, ja niiden ominaisuudet helpottavat yleisen tietosuoja-asetuksen (GDPR) sekä yritysvastuuvaatimusten (CSR) noudattamista. Nämä suoraan tuotteisiimme integroidut turvatoimet antavat sinulle varmuuden siitä, että yrityksesi täyttää tietosuojavaatimukset.

Keypoint Intelligence on riippumattomasti testannut laitteemme ja varmistanut niiden turvallisuuden. Epsonin oma tulostin- ja skannerialustateknologia (SoC ja laiteohjelmisto) suojaa asiakastietoja ja tuotteita turvallisuushiltiltä.



Suojattu tulostus ja skannaus

Varmista asiakirjosi yksityisyys ja estä luvattomia henkilöitä näkemästä laitteelle jääneitä tulosteita lähettämällä asiakirjat tulostusajurista "Luottamuksellinen työ"-tilassa.

Pääsyä laitteen toimintoihin voidaan rajoittaa etupaneelin lukituksen avulla.

Suojattu viestintä

Suodata Epsonin laitteita käyttävät IP-osoitteet, palvelut sekä vastaanottavien ja lähettävien porttien numerot. IPSec-toiminnolla voit myös salata verkon kaiken tietoliikenteen.

Laitteessa

Epson Device Admin (EDA) helpottaa laitteen tietoturvan hallintaa. Ohjelmisto on yhteensopiva monien verkkoyhteydellä varustettujen tulostimien kanssa, ja sillä voi hallita kaikkea älykkään ja helpokäyttöisen käyttöliittymän kautta.

PDF-tiedostojen suojaus

Lisää skannattuihin PDF-tiedostoihin salanasuojauks³, jolla voit estää luvattoman katselun sekä asiakirjojen muokkauksen ja tulostuksen.

Asiakirjojen käsittely ja tiedonhallinta

Hallitse keskitetysti useita tehtäviä aina skannaustöiden profiileista käyttäjien käyttöoikeuksiin. Järjestelmänvalvojat voivat hallita keskitetysti useita tehtäviä, aina skannaustöiden profiileista käyttäjien käyttöoikeuksiin. IT-järjestelmänvalvojat voivat hallita töiden käyttöoikeuksia monella eri tavalla, muun muassa henkilökorttiin perustuvalla kirjautumisella, käyttäjätunnuksella/salasanalla tai PIN-koodilla.

Saumaton integrointi IT-infrastruktuuriin paikallisen käyttäjätietokannan tai hakemistopalveluiden, kuten Microsoft EntraID:n ja Google Cloud Directoryn, kanssa.

Lisätietoja Epsonin tietosuojasta tai ratkaisuksista saat skannaamalla koodit tai klikkaamalla alla olevia linkkejä.

Epson
Solutions Suite



[Epson Solutions Suite](#)



[Tuoteturvallisuus](#)

Turvallisuus, joka tunnetaan ympäri maailmaa

Epsonilla me vertaamme ja arvioimme tietoturvaamme maailmanlaajuisesti. Täytämme ISO/IEC 15408³ -standardin, jota kutsutaan myös Common Criteria (CC) -standardiksi ja joka on kansainvälinen standardi IT-tuotteiden ja -järjestelmien tietoturvallisuuden arvioinnille. Lisäksi meillä on CCRA-sertifiointi, joka osoittaa, että tuote on sertifioitu Japanin tietotekniikan turvallisuuden arviointi- ja sertifiointijärjestelmän (JISEC) mukaisesti.



Verkon suojaus

Koska verkon turvallisuus on ensisijainen prioriteetti, ylläpitäjät voivat määrittää yksilölliset käyttöoikeudet ja rajoitukset monenlaisiin verkkotoimintoihin. WorkForce Enterprise 2 -tulostimilla järjestelmänvalvojat voivat myös suodattaa IP-osoitteita, palvelutyyppejä ja vastaanottavien ja lähettävien porttien numeroita IP Sec/IP Filtering -toiminnon avulla. Samalla he voivat päättää, hyväksytäänkö vai estetäänkö tietyt IP-osoitteet. Tuemme myös SNMPv3-sähköpostisalausta ja TLS1.3-protokollaa.



Monitoimitulostimen suojaaminen

Tulostimien lisäsuojauksia varten voit estää tietokoneyhteyden USB:n kautta sekä poistaa muistikortti- ja USB-muistiliitännät käytöstä. Voit myös käyttää kopiointin estävää vesileimaa⁵ alkuperäisten asiakirjojen luvattoman kopiointin estämiseen sekä PDF-salausta⁵ digitaalisten asiakirjojen turvallisuuden varmistamiseen.



Suojattu tulostus/skannaus

"Luottamuksellinen työ" -asetus tarkoittaa, että voit suojata asiakirjojen yksityisyyden ja estää laitteelle jääneiden tulosteiden luvattoman katselun.



WPA3

Epsonin uusimmat monitoimitulostimet tukevat WPA3-tekniikkaa⁵, joka on Wi-Fi-verkon uusi todennus- ja salaustekniikka. Se tarjoaa yrityksille entistä vahvemman suojan tietojen käsittelyyn langattomassa verkossa.



Asiakirjojen suojaus

Paranna tuottavuutta ja valvo käyttöä suojatulla tulostuksella, skannauksella ja kopiointilla käyttäjän todennuksen avulla.



Kulunvalvonta

Käyttäjän todennus ja toimintorajoitukset.



Laitteen suojaus

Laiteohjelmiston allekirjoituksen tarkistus, turvallinen käynnistys ja uusien haittaohjelmien käytönaikainen tunkeutumisentunnistus.



Väärentämistä estävä muste

DURABrite™ Pro -musteet imeytyvät syvälle paperin kuituihin suojaten tärkeitä asiakirjoja väärentämiseltä, ja ne täyttävät ISO 11798:2023 -standardin vaatimukset.



Käyttäjätietojen suojaus

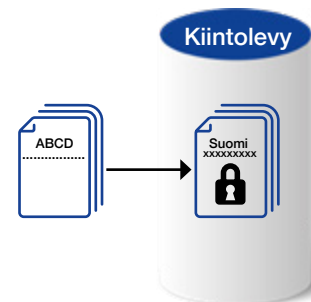
Voit asettaa yksilöllisiä salasanoja jaetuille sähköpostitileille⁵, asiakirjoille ja osoitekirjoille Epson-tulostimillasi. Täydellisen turvallisuuden takaamiseksi tiedot poistetaan tulostimesta, kun tulostus/skannaus on suoritettu loppuun tai virta on katkaistu. Jos laitteessa on kiintolevy, kaikki tiedot salataan ja tiedot poistetaan jokaisen tulostustyön jälkeen. Turvallisuuden lisäämiseksi järjestelmänvalvoja voi myös ylikirjoittaa kiintolevyn. Lue lisää [turvallisuusoppaastamme](#).

Tietosuojat

Kovalevyn salaus, kovalevyn tietojen poisto, Trusted Platform Module (TPM) ja salasanojen salaus.

Tallennettujen tietojen salaus kiintolevyllä

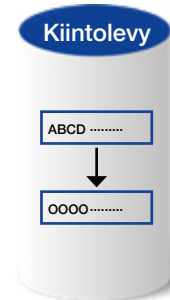
Suojaamme aina asiakastiedot salauksella, kun ne tallennetaan monitoimitulostimen sisäiselle kiintolevyille. Tietojen salaaminen estää luvattoman pääsyn tai haitallisen hyökkäyksen henkilötietoihin, jos kiintolevy varastetaan. Kiintolevyssä on itsensä salaava asema, ja asiakirjatiedot suojataan AES-256-salauksella.



Tulostustyön tietojen turvallinen poistaminen

Kun tämä on käytössä, kiintolevyllä olevat poistetut tiedot⁵ ylikirjoitetaan seuraavilla tavoilla tietojen palautuksen estämiseksi. Vaihtoehtoja on useita:

1. Nopea poisto: Salasavainta muutetaan, jotta poistettuja tietoja ei voi palauttaa.
2. Suojattu säännöllinen poisto: Salasavainta muutetaan, ja kiintolevyllä olevat poistetut tiedot ylikirjoitetaan arvolla "0", jotta poistettuja tietoja ei voi palauttaa.



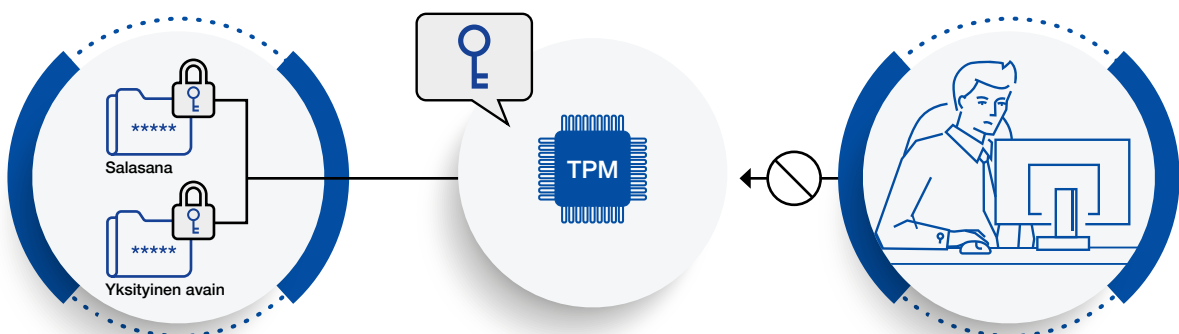
Katso yksityiskohtaiset tiedot tulostustöiden tietojen poistamisesta tuotteesi käyttöoppaasta.

TPM

TPM-järjestelmällä (Trusted Platform Module) varustetuissa malleissa suojaustaso on seuraavilla tavoilla parempi:

- Salattujen salasanojen ja yksityisten avaintietojen palauttamiseen tarvittavat salausavaimet säilytetään TPM-sirulla.
- TPM-siru voidaan suojata luvattomalta analyysiltä laiteasolla, koska TPM-sirua ei voi käyttää tulostimen ulkopuolelta.
- Selaimen (Web Config) kanssa käytävässä viestinnässä istuntoavaimina hyödynnetään TPM:n tuottamia aidosti satunnaisia lukuja.
- Salatun kiintolevyn todennusavaimet generoidaan TPM:n tuottamien aidosti satunnaisen lukujen avulla.

Monitoimitulostimissa on TPM 2.0 -siru.



	WorkForce Enterprise	WorkForce Enterprise AM	
Tuotteen nimi	WF-C21000/C20600/C20750	AM-C4000/C5000/ C6000 ja AM-M5500	AM-C400/C550/ C550z
Tyyppi	A3	A3	A4
Verkon suojaus			
TLS-viestintä	✓	✓	✓
TLS1.1, TLS1.2, TLS1.3	✓	✓	✓
Protokollien käyttöoikeuksien ja rajoitusten hallinta	✓	✓	✓
IPsec/IP Filtering	✓	✓	✓
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-todennus	✓	✓	✓
EAP-TLS, PEAP-TLS	✓	✓	✓
PEAP/MSCHAPv2	✓	✓	✓
EAP-TTLS	✓	✓	✓
AES128/AES256/3DES/RC4	✓	✓	✓
SNMPv3	✓	✓	✓
WPA3	✓	✓	✓
Käyttöliittymien erottaminen	✓	✓	✓
Monitoimitulostimen suojaaminen			
USB-yhteyden estäminen tietokoneesta	✓	✓	✓
Ulkaisen käyttöliittymän poistaminen käytöstä	✓	✓	✓
USB-muistin kautta tulevien virusten käsittely	✓	✓	✓
Tulostuksen/skannauksen suojaus			
Luottamukselliset työt	✓*6	✓	✓
Kopioinninestokuvio ⁶	✓	✓	✓
Vesileima ⁶	✓	✓	✓
PDF-salaus	✓	✓	✓
S/MIME	✓	✓	✓
AES-128/AES-192/AES-256/3DES	✓	✓	✓
SHA-1/SHA-256/SHA-384/SHA-512/MD5	✓	✓	✓
Verkkotunnusrajoitukset	✓*7	✓	✓
Valtuutussalasana verkkokansioon/FTP:lle skannaamiseen, sähköpostiin skannaamiseen ja sähköposti-ilmoituksiin	–	✓*7	✓
Pitkien todennussalasanojen tuki	–	–	✓*8
Tiedostokäytön oletusarvoinen estäminen PDL:n kautta	✓*7	✓	✓
Suojattu tulostus	✓	✓	✓
Faksin suojaus⁹			
Suoravalintarajoitukset	✓	✓	✓
Osoiteluettelon vahvistus	✓	✓	✓
Soittoäänien tunnistus	✓	✓	✓
Toimenpiteet hylättyjä fakseja vastaan	✓	✓	✓
Siirron vahvistusraportti	✓	✓	✓
Vastaanotettujen faksien varmuuskopiotietojen poistaminen	✓	✓	✓
Lähetyksen rajoitus useille vastaanottajille	✓	✓	✓
Tulostimen suojaus			
Automaattiset laiteohjelmistopäivitykset	✓	✓	✓
Suojaus luvattomia laiteohjelmistopäivityksiä vastaan	–	✓	✓
Turvallinen käynnistys	–	✓	✓
Haittaohjelmien havaitseminen	✓*7	✓	✓
Turvatoimet tulostinta hävittäessä			
Tehdasasetusten palautus	✓	✓	✓
Tietoturvasertifikaatit ja standardit			
ISO15408/IEEE2600.2™	✓	✓	✓

	WorkForce Enterprise	WorkForce Enterprise AM	
Tuotteen nimi	WF-C21000/C20600/C20750	AM-C4000/C5000/ C6000 ja AM-M5500	AM-C400/C550/ C550z
Tyyppi	A3	A3	A4
Turvaominaisuudet kolmannen osapuolen ohjelmistojen yhteensopivuuden ansiosta			
Open Platform -yhteensopiva malli	✓	✓	✓
Epson Print Admin (EPA) / EPA Serverless			
Käyttäjän todennus henkilökorttien/kirjautumistunnusten/ PIN-koodin avulla	✓	✓	✓
Laitteen toimintojen täydellinen hallinta käyttäjäkohtaisesti	✓	✓	✓
MFP-valikon yksilöinti	✓	✓	✓
Pull printing ja suoratulostus	✓	✓	✓
Skannaus ja lähetys omaan sähköpostiin tai kansioon	✓	✓	✓
Skannaus pilvipalveluihin (OneDrive for Business, SharePoint Online, Teams ja Google Drive) ¹⁰	✓	✓	✓
Skannaus salasanalla suojattuihin PDF-tiedostoihin	✓	✓	✓
Skannauksen työnkulun lisäasetukset ¹¹	✓	✓	✓
Ajuritön tulostus pilvipalveluista (OneDrive for Business, Share- Point Online ja Teams) ¹⁰	✓	✓	✓
Synkronointi hakemistopalvelun kanssa (LDAP, Open LDAP, Microsoft EntraID, Microsoft Entra DS, Google Secure LDAP ja Google Cloud Directory) ¹⁰	✓	✓	✓
Raportit – Käyttäjän suojausasetus – Piilota tiedostonimi	✓	✓	✓
Salasanakäytäntö, tilin lukitseminen ¹¹	✓	✓	✓
Tulostussäännöt ja -käytännöt ¹¹	✓	✓	✓
Seuranta ja raportointi	✓	✓	✓
Kiintiö ¹⁰	✓	✓	✓
Suojattu mobiilitulostus (AirPrint ja Mopria) ¹²	–	✓	✓
Käyttäjätietojen suojaus			
Tallennusalueen suojaus	✓	✓	✓
Osoitekirjan suojaaminen	✓	✓	✓
Monitoimitulostimen tietojen käsittely	✓	✓	✓
Tallennettujen tietojen salaus kiintolevyllä	✓	✓	✓
Tulostustyön tietojen turvallinen poistaminen	✓	✓	✓
Salasanojen salaus	✓	✓	✓
TPM	✓ ¹³	✓	✓
Kiintolevyn peilaus	–	✓	–
Toiminnan rajoittaminen			
Ohjauspaneelin lukitus	✓	✓	✓
Kulunvalvonta	✓	✓	✓
Todennettu tulostus/skannaus ⁸	✓	✓	✓
Salasanakäytäntö	✓	✓	✓
Seurantalogi	✓	✓	✓

Saat lisätietoja ottamalla yhteyttä Epson-myyntiedustajaan.

Asiakkaan nimi:

Puhelinnumero:

Sähköposti:

1. Print Security Landscape, 2025 - Identity, AI, and Quantum: Navigating the New Threat Landscape', Quocirca, July 2025.
2. Keypoint Intelligence Security Validation Testing Seal 2024–2026 koskee malleja AM-C400 ja AM-C550.
3. ISO/IEC 15408 -sertifiointi ei koske laitteen oletusasetuksia. Vaatii erityisen laiteohjelmiston ja määrittäprosessin.
4. CCRA-sertifiointilogo osoittaa, että tuote on arvioitu ja sertifioitu Japanin tietotekniikan turvallisuuden arviointi- ja sertifiointijärjestelmän (JISEC) mukaisesti. Se ei tarkoita, että tuotteessa ei olisi mitään haavoittuvuuksia. Se ei myöskään tarkoita, että tuotteessa olisi kaikki tarvittavat suojaustoiminnot kaikissa käyttöympäristöissä.
5. Täydellinen luettelo mallin teknisistä tiedoista on osoitteessa support.epson.net/security/en
6. Tukee vain Windows-tulostinajuria.
7. Jos haluat käyttää tätä toimintoa, päivitä tulostimen laiteohjelmisto uusimpaan versioon.
8. Edellyttää todennettua tulostusmenetelmää.
9. Saatavilla vain, kun olet asentanut lisävarusteena saatavan faksikortin.
10. Koskee Epson Print Adminia ja vain tiettyjä Epson Print Admin Serverless -yhteensopivia tuotteita.
11. Koskee vain Epson Print Admin -ratkaisua.
12. Koskee vain Epson Print Admin Serverless -ratkaisua.
13. Ei välttämättä tueta alueesta riippuen. Saat lisätietoja tuotteiden saatavuudesta maassasi ottamalla yhteyttä paikalliseen myyntipisteeseen.



Kierrätä vastuullisesti

Epson Suomi
Puhelin: 09-3158 3267
Palvelemme arkisin klo 09.00-18.00
E-mail: level.one@epson.fi
www.epson.fi/contactus

Rajatorpantie 41 C
01640 Vantaa



@epsonsuomi
epson-suomi

Ajurit, ohjelmistot ja käyttöohjeet: epson.sn

Tavaramerkit ja rekisteröidyt tavaramerkit ovat Seiko Epson Corporationin tai omistajiensa omaisuutta.
Tuotetietoja voidaan muuttaa ilman ennakkoilmoitusta.