

Helyszíni adatgyűjtő ügynök / DCA

Biztonsági és üzemeltetési tájékoztató

Műszaki referencia az informatikai jóváhagyáshoz és üzemeltetéshez

Dokumentumverzió: 1.21 · Felülvizsgálva: 2026. október 25.
Címzettek: IT-üzemeltetés, hálózatbiztonság, végpontvédelem, adatvédelem
Kiadó: Sziráki Márton e.v. / PrinterMS · Műszaki leírás, önálló SLA-vállalás nélkül.

A PrinterMS ügynök a nyomtatók azonosítóit, számlálóit, kellékanyag-szintjeit és állapotát olvassa ki, majd a szolgáltató PrinterMS-fiókjába továbbítja. E dokumentum a telepítés jóváhagyásához és a működés ellenőrzéséhez szükséges műszaki feltételeket rögzíti.

1. Nyomtatók SNMP / IPP / IPPS Célzott, olvasási lekérdezések	→	2. Helyi ügynök Ellenőrzés, helyi adatsor Ütemezett továbbítás	→	3. PrinterMS API HTTPS / TCP 443 Tárolás és jogosult megjelenítés
Nyomtatási tartalom	Nem kérdez le dokumentumot, nyomtatási feladatot, várólistát, címjegyzéket vagy felhasználói fájlt; nem küld nyomtatási feladatot és nem módosít nyomtatóbeállítást.			
Hálózati hozzáférés	Kimenő HTTPS az <code>api.printerms.com</code> felé; LAN SNMP/IPP. Alapesetben időszakos felderítés és helyi mDNS. Nincs távoli belépést fogadó ügynökszerver.			
Távoli irányítás	A kimenő HTTPS-kérések válasza konfigurációt és meghatározott műveleti utasításokat is közölhet. Nincs általános távoli parancssor vagy tetszőleges szkriptfuttatási művelet.			
Helyi védelem	Elkülönített gyűjtőszolgáltatás Windows, Linux és macOS alatt. Saját állományok és hitelesítők hozzáférés-korlátozással; a token Windows alatt DPAPI-védett (E1), az adatsor nincs külön alkalmazásszinten titkosítva.			
Leállítás hatása	A közvetlen nyomtatási útvonala tovább működik. Az új műszaki megfigyelések és az ezekre épülő jelzések szünetelnek; a felhőben tárolt korábbi adatok megmaradnak.			

A leírás a felülvizsgálatkor elérhető működésre vonatkozik. A tényleges kiadás verzióját és SHA-256 azonosítóját a letöltőoldal, az ügynök verziójelzése és a telepítési jegyzőkönyv rögzíti. A platformok és a telepítési módok eltéréseit a 6. és 9. oldal részletezi.

Adatok és adatminimalizálás	2	Műszaki metaadatok célja	3
Hálózati kapcsolatok	4	Protokollok és felderítés	5
Telepítés és jogosultságok	6	Helyi tárolás és üzemzavar	7
Felhő, hozzáférés és megőrzés	8	Aktiválás és távoli műveletek	9
Fenyegetések és védelmek	10	Ellenőrzés, leállítás, kapcsolat	14

Gyűjtött és továbbított adatok

A mérési csomagok műszaki eszközadatokat tartalmaznak. A gazdagép és az ügynök működéséről külön metaadatok szükségesek az aktiváláshoz, a hibakereséshez és a kapcsolat felügyeletéhez. Az alábbi mezők egy része csak akkor szerepel, ha a készülék közli, illetve az adott funkció használja.

Adatkör	Pontos tartalom és cél	Kezelés helye
Nyomtatóazonosítók	Gyári szám, gyártó, modell, nyomtató-IP és elérhető firmware-verzió; a mérés eszközhöz rendeléséhez. Helyi USB-kapcsolatnál a loopback cím nem kerül nyomtató-IP-ként beküldésre.	Helyben és a PrinterMS felhőben.
Számlálók	Összes, mono, színes és szkennelési számláló, a teljes számláló mértékegysége; mérési idő, esetenként eszközüzemidő és számláló-visszaállítás jelzése.	Helyi adatsor, majd felhő.
Kellékanyagok	Kellék megnevezése, osztálya, színe, százalékos vagy nyers szintje, kapacitása, mértékegysége és állapota.	Helyi adatsor, majd felhő.
Állapot és hibák	Hibabitek, aktív hibakódok, súlyosság, forrás és tisztított gyártói hibaleírás; mérési idő, esetenként teljes lapszám.	Helyi adatsor, majd felhő.
Olvashatósági jelzések	A számláló-, toner- és hibakiolvasás eredményessége, forrása, kötött okkódja, a használt lekérdezési definíció verziója.	Helyi adatsor, majd felhő.
Eszköztámogatási beolvasás	Kifejezett kérésre, vagy ha a szervezet Tulajdonosa belépett az eszköztámogatási programba (lásd 08): egy nyomtató beépített, nyomtatós MIB-ágainak egyszeri, kitakart beolvasása, hogy a PrinterMS támogatást írhasson egy még nem teljesen olvasott géphez. Opcionálisan a kérés által csatolt számlálólap- vagy kijelzőfotó.	Helyben kitakarva, majd felhő; 12 hónapig.
Próbaszabály-leolvasás	Csak ha a PrinterMS aláírt próbacsomagot tesz közzé: a napi számlálóleolvasáskor az ügynök a próbaszabály szerint is kiolvassa ugyanazon nyomtató számlálóit. Az eredmény nem jelenik meg, nem számlázódik és nem írja felül az élő értéket; csak a szabály ellenőrzésére szolgál.	Felhő; 30 napig.
Aktiválási metaadatok	A gazdagép neve, platformja, processzorarchitektúrája, ügynökverziója és a gép által látott privát IPv4-alhálózatok (legfeljebb 16). A szerver a kapcsolat forrás-IP-jét is rögzíti.	Az aktiválási folyamat és a felhőbeli ügynökrekord.
Ügynökállapot	Verzió, platform, architektúra, kapcsolat időpontja, eszközszám; függő és visszautasított csomagok száma, adatsorméret, telítettség; frissítési állapot, kötött hibakód és rögzített listából választott hibaok (például névfeloldás, tanúsítvány vagy zárolt fájl), URL, elérési út és nyers hibaszöveg nélkül; a helyi agent .json fájlban megadott IP-címek és címtartományok (legfeljebb 64); a felhős lista korlátozási módja, a kihagyott felhős tartományok, a hatókörön kívüli nyomtatók száma, a frissítési mód, a legalacsonyabb SNMP-verzió és a gyenge SNMPv3-titkosítás engedélyezése.	Állapotjelzés a felhőnek; helyi működési állapot.
Helyi technikai állapot	Ismert nyomtatók útvonalai és rendszerleírásai, SNMP-változat, korábbi számlálóértékek, esedékes mérések, konfiguráció és naplók.	Saját helyi állományok. Ezek teljes tartalmát az ügynök nem tölti fel automatikusan.
Hitelesítők	Aktiválási titkok, saját eszköztoken; helyben megadott SNMP community vagy SNMPv3 felhasználónév és kulcsok. Ezek nem mérési adatok.	Aktiválás/API-hitelesítés, illetve helyi SNMP. Az SNMP-hitelesítők nem részei a felhős telemetriának.

A gyűjtésen kívül eső tartalmak

Az ügynök nem olvassa a nyomtatási, szkennelési, másolási vagy faxfeladatok tartalmát és történetét, a spoolfájlokat, fájlneveket, címjegyzékeket, e-maileket, böngészési előzményeket vagy billentyűleütéseket. Nem kérdez le felhasználói munkameneteket és nem készít képernyőképet. Saját konfigurációját és állományait olvassa és írja.

Támogatási adatátadás: az ügynök nem tölti fel automatikusan a teljes helyi naplót. Hibajegyhez verzió, OS, időpont, hibakód és ellenőrzött naplórészlet adható. Titkot vagy teljes adatkönyvtárat csak külön egyeztetett védett csatornán adjon át.

Személyhez kapcsolható metaadatok. Egy gazdagépnév, IP-cím vagy szabad szöveges nyomtatómező az ügyfél környezetében személyt is azonosíthat. Ezért nem állítjuk, hogy minden műszaki adat szükségszerűen személytelen. A tisztított hibaszöveg sem jelent automatikus anonimizálást; célszerű személynevek nélküli eszköznevezést használni.

Miért szükségesek ezek az adatok?

A nyomtatómérések mellett a telepítés azonosításához, a kompatibilis szoftver kiválasztásához és a működési hibák feltárásához is kezelünk műszaki adatokat. Az alábbi táblázat megmutatja, melyik adat milyen üzemeltetési feladatot segít.

Adat	Felhasználási cél és értelmezés
Az ügynök gazdagépneve (hosztnév)	Az aktiválás jóváhagyója és az üzemeltető felismerheti, melyik számítógépre került az ügynök. Több telepítésnél segít a megfelelő gép kiválasztásában, például hibaelhárítás vagy távoli karbantartás előtt. A gépnév nem felhasználónév és nem hitelesítő adat.
A kapcsolat forrás-IP-címe	A szerver által látott hálózati forrást rögzíti. Kapcsolati hiba vagy incidens vizsgálatakor összevethető az ügyfél tűzfal- és proxynaplójával. NAT vagy proxy esetén több gép közös kilépési címe is lehet; nem feltétlenül a gazdagép belső IP-je, és önmagában nem azonosít megbízhatóan egy gépet. Aktiváláskor a jóváhagyó azt is látja, hogy a cím egyezik-e a szervezet egy meglévő ügynökének címével.
A nyomtató belső IP-címe	A helyi ügynök ezen a címen éri el a nyomtatót. A felhőbeli eszközkönyvtárban az IT számára segít megkeresni az érintett készüléket és kivizsgálni a címváltozást vagy elérési hibát. Az IP-cím ismerete nem biztosít a PrinterMS felhőnek közvetlen belépést az ügyfél hálózatába.
Platform és processzorarchitektúra	A Windows/Linux/macOS platform és az amd64/arm64 jellegű architektúra alapján dönthető el, melyik ügynökcsoomag kompatibilis, és mely karbantartási mód támogatott. Ezek nem a processzor sorozatszámát, teljesítményét vagy az alkalmazott munkáját írják le.
Ügynökverzió és frissítési állapot	A támogatott kiadás és funkciók ellenőrzését, a frissítési cél kiválasztását, valamint a sikeres, sikertelen vagy visszaállított frissítés megkülönböztetését szolgálja. Hibabejelentésnél segít a problémát a megfelelő szoftververzióhoz kötni.
Gyári szám, gyártó, modell és firmware	A gyári szám a mérés megfelelő nyomtatóhoz rendelését, a gyártó és modell a megfelelő kiolvasási szabály használatát segíti. Az elérhető firmware-verzió kompatibilitási és szervizhibák vizsgálatára használható. A firmware kiolvasása nem jelent nyomtatófirmware-frissítési jogosultságot vagy funkciót.
Időpontok, eszközszám és adatsorállapot	Az utolsó kapcsolat és mérés ideje jelzi az adatok frissességét. Az eszközszám a felderítés ellenőrzését, a függő/visszautasított csomagok száma és az adatsorméret az adatküldési elakadás felismerését segíti. Ezek műszaki működési jelzések, nem nyomtatott dokumentumok tartalmait.
Megadott IP-címek és címtartományok	A figyelt nyomtatói kör meghatározására és a felderítési munka kiosztására szolgálnak. Az aktiváláskor jelzett helyi alhálózatok csak javaslatként jelennek meg egy új hálózat címtartományaként; a felhőből nem megadható javaslatot a szerver elhagyja, a többit a jóváhagyó módosíthatja. A felhős címlista helyi korlátozási módja, a kihagyott tartományok és a hatókörön kívüli nyomtatók száma azt mutatja meg a hálózat oldalán, hogy a felhős címlista mely része nem érvényesül. A multicast felderítés külön beállítás; a célcímek tényleges hálózati korlátozását az ügyfél tűzfalszabályai is érvényesítheti.

Mit érdemes az IT-jóváhagyáskor rögzíteni?

Használjanak személynevet nem tartalmazó gazdagép- és nyomtatóelnevezéseket; határozzák meg a figyelt címeket, a gyűjtési kategóriákat és az adatokhoz hozzáférő munkatársakat. Az IP és a hosztnév az ügyfél környezetében személyhez kapcsolható lehet. A gyűjtési kategóriák kikapcsolása nem kapcsolja ki automatikusan az aktiválási és kapcsolati metaadatokat; ezekhez jelenleg nincs külön mezőnkénti tiltás.

A nyomtatói mérési adatok, a gazdagép metaadatai és a csak helyben tárolt hitelesítők eltérő adatkörök. Tárolási helyüket az adatleltár, hozzáférésüket és megőrzésüket a felhőbeli adatkezelés fejezete részletezi.

Hálózati kapcsolatok és végpontok

Az ügynök nem biztosít bejövő alkalmazáskapcsolatot fogadó szervert, webes kezelőfelületet vagy távoli asztalt. A kapcsolatok az ügynök felől indulnak; a felderítéshez rövid ideig UDP-válaszokat fogadó socketek is nyílnak. Porttovábbításra és internet felől nyitott kezelőportra nincs szükség.

Cél / irány	Port, protokoll	Feladat és bekapcsolási feltétel
api.printerms.com Kimenő, internet	TCP 443 HTTPS	Üzemszerű felhőkapcsolat. Aktiválás, telemetria, állapotjelzés, konfiguráció, tokenkezelés, aláírt definíciók és frissítési jegyzék. Ha a frissítési fájl az agent.printerms.com címről nem tölthető le, az ügynök (1.9.0-tól) egyszer ezen a címen keresztül, eszköztokennel kéri le ugyanazt a fájlt.
Engedélyezett nyomtató-IP-k Kimenő, helyi/routolt hálózat	UDP 161 SNMP	Elsődleges azonosítás és olvasás. A felderítés címjelöltjeit is megkeresi; azok között nem nyomtató eszköz is lehet.
Engedélyezett nyomtató-IP-k Kimenő, helyi/routolt hálózat	TCP 631 IPP / IPPS	Alapesetben engedélyezett azonosítás és tartalék lekérdezés. Helyben teljesen kikapcsolható.
224.0.0.251 ff02::fb Helyi multicast és válaszok	UDP 5353 mDNS / DNS-SD	Alapesetben engedélyezett, időben korlátozott _ipp._tcp és _ipps._tcp keresés. Külön letiltható; a scanless mód is tiltja.
239.255.255.250 ff02::c Helyi multicast és válaszok	UDP 3702 WS-Discovery	Opcionális, alapból kikapcsolt. Csak engedélyező helyi vagy felhős beállítással; a scanless mód ezt is tiltja.
127.0.0.1 / ::1 Csak a gazdagépen belül	TCP 60000-65535 HTTP / IPP	Opcionális, alapból kikapcsolt IPP-over-USB csatlakozó. A külön telepített OpenPrinting ipp-usb szolgáltatást kérdezi le; nem általános helyi portpásztázás.
A gazdagép beállított névfeloldói OS-szolgáltatás	A helyi DNS- szabály szerint	A felhőcímek feloldásához. Az ügynök nem ír elő saját nyilvános DNS-kiszolgálót. A HTTPS elérés IPv4-en vagy IPv6-on is történhet.

Telepítés és frissítés: külön engedélyezési kör

A nyilvános letöltőoldal az agent.printerms.com címen, HTTPS-en érhető el; a nyilvános oldal, telepítő és parancs nem tartalmaz titkot, és a telepítő gépen nincs szükség PrinterMS-bejelentkezésre. A kiadási fájlok és a parancsalapú telepítés a github.com/PrinterMS/agent-releases tárhelyet használhatják, GitHub által kijelölt letöltési hosztra történő átirányítással. A rövid telepítőparancsok (curl -fsSL https://agent.printerms.com/install.sh | sudo sh, illetve irm https://agent.printerms.com/install.ps1 | iex) az agent.printerms.com címről egy kis indítószkriptet töltenek le, amely a rögzített kiadás telepítőjét csak az SHA-256 lenyomat (Windows alatt a PrinterMS digitális aláírása) egyezése után futtatja rendszergazdaként; a szkript egyetlen, az utolsó sorban meghívott függvény, így egy megszakadt letöltés semmit nem futtat. A letöltőoldalon a hosszabb, lenyomattal rögzített „Ellenőrzött telepítés” parancs is elérhető. Docker esetén a kiválasztott képtár (jellemzően ghcr.io) elérése is szükséges. A Windows Setup a gépen csak jóváhagyott aktiválás után véglegesíti; Linux, macOS és Docker alatt a szolgáltatás előbb települ, és a jóváhagyásig felderítés és adatküldés nélkül várakozik.

Telepítési link: a link az agent.printerms.com/t#TOKEN oldalt nyitja; a token a # utáni részben van, így a böngésző az oldal lekérésekor nem küldi el. A Windows Setup és a macOS-csomag a saját fájlnevéből (PrinterMS-Agent-Setup-TOKEN.exe), az install.sh a DCA_INSTALL_TOKEN_FILE fájlból (induláskor törli) vagy a DCA_INSTALL_TOKEN változóból olvassa, ezért a linket, a fájlt és a parancsot a lejáratig titokként kell kezelni. Sikertelen linkes telepítésnél csak a token és egy rögzített hibakód (például PMS-S001) megy az api.printerms.com címre.

Windows telepítés/frissítés közben az operációs rendszer a kiadás aláíró- és időbélyeg-tanúsítványának láncát és visszavonási állapotát ellenőrzi. A tanúsítványban megadott PKI/CRL/OCSP végpontok TCP 80/443 elérése szükséges lehet. Ezek a letöltési és bizalmi kapcsolatok nem nyomtatói telemetriát továbbítanak.

Minimális üzemeltetési szabály. A natív, kézzel frissített telepítéshez az API TCP/443 és a választott nyomtatói protokollok elegendők, a névfeloldás és a szükséges válaszforgalom mellett. Letöltéshez a konkrét kiadás tényleges URL-láncát kell jóváhagyni. Automatikus frissítést csak ismert, kiadáshoz kötött célhosztokkal szabad engedélyezni; nincs általános internetelési igény.

A felhőszolgáltatók belső adatútja nem igényel közvetlen adatbázis-, Google Cloud- vagy AWS-kapcsolatot az ügyfél ügynökétől. A weboldal és a telepítés hálózati forgalmát külön kell értékelni az állandó gyűjtőszolgáltatástól.

Felderítés és lekérdezési protokollok

Olvasási műveletek és titkosítás

SNMP: az ügynök GET és korlátozott táblalekérdezési műveleteket használ; nem küld SNMP SET-et. A nyomtatón kizárólag olvasási jogosultságú hozzáférést kell biztosítani. Az `snmp.min_version` a legalacsonyabb kipróbált verzió: `v1` (alapérték) esetén a beállított `v3` után `v2c`, majd `v1`, `v2c` esetén `v1` nélkül, `v3` esetén csak `v3`, community nélkül. A `v1/v2c` community és forgalom titkosítatlan; a gyári `public` csak megadott community hiányában használatos.

Szigorú SNMPv3-környezet: az SNMPv3 csak megfelelő `authPriv` beállítással biztosít hitelesítést és titkosítást; MD5-vagy DES-alapú hitelesítő csak `snmp.allow_weak_v3_crypto: true` mellett töltődik be (lásd 09, F1).

IPP: kizárólag `Get-Printer-Attributes` művelet történik, nyomtatási feladat beküldése nélkül. A közvetlen IPP alpból titkosítatlan HTTP-t használ. IPPS-hez az operációs rendszer tanúsítványbizalma vagy egy adott nyomtató előre jóváhagyott SHA-256 tanúsítványlenyomata használható. IPPS-ellenőrzési hibánál az adott IPPS-útvonal nem esik vissza titkosítatlan IPP-re.

Hatókör, gyakoriság és terhelés

A felhőből kapott címlista elsőbbséget élvez a helyi `cidrs` beállítással szemben, de csak két korláton belül. Abban csak magánhálózati, CGNAT (`100.64.0.0/10`) vagy IPv6 ULA cím, illetve ilyen, legfeljebb 65 536 címes tartomány lehet; nyilvános, loopback, link-local vagy felhős metaadat-címet (például `169.254.169.254`) a szerver nem fogad el, az ügynök kihagyja és jelenti. A helyi `remote_config.scan_ranges` beállítás `bounded` értéke a felhős listát a helyi `cidrs` által lefedett részre szűkíti, `locked` értéke kizárja (lásd 09). Felhős lista nélkül a helyi lista, ennek hiányában a helyi magánhálózati interfészek tartománya érvényes. Minden nyomtatói kapcsolat, az ismert nyomtatóké is, ezen a hatókörön belül marad. Az ügynök a helyi lista felhőből is megadható elemeit jelenti, így a webes felület megmutatja, ha abban a felhős listán kívüli cím szerepel; a felhős listába csak egy jogosult felhasználó veheti fel. A VPN-, alagút- és konténerinterfészek szűrése nem helyettesíti az IT által jóváhagyott címlistát és tűzfalszabályt.

Művelet / korlát	Alapérték és kivételek
Újrafelderítés	30 percenként; indításkor, hatókörváltáskor és kezelői kérésre is. Aktív/tartalék csoportban a tartalék ügynök nem végez rendszeres gyűjtést.
Számláló / kellék / állapot / heartbeat	Számláló és kellék: alpból naponta; hálózatonként külön állítható óránként és 90 naponként között. Állapot: 15 percenként; heartbeat: 5 percenként. Új eszköz, elmaradt mérés, elszámolási forduló vagy kézi kérés további leolvasást indíthat.
Felderítési keret	Alpból 8192 cím ciklusonként, 50 ms indítási köz (legfeljebb kb. 20 új cím/s). Ezek konfigurációs értékek, nem minden kiadásra érvényes teljesítménygaranciák.
Párhuzamosság / várakozás	Általános alapérték: 16 felderítési feladat; a natív Windows Setup 64-et állít be. SNMP-várakozás: 2 s, 1 újrapróbálkozás. Egy cím több protokollkérést is kaphat.

Felderítés nélküli, szűkített beállítás

Az alábbi részletet az érvényes `agent.json` megfelelő mezőibe kell beilleszteni. Példacím helyett jóváhagyott nyomtató-IP-t kell megadni; a felhőben beállított címeknek is egyezniük kell.

```
{
  "cidrs": ["192.168.10.25"],
  "discovery": { "scanless": true },
  "ipp": { "disabled": true },
  "updates": { "mode": "managed" },
  "remote_config": { "scan_ranges": "locked" }
}
```

Ez SNMP-alapú működést tart meg, és tiltja a tartománykibontást, az mDNS-t, a WSD-t és az IPP-t. IPP megtartásához a `disabled` értéke legyen `false`; csak az mDNS külön tiltásához `ipp.mdns_disabled: true` használható. A helyi módosítás után a szolgáltatást újra kell indítani. Egy puszta IP-lista nem helyettesíti a `scanless: true` beállítást. A `locked` érték miatt a felhő nem bővítheti a hatókört.

Eszközazonosság: a nyomtató által közölt egyértelmű gyári szám szükséges; az IP-cím, a hirdetett név vagy UUID önmagában nem elég. A kód minden mérésnél újra igazolja a gyári számot. Ez az összerendelési hibákat csökkenti; titkosítatlan protokollon nem jelent kriptográfiai eszközhitelesítést.

Telepítés és futási jogosultságok

A telepítés helyi adminisztrátori jogosultságot igényel, PrinterMS-felhasználói jelszót nem. A szolgáltatás rendszerindításkor elindul, hibás kilépés után pedig a szolgáltatáskezelő újraindíthatja.

Telepítési mód	Futási jogosultság	Hatás és támogatási keret
Natív Windows	A gyűjtő: NT SERVICE\printerms-agent. Két külön, igény szerint indított karbantartási szolgáltatás: LocalSystem.	Az elsődleges telepítési út. x64 Windows 10/11, Windows Server 2016 vagy újabb technikai célplatform; csak az ügyfél által támogatott, frissített OS-kiadáson telepítendő.
Linux / systemd	Elkülönített printerms-agent felhasználó. Külön rövid életű root segédprogram a karbantartáshoz.	x64/arm64 kiadás; írásvédett rendszerterület, korlátozott írható állapottároló, üres capability-készlet, eszköz- és kernelkorlátozások.
macOS / launchd	A gyűjtő LaunchDaemon a rejtett, bejelentkezésre nem használható _printerms fiókkal fut, az agent.json fájlt csak olvassa. Frissítéshez és távoli leszereléshez külön root LaunchDaemon (E2).	x64/arm64 bináris. A menedzselt Mac-környezethez szükséges aláírási/notarizációs és telepítési bizonyítékot kiadásonként ellenőrizni kell; a bináris elérhetősége önmagában nem ilyen igazolás.
Docker	A kiadási Dockerfile nem root felhasználót használ (65532). Az állapothoz írható kötet szükséges.	A konténerképet az IT cseréli. A LAN-útvonal és multicast-elérés a host/bridge/Desktop hálózati módtól függ; külön ellenőrzendő.

Szolgáltatások és alapértelmezett helyek

Windows program / konfiguráció	C:\Program Files\PrinterMS\Agent\printerms-agent.exe C:\Program Files\PrinterMS\Agent\agent.json
Windows állapot / telepítő	C:\ProgramData\PrinterMS\Agent C:\ProgramData\PrinterMS\Installer (telepítési, helyreállítási és diagnosztikai állományok)
Windows-szolgáltatások	printerms-agent printerms-agent-decommission-helper printerms-agent-update-helper
Linux	/usr/bin/printerms-agent /etc/printerms-agent/agent.json /var/lib/printerms-agent; karbantartáskor védett /run és frissítési állapotterületek is használatosak.
macOS	/usr/local/bin/printerms-agent /Library/Application Support/PrinterMS/Agent (agent.json; állapot: Data) /Library/LaunchDaemons/com.printerms.agent.plist; külön frissítési és leszerelési LaunchDaemon is települ.
Docker	A data_dir / DCA_DATA_DIR által kijelölt tartós kötet. A tényleges elérési út és újraindítási szabály a konténer telepítési leírásának része.

A gazdagép módosításának határa. Saját könyvtárak, szolgáltatások, ACL-ek és eltávolítási bejegyzés készülnek. Nyomatatódriver és nyomtatási útvonal nem változik. Az opcionális ipp-usb külön szoftver, saját USB-jogosultságokkal.

Helyi adattárolás és megőrzés

Állomány / csoport	Tartalom	Megőrzés / törlés
agent.json device_token	Hálózati és működési beállítások; SNMP-hitelesítők, ha megadták őket; külön fájlban az ügynök API-tokenje.	A telepítés élettartamáig, módosításig vagy tokenrotációig. Teljes eltávolításkor törlendők.
outbox.db	bbolt adatbázis: továbbításra váró JSON mérési csomagok; külön részben a végleg visszautasított vagy hibás csomagok.	A sikeresen átvett csomag logikailag törlődik. A visszautasított csomag megmarad diagnosztikához/újraküldéshez; nincs automatikus időalapú helyi lejárat.
known_devices.json	Gyári számok, címek, IPP-útvonalak, rendszerleírások, lekérdezési mód, utolsó sikeres megfigyelés és esedékes mérések.	A készüléknyilvántartás frissül; 7 napja nem igazolt nyomtató kikerülhet. A lemezállapot futás közben frissül.
reset_baselines.json anchor_state agent_role	Számláló-visszaállítás felismeréséhez használt előzmény, elszámolási forduló és aktív/tartalék szerep.	Új állapot felülírásáig, illetve teljes eltávolításig; nincs minden fájlra közös időkorlát.
agent.log és mentései	Indulás, kapcsolat, felderítés, hibák, műveletek. Tartalmazhat IP-címet, gyári számot, helyi útvonalat és technikai hibaszöveget; az aktiválási kódot csak kitakarva (lásd 09, E4).	Méret szerinti forgatás: 5 MiB aktív napló, legfeljebb 3 korábbi fájl. Ez méretkorlát, nem napokban megadott megőrzés.
Definíciók, frissítések, telepítőállapot	Aláírt definíció/jegyzék, visszalépést tiltó állapot, letöltött jelölt, korábbi bináris és tranzakciós diagnosztika.	A frissítés/telepítés életciklusa és takarítása szerint. Sikertelen művelet helyreállítási állományokat hagyhat.

Tárolási védelem

Windows alatt szolgáltatásazonosítóhoz kötött ACL-ek, Linux és macOS alatt elkülönített felhasználó és korlátozott állományjogok védik a saját adatokat. Windows alatt az eszköztoken gépszintű DPAPI-védelmet kap (E1); az adatsor, más rendszeren a token is, **nem kap külön alkalmazásszintű titkosítást**. A szükséges lemeztitkosítást, biztonsági mentést és adminisztrátori hozzáférés-védelmet a gazdagép IT-szabályai biztosítják.

A logikai rekordtörlés nem biztonságos lemeztörlés: a bbolt felszabadult lapokat újrahasznál, és nem zsugorítja a fájlt minden átvétel után. Az adminisztrátori hozzáférés a helyi adatokat is elérheti. A tokenfájlt és a teljes adatkönyvtárat nem szabad másik ügynök klónozására használni.

Internetkimaradás és megtelt adatsor

A már lemezre írt mérések újraindítás után is megmaradnak. Az ügynök átmeneti kapcsolati hibánál késleltetve újrapróbálkozik; sikeres API-átvételig nem törli a csomagot. A szerver átvételi visszaigazolása a befogadást jelenti, a további feldolgozás külön lépés.

A teljes helyi keret **5000 csomag vagy 512 MiB logikai csomagtartalom**, beleértve a visszautasított csomagokat. Ebből 200 csomag és 32 MiB hibajelzéseknek fenntartott tartalék. A fizikai adatbázisfájl és az egyéb állományok miatt a teljes lemezhasználat nagyobb lehet.

A kimaradásvédelem korlátja. Telítődéskor a meglévő bizonyíték megmarad, de új pillanatfelvételek tárolása korlátozódhat. Rövid életű hibák elveszhetnek; leállított vagy alvó gazdagép nem mér. A sor nem jelent korlátlan kieséstűrést vagy általános adatvesztés-mentességi garanciát.

A systemd journal, a macOS külön stderr-naplója, a Windows-telepítő naplói és a konténernaplók megőrzését külön kell kezelni; az agent.log forgatási korlátja ezekre nem vonatkozik.

Felhőbeli adatkezelés és hozzáférés

Az ügynök az `api.printerms.com` API-n keresztül a hozzá rendelt szervezethez és hálózathoz küldi az adatokat. Az API az eszköztokenből állapítja meg az ügynök jogosultságát; a telemetria nem adhat szabadon másik szervezetazonosítót. A kóddal aktivált ügynök a jóváhagyás után az első méréstől megbízható; a jóváhagyást a szervezet jogosult felhasználója adja meg a futtató gép adatainak ismeretében. A megjelenítést szervezeti jogosultságellenőrzés és adatbázisoldali, soronkénti hozzáférési szabályok (RLS) korlátozzák.

Szolgáltatási elem	Szerep a DCA adatútjában	Dokumentált hely
Google Cloud / Cloud Run	API és háttérfeldolgozás, műszaki kérések kezelése.	Belgium, europe-west1.
Google Cloud	Felhőbeli adatbázis és fájl tárolás, napi mentésekkel.	Belgium, europe-west1; mentések az EU-n belül.
Amazon Web Services	A PrinterMS felhasználóinak hitelesítése (Amazon Cognito).	Írország, eu-west-1.
Cloudflare	Weboldal, letöltőoldal és DNS/CDN-kiszolgálás; webes kérési metaadatok.	Globális peremhálózat; nem az ügynök helyi mérési adatbázisa.
E-mail és támogatás	Bekapcsolt értesítések és külön elküldött támogatási megkeresések.	Az alfeldolgozói jegyzék szerint. A támogatási levelezés nem kizárólag EU-régiós.

Az EU-régiós elsődleges tárolás mellett járulékos nemzetközi támogatási vagy szolgáltatói hozzáférés lehetséges. Szolgáltatók és továbbítási feltételek: printerms.com/alfeldolgozok.

Hozzáférés és felelősség

A nyomtatóüzemeltető szervezet megfelelő megtekintési joggal rendelkező felhasználói férnek hozzá a saját adatokhoz; a konfiguráció, tokenkezelés és eltávolítás külön módosítási/törlési jogosultsághoz kötött. A PrinterMS szolgáltatói üzemeltetése privilegizált rendszer-hozzáférést igényelhet; az RLS nem jelent az adatbázis-üzemeltetővel szembeni titkosítást.

Az ügyféllel közvetlenül szerződő nyomtatóüzemeltető határozza meg a gyűjtés célját és jogosultjait; a PrinterMS adatfeldolgozói szerepét az adatfeldolgozási megállapodás rögzíti. Személyhez kapcsolható technikai adata is ezek a feltételek alkalmazandók. A titoktartási, incidensjelzési és ellenőrzési feltételek közvetlenül elérhetők a dokumentum végén.

Megőrzés és törlés

Felhőbeli adatkör	Dokumentált működés
Lezárt nyers beküldési feladatok	Alapértelmezett takarítás: számláló- és kellékadatnál 7 nap, egyéb beküldésnél 30 nap. Folyamatban lévő/újrapróbálható munka nem ilyen lezárt rekord.
Részletes DCA műszaki előzmények	Kellékadat: alapból 90 nap; állapot: 30 nap; megszünt riasztás: a megszüntéstől 180 nap. Az aktív hiba és az aktuális eszközpillanatkép nem ezen időkorlát szerint törlődik.
Mérőállások és üzleti eszközrekordok	A szervezet adatállományának részei. Egy ügynök eltávolítása vagy eszköz deaktiválása nem törli automatikusan a korábbi adatokat.
Eszköztámogatási beolvasás és fotó	12 hónap után törlődik, a kérés eredménye megmarad; csak a PrinterMS munkatársai látják. A szervezet törlésével együtt törlődik.
Próbaszabály-eredmények	30 nap után törlődnek; nem jelennek meg és nem számláznak.
Fiók megszűnése / adattörlés	Az adatfeldolgozási megállapodás szerinti export, 30 napos visszaadási/türelmi idő és végleges törlés; jogszabályi megőrzési kivételekkel.

A műszaki előzmények időablakai kiszolgálóoldali alapértékek; az éles konfiguráció és a takarítófeladat működése határozza meg a tényleges végrehajtást. Szerződéses követelmény esetén a konkrét adatkörre érvényes megőrzést írásban kell rögzíteni.

Mentés és visszaállítás. Az adatfeldolgozási megállapodás 9.3 pontja szerint az adatbázisról naponta automatikus, titkosított mentés készül az EU-n belül, hét napra visszamenőleg időpont szerinti visszaállítással (PITR) és heti teljes exporttal; a mentéseket legfeljebb 42 napig őrizzük. A helyi adatsor nem felhőmentés. Saját archiválásra export használható; külön RPO/RTO-vállalás csak kifejezett megállapodással tekinthető biztosítottnak.

Aktiválás, távoli műveletek és frissítés

Aktiválás kóddal és jóváhagyással

Telepítés után az ügynök ABCD-EFGH aktiválási kódot mutat; ez 60 percre érvényes, és legfeljebb 7 napig automatikusan megújul. Az `agents.create` jogosultságú PrinterMS-felhasználó az **Hálózatok** → **Új ügynök** menüben a gépnév, a verzió, a forrás-IP és az észlelt alhálózatok alapján elutasítja a kérést, vagy új vagy meglévő hálózathoz rendeli a gépet. Hibás kódra felhasználónként 15 percenként 10, szervezetenként óránként 30 próbálkozás jut.

A rövid kód nem jogosít tokenet kérni: az eszköztokent csak a külön, 256 bites privát eszközkód birtokosa veheti át. A token gépi API-hozzáférés, nem felhasználói munkamenet; visszavonható és rotálható. Az ügynök kijelzi, hová csatlakozott; bekapcsolt értesítéseknel a jóváhagyásról biztonsági e-mail megy.

Telepítési link: az `agents.create` jogosultságú felhasználó szervezethez, ügyfélhez és hálózathoz kötött, legfeljebb 30 napig és 1–10 telepítésre érvényes, visszavonható linket vagy e-mail-kampányt készíthet. A 128 bites tokenből a szerver SHA-256 lenyomatot és az újraküldéshez titkosított másolatot tárol. Érvényes tokennel a kérés a kötött hálózatra automatikusan jóváhagyódik; az eszköztokent ekkor is csak a 256 bites eszközkód veszi át, a Setup a tokenet nem menti el, elutasított tokennél kódos aktiválás jön. Minden használatról e-mail megy, a napló rögzíti; a Windows Setup csak olvasható „PrinterMS Ügynök állapota” parancsikont tesz fel.

A felhőből közölhető műveletek

Művelet	Hatás és korlát
Konfiguráció	Címtartományok, leolvasási ütem, gyűjtési kategóriák, aktív/tartalék szerep; WSD és helyi USB-csatlakozó engedélyezése. A felhős címlista csak a 09. fejezet B1 és B2 szabályán belül érvényes.
Azonnali lekérdezés	Felderítés, számláló-, kellék- vagy állapotlekérdezés. A feldolgozó csak előre meghatározott parancsneveket fogad; nincs tetszőleges shellparancs vagy feltöltött szkript.
Eszköztámogatási beolvasás	Csak egy <code>agents.edit</code> jogosultságú felhasználó tájékoztatás utáni, kifejezett kérésére, egy már felderített nyomtatóra. Ha a Tulajdonos külön belépett az (alapból kikapcsolt) eszköztámogatási programba, a PrinterMS éjszaka (20:00–06:00) ütemezhet beolvasást az elmúlt 48 órában látott nyomtatókra, futásonként legfeljebb tízet, típusonként és firmware-verzióként az összes ügyfél között legfeljebb egyet. Az ügynök egyszer, lassítva, nyomtatás közben nem, legfeljebb 5 percig olvassa a beépített MIB-ágakat. Nem olvassa a nyomtatási naplót, a címjegyzéket, a felhasználókat és a hálózati táblákat. A gyári számot, az IP- és MAC-címeket, az e-mail-címeket, a gépneveket, a telefonszámokat és a hosszú szövegeket helyben kitakarja (09, F6), a szerver ezt újraellenőrzi.
Helyi korlátozások	A scanless, az IPP teljes tiltása, a helyi managed frissítési mód és a <code>support.device_walks: disabled</code> (vagy <code>DCA_DEVICE_WALKS=disabled</code>) korlátot jelent a kapcsolódó műveletekre. A beolvasás tartalma előre, helyben megnézhető: <code>printerms-agent --walk-device <nyomtató-IP> --walk-out <új fájl></code> ugyanazt írja helyi fájlba, és semmit nem küld el.
Token és leszerelés	Tokenrotáció, visszavonás és távoli öneltváltoztatás. A leszerelés a telepítéskor létrehozott, korlátozott feladatú privilegizált segédet használhatja.
Lekérdezési definíció	Önállóan aláírt, korlátozott adatformátum módosíthatja a támogatott kiolvasási szabályokat. Nem adhat végrehajtható kódot, általános szkriptet vagy új hálózati célcímeket.

Az utasításokat az ügynök a saját HTTPS-kérésének válaszában kapja. Offline gépen nem hajtódnak azonnal végre. A helyi naplók műveleti eseményeket tartalmaznak; a felhőből indított változásokat a szervezet naplója rögzíti (09, B3).

Programfrissítés és kiadási bizalom

Frissítési mód: a PrinterMS szervezeti vagy hálózati beállítása dönt, ezt követi az új telepítés `updates.mode: automatic` módja. Az IT parancssorból szigoríthat: `updates.mode: approval` mellett csak kérésre, `managed` mellett soha nem települ kiadás. Minden önfrissítéshez legalább két aláírás és 24 óra várakozás kell (09, A1, A3, A4).

Natív Windows Setup: a cserét egy külön LocalSystem jogosultságú natív folyamat végzi, amely ellenőrzi a manifest aláírását, az SHA-256 azonosítót és a rögzített PrinterMS Authenticode-azonosságot. A csere után hitelesített állapotjelentést vár, hibánál visszaállítja az előző binárist; PowerShellt nem használ.

Más natív utak: ugyanígy ellenőriznek és visszaállítanak; széles éles használatuk nem igazolt.

Docker: a konténer saját képét nem írja át, az új képet az IT telepíti; a `managed` mód csak a programcserét tiltja.

Végpontvédelem. Az aláírás ellenőrizhető eredetet ad, nem helyettesíti az EDR-szabályokat; kivétel csak igazolt kiadáshoz vagy pontos hashhez és szűk útvonalhoz tartozzon. A VirusTotal csak a nyilvános kiadási fájlokat kapja, ügyféladatot nem.

Fenyegetések és beépített védelmek

Az alábbi táblázat azokat a hiba- és visszaélési helyzeteket sorolja fel, amelyek ellen az ügynök és a PrinterMS felhő kódszinten véd, a védelem hatáiraival együtt. A sorazonosítók állandók, így a jóváhagyási jegyzőkönyv hivatkozhat rájuk. A harmadik oszlop azt mutatja, mit állíthat be helyben az IT, és milyen kockázat marad.

Fenyegetés	Beépített védelem	Helyi beállítás és maradó kockázat
B1 · Felhős címlista Hibás vagy jogosulatlan felhős beállítás az SNMP-lekérdezéseket, a titkosítatlan v1/v2c community-vel együtt, internetes címre, a gazdagépre vagy felhős metaadat-szolgáltatásra irányítja.	A felhőből csak magánhálózati (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16), CGNAT (100.64.0.0/10) vagy IPv6 ULA (fc00::/7) cím vagy tartomány adható meg, tartományonként legfeljebb 65 536 címmel: IPv4 esetén legalább /16, IPv6 esetén legalább /112 előtaggal. Nem adható meg nyilvános cím, loopback (127.0.0.0/8, ::1), link-local (169.254.0.0/16, fe80::/10), felhős metaadat-cím (169.254.169.254, 100.100.100.200, fd00:ec2::254) vagy azt tartalmazó tartomány, multicast, broadcast és 0.0.0.0/8. A szerver az új felhős bejegyzést elutasítja, a telepítő által javasolt tartományok közül a nem megengedetteket elhagyja. Az ügynök a kapott listára ugyanezt a szabályt alkalmazza: a nem megengedett elemet kihagyja és jelenti; ha semmi sem marad, a helyi engedélyt használja.	Nyilvános tartomány csak helyben, az agent.json cidrs mezőjében adható meg; ez az IT kifejezett döntése. A korábban tárolt, már nem megengedett felhős bejegyzés megmarad, és más módosítást nem akadályoz; a hálózat oldala jelzi, és egy lépésben eltávolítható. A szabályt még nem ismerő régebbi ügynök ezt a bejegyzést továbbra is használja, ezért érdemes eltávolítani.
B2 · Helyi korlát A felhős lista a helyileg jóváhagyottnál szélesebb hálózatot pásztáztat, felhőből bekapcsolja a WSD-t vagy a helyi USB-csatlakozót, vagy egy korábban megismert, azóta hatókörön kívüli nyomtatót tovább kérdeztet.	Az agent.json remote_config.scan_ranges mezője (vagy a DCA_REMOTE_SCAN_RANGES környezeti változó) korlátozza a felhős listát. open (alapérték): a B1 szabálynak megfelelő felhős lista érvényes. bounded: csak a helyi cidrs által, üres lista esetén a gép saját hálózatai által lefedett felhős elemek. locked: egyetlen felhős tartomány sem, csak a helyi engedély. Minden nyomtatói kapcsolat (felderítés, számláló-, kellenk- és állapotlekérdezés, eszköztámogatási beolvasás) egyetlen hatókör-ellenőrzésen megy át, a már ismert nyomtatóknál is: a hatókörön kívüli nyomtató nem kap kérést, és kikerül a nyilvántartásból. Az ügynök jelenti a módot, a kihagyott tartományokat és a kívül eső nyomtatók számát; a webes felület ezeket a hálózat oldalán mutatja.	Az alapérték open, ezért a korlátot az IT-nak kell beállítania; a módosítás a szolgáltatás újraindítása után érvényes. bounded és locked módban a felhő a WSD-t és a helyi USB-csatlakozót nem kapcsolhatja be, csak ki. Munkamegosztásos hálózaton egy nyomtatót csak akkor olvas az ügynök, ha a szerver által kiosztott munkakör és a helyi korlát is lefedi. A gépen belüli IPP-over-USB csatlakozóra a hatókör nem vonatkozik.

Fenyegetés	Beépített védelem	Helyi beállítás és maradó kockázat
C1 · Számlálóugrás Téves leolvasás vagy manipulált nyomtató egyetlen leolvasásban, egy nap sok kis lépésében, vagy egy olyan leolvasás után, amelyből a számláló hiányzott, valószerűtlenül nagy számlálónövekedést jelent, amely díjként kerülne a számlára.	A Platform csomagban a szerver minden ügynökleolvasást mér az eszköz előző állásához, és minden számlázott számlálót (fekete-fehér, színes, szkennelés) a saját utolsó ismert értékéhez: a legutóbbi olyan korábbi napi ügynökleolvasáshoz, amely tartalmazza, visszamenőleg addig a leolvasásig, amelyhez a számlázás méri (a legutóbb számlázott, kiszállításkori vagy beszerzési leolvasás). Ha a nyomtató számlázása az ügynökön alapul, minden számlálót ehhez a számlázási leolvasáshoz is mér, és ez pótolja a hiányzó vagy régebbi utolsó ismert értéket, így az ugrást akkor is visszatartja, ha a nyomtató első ügynökös napjára vagy e leolvasás napjára esik, vagy ha később korábbi dátummal rögzítenek kiszállításkori vagy beszerzési leolvasást. Ha egy számláló az előző álláshoz képest eltelt naponként (legalább egy napra vetítve), vagy az utolsó ismert értékéhez, illetve a számlázási leolvasáshoz képest naptári naponként több mint 20 000 oldallal nő, az eszköz számlálóit visszatartja (<code>counter_jump</code>): amíg egy <code>readings.financial.manage</code> és <code>printers.edit</code> jogosultságú felhasználó a nyomtató oldalán, megerősítés után nem dönt, nem keletkezik leolvasás és nincs számlázás. <i>Új alapérték:</i> a következő leolvasás díj nélküli kiindulópont. <i>Számlázás a mért értékkel:</i> a következő leolvasást csak az előző álláshoz méri, és a legutóbb számlázott álláshoz mérve, az ugrással együtt számlázza; az aznapi későbbi leolvasások nem tárolódnak, a következő napot ehhez méri. Bármelyik döntés után a leolvasásokat a később rögzített számlázási leolvasáshoz, korábbi dátummal is, ismét méri, és a döntés hatása megszűnik, ha az eszközt másik nyomtatóhoz rendelik vagy leválasztják. A számlálóértelmezés változásából eredő törést (<code>counter_rule</code>) minden csomag visszatartja, és csak új alapértékkel oldható fel.	A határ nem állítható, így egy valós, kiugróan nagy nyomtatási nap is visszatartást okoz. A más forrásból, például e-mailes számlálójelentésből számlázott nyomtatót nem a számlázási leolvasáshoz, csak a saját ügynökleolvasásaihoz méri, mert az a forrás másképp számolhat; az általa kihagyott hónapot számlázó ügynökleolvasás csak akkor számlázódik, ha a számlázási leolvasáshoz képest ezen a határon belül marad. Az ügynökleolvasásokat, amelyek akkor tárolódtak, amikor a nyomtatót más forrásból számlázták, utólag sem méri a számlázási leolvasáshoz, ha a nyomtató számlázását később az ügynökre állítják. Döntés után a leolvasásokat nem méri ahhoz a számlázási leolvasáshoz, amely a döntést követő első leolvasás tárolásakor már megvolt, és nem későbbi dátumú annál. Értelmezésváltozás nélküli csökkenést nem tart vissza, a számlázás új kiindulópontként kezeli. A PrinterMS Monitorban az ügynök leolvasása nem számlázódik, ott nincs ugrás-visszatartás. A védelmet a PrinterMS üzemzavar esetén ideiglenesen kikapcsolhatja; a meglévő visszatartások ekkor is megmaradnak.
D1 · Eszköztápvétel Egy tartalék vagy idegen csomópont, vagy egy másik hálózat ügynöke ugyanazt a nyomtatót jelenti, és a saját számlálóival átveszi vagy megkettőzi a számlázott sort.	Hálózaton belül az eszköz ahhoz a csomópontához kötve marad, amelyik jelentette. Másik csomópont csak akkor veszi át, ha aktívra állított vagy az aktív helyet tartja, és a megfigyelése nem régebbi, vagy ha az eddigi csomópont már nem aktív (például visszavonták). Más csomópont jelentéséből az azonosító-, kellék- és állapotadat frissül, a számláló nem tárolódik és nem számlázódik. A Platform csomagban, ha a nyomtatót már egy másik hálózat eszköze számlálja, az új eszköz nem kapcsolódik hozzá, és a felület megnevezi a számláló hálózatot; az összekapcsolás (<code>agents.edit</code> és <code>printers.edit</code>) ugyanabban a lépésben leválasztja a másik hálózat eszközét.	Az aktív szerep kiosztása (<code>agents.edit</code>) továbbra is áthelyezheti a számlálást. Átfedő címtartományú hálózatoknál a második hálózat eszközei összekapcsolatlanul jelennek meg. A PrinterMS Monitor ütközéskezelése változatlan. A védelmet a PrinterMS üzemzavar esetén ideiglenesen kikapcsolhatja.
E4 · Aktiválási kód a naplóban Egy hibajegyhez csatolt, naplójújtóbe továbbított vagy más által olvasható naplóból egy harmadik fél kiolvassa a még érvényes aktiválási kódot, és a saját PrinterMS-fiókjában hagyja jóvá a gépet.	Az ügynök és a Windows Setup naplóbejegyzései (például <code>agent.log</code>) a kódot csak kitakarva tartalmazzák (<code>AB**_****</code>): az első két karakter marad, a kód többi része és hossza nem. A teljes kódot csak a kezelőnek szóló kijelzés mutatja: a konzolüzenet, a <code>--activation-code</code> parancs, a helyi aktiválási állapottájl és a Setup ablaka. A kód 60 percig érvényes; jóváhagyás után az ügynök kijelzi, melyik szervezethez csatlakozott.	A konzolüzenet a szolgáltatás szabványos kimenetére kerül, ezért Linuxon a <code>systemd</code> -naplóban, Dockerben a konténer kimenetében a teljes kód olvasható; ezekhez a hozzáférést korlátozni kell. A korábbi ügynökverziók naplói a teljes kódot tartalmazhatják.
F1 · SNMP-visszaesés A v3-ra beállított ügynök v2c vagy v1 próbálkozással titkosítatlanul küldi a <code>community</code> -t, akár a gyári <code>public</code> értéket, vagy gyenge, MD5- vagy DES-alapú v3-hitelesítőt használ.	Az <code>snmp.min_version</code> a legalacsonyabb kipróbált verzió. <code>v3</code> : csak v3, <code>community</code> nem kerül a hálózatra. <code>v2c</code> : v1 nem. Egy ismert nyomtatót a minimum alatti, korábban tárolt útvonalon sem kérdez le. A <code>public</code> csak megadott <code>community</code> hiányában és v1 vagy v2c engedélyezése mellett használatos. MD5- vagy DES-alapú v3-hitelesítővel a konfiguráció nem töltődik be, kivéve <code>snmp.allow_weak_v3_crypto: true</code> esetén. Az ügynök mindkét beállítást jelenti a felhőnek.	Az alapérték <code>v1</code> , ezért a szigorítást az IT-nak kell beállítania. <code>v3</code> esetén <code>snmp.v3</code> felhasználónév nélkül az ügynök egy nyomtatót sem olvas, csak az állapotjelzést küldi. A <code>v1/v2c</code> forgalom titkosítatlan marad; a régebbi verziókat a nyomtatón és a hálózaton is érdemes korlátozni.

Fenyegetés	Beépített védelem	Helyi beállítás és maradó kockázat
F6 · Szabad szöveg a beolvasásban A nyomtatónak adott név, vagy egy gyártói mezőbe beírt név, részleg vagy megjegyzés az eszköztámogatási beolvasással a PrinterMS-hez kerül.	Az ügynök a beolvasásból elhagyja a nyomtató saját nevét (<code>prtGeneralPrinterName</code>), a rendszerkapcsolati, hely- és kezelőmezők mellett. A gyártói ágakban minden 16 bájtnál hosszabb szöveget helyben <code><redacted text len=N></code> alakra cserél, kivéve a számot, a pontozott verziószámot és a hexadecimális számjegyeket; a gyári szám mezői és a hexadecimálisan megtartott számértékek kivételek. A megtartott érték is átmegegy a cím-, gyáriszám- és elérhetőségszűrőn. A szerver a feltöltést újraellenőrzi.	A szabványos ágak szövegei és a legfeljebb 16 bájtos gyártói szövegek (például kellékanyag-megnevezések) megmaradnak. A korábbi ügynökvérziók a nyomtató nevét is feltölthetik. A beolvasás előre megnézhető (<code>--walk-device</code>) és helyben tiltható (<code>support.device_walks: disabled</code>).
A7 · Leszerelés és törlés Egy felhasználó felhatalmazás nélkül leszerel vagy töröl a felhőből egy hálózatot vagy csomópontot, és ezzel leállítja a nyomtatók számlálóinak gyűjtését.	A hálózat vagy a csomópont leszerelése és kényszerített törlése az <code>agents.delete</code> jogosultsághoz kötött; nélküle a szerver 403-as hibával elutasítja, és a felület fel sem kínálja. A Technikus alapsablonja ezt a jogosultságot nem tartalmazza, megadni csak a Tulajdonos tudja. Minden leszerelési kérés és törlés a szervezet naplójába kerül (B3).	A Tulajdonos a jogosultságot sablonnal más tagnak is megadhatja; ez szándékos átruházás. Helyi rendszergazdai joggal a szolgáltatás a gépen a felhő nélkül is leállítható vagy eltávolítható.
B3 · Nyomon nem követhető változás Egy hálózati beállítás, utasítás, aktiválás, visszavonás vagy számláló-visszatartás feloldása után nem deríthető ki, ki és mikor változtatott.	A felhő az ügynökhálózatok minden változását (beállítás és frissítési szabály, utasítás, aktiválás és elutasítás, visszavonás, leszerelés és törlés, tokencsere, eszköz-hozzárendelés, számláló-visszatartás és feloldása) a változással egy tranzakcióban a szervezet naplójába írja: időpont, végrehajtó (felhasználó, ügynök vagy rendszer), hálózat és csomópont. A bejegyzés nem módosítható, és amíg a szervezet létezik, nem törölhető; a törölt hálózatok és csomópontok bejegyzései megmaradnak. Token, kód, community és jelszó nem kerül bele. A Hálózatok oldal és a hálózat oldala Napló részén <code>agents.view</code> jogosultsággal olvasható.	A napló a felhőből indított változásokat rögzíti; a helyi <code>agent.json</code> módosítását és a gépen végzett műveleteket nem, ezekre a gép saját naplói szolgálnak. A bejegyzések a szervezettel együtt törölődnek.
C3 · Aktiválási kérésáradat Egy támadó tömegesen indít névtelen aktiválási kérést, hogy elfogyassza a várakozó kérések keretét, és a valódi telepítések ne tudjanak aktiválódni.	A névtelen aktiválási végpontok hívócímenként (IPv6-on / 64-enként) percenként 10 kérést fogadnak. A számlálás közös adatbázisban történik; ha az nem érhető el, a szerver a kérést elutasítja (429, újrapróbálás egy perc múlva), nem engedi át. Egy forráshálózatról (IPv4 / 24, IPv6 / 48) egyszerre legfeljebb 20, a szolgáltatásban összesen 5000 kérés várhat. 2500 várakozó kérés felett az új kód 60 helyett 15 percre érvényes. Az ügynök elutasítás vagy lejárta után magától újrapróbálkozik, és jóváhagyás nélkül egyik kérés sem kap hozzáférést.	Közös kilépési címről (NAT, CGNAT) vagy egy / 24-es hálózatról egyszerre legfeljebb 20 gép várhat jóváhagyásra, a többi később kap kódot. A korlátszámláló kiesése alatt nem indul új aktiválás. Sok forráshálózatról érkező áradat az egész szolgáltatásban késleltetheti az új aktiválásokat; a már aktivált ügynököket nem érinti.
C4 · Lecserélt token Egy klónozott, visszaállított vagy elloptott gépen maradt régi eszköztoken a tokencsere után is hozzáfér a PrinterMS-hez.	Tokencserénél a régi token akkor veszíti el érvényét, amikor az ügynök először jelentkezik az újjal, ezzel igazolva, hogy elmentette; addig a régi működik, így a csere nem zárhatja ki az ügynököket. A lecserélt token minden későbbi használata 401-es elutasítást kap. Ha a csere óta több mint 10 perc telt el, a szervezet naplójába <code>node.token_stale_use</code> esemény kerül (csomópontonként óránként legfeljebb egy), és a szerver figyelmeztetést naplóz. Visszavonás és leszerelés után a csomópont egyik tokenje sem érvényes.	A tokencserét és a visszavonást <code>agents.edit</code> jogosultságú felhasználó indítja. Az aktuális token másolatát a szerver nem különbözteti meg az eredetitől; gyanú esetén cserélni vagy visszavonni kell. Az eseményről külön e-mail nem megy.
A6 · Telepítőparancs A rövid telepítőparancsot kiszolgáló <code>agent.printerms.com</code> vagy annak frissítési folyamata idegen lenyomatot, gyengébb Windows-ellenőrzést vagy más aláíró-t ír az indítószkriptbe, és a gép rendszergazdaként idegen programot futtat.	Az éles indítószkript Windows alatt csak a PrinterMS Authenticode-aláírását fogadja el, rögzített aláírásonossággal; a csak SHA-256-alapú ellenőrzés a tesztkörnyezetre korlátozódik, más beállítással az éles kiszolgáló nem ad ki szkriptet. Az éles kiszolgáló a megadott lenyomatokat csak az adott kiadás <code>agent-release.yml</code> kiadási folyamatától fogadja el, annak tesztkörnyezeti ellenőrzése és védett jóváhagyása után; kézi frissítéskor a legutóbbi kiadásból számítja ki őket. Minden lenyomatot a kiadás letöltött fájljaihoz mér, mielőtt élesít.	Az indítószkriptet és a benne lévő lenyomatokat ugyanaz a kiszolgáló adja, ezért a tőle független ellenőrzés a kiadás aláírt <code>checksums.txt</code> fájlja: <code>cosign verify-blob</code> a GitHub-kiadásból letöltött <code>checksums.txt.sig</code> és <code>checksums.txt.pem</code> fájljal, az <code>agent-release.yml</code> folyamat adott kiadáshoz kötött azonosságára. Az ellenőrzés bármely internetet elérő munkaállomáson futtatható; a gyűjtőgépnek nem kell a Sigstore-t elérnie.

Fenyegetés	Beépített védelem	Helyi beállítás és maradó kockázat
A1 · Frissítési mód Egy új kiadás az IT döntése nélkül, egyszerre települ minden gépre.	A PrinterMS szervezeti vagy hálózati beállítása dönt, az új telepítés helyi <code>automatic</code> módja ezt követi: automatikus beállításnál az ellenőrzött kiadás kérés nélkül, a 24 órás várakozás (A3) után települ, <code>managed</code> beállításnál csak egy <code>agents.edit</code> jogosultságú tag kérésére. A helyi és a felhős mód közül a szigorúbb érvényes.	A döntés a felhőben van; a fiók feltörése ellen A3 és A4 véd. Független helyi korlátot csak az IT állít parancssorból: <code>--update-mode</code> vagy <code>DCA_UPDATE_MODE</code> (<code>approval</code> , <code>managed</code>); az alkalmazás jelzi, ha ez szigorúbb. <code>approval</code> módban a gép rendszergazdája is jóváhagyhat (tálcaikon, UAC, napló).
A3 · Azonnali kiadás Egy feltört kiadási folyamat aláírt, de hibás vagy rosszindulatú kiadása a felfedezése előtt eléri a gépeket.	Az ügynök egy kiadást az aláírt kiállítási idő és a gépen történt első ellenőrzés közül a későbbi után 24 órával tölt le és telepít, így visszadátumozás vagy újraindítás nem rövidíti. Addig <code>soak_waiting</code> állapotot és a várakozás végét jelenti, a felület „Biztonsági várakozás” állapotot mutat. Ezalatt a PrinterMS a kiadást leállíthatja.	A várakozás sürgős javításra is vonatkozik; hibás új verzióval az egészségellenőrzéshez kötött visszaállítás véd. A Docker-képet az IT cseréli, ott nincs várakozás.
A4 · Aláírókulcs Egyetlen ellopott vagy visszaélésre használt aláírókulcs futtatható programot hagy jóvá a gépeknek.	A frissítési jegyzéket legalább két független kulcs aláírása hitelesíti: az ügynök, a bizalmi gyökeret készítő eszköz és a kiadási ellenőrzés elutasítja a 2-nél kisebb küszöböt, ilyen gyökérrel az ügynök nem frissít. A privilegizált segéd telepítés előtt újra ellenőrzi az aláírásokat és a fájl lenyomatát.	A küszöb csak akkor jelent két független döntést, ha a kulcsokat külön személyek vagy rendszerek kezelik. A két kulcs ma egy felhős projektben, egy tulajdonosi azonosság alatt van; szétválasztásuk a PrinterMS tervezett feladata.
E1 · Eszköztoken a lemezen Lemezképből, mentésből vagy a gépről másolt eszköztokennel valaki az ügynök nevében küld adatot vagy kap utasítást.	Windows alatt a token gépszintű DPAPI-védelemmel tárolódik (<code>dpapi:v1</code>): a friss Setup így írja, a meglévő telepítés az aktuális Setup futtatása után, az első hitelesített jelentkezéskor, frissítési tranzakción kívül alakítja át. Linux, macOS és Docker alatt a token 0600-as fájl, csak a szolgáltatásfiók és a root olvassa. Az ügynök jelenti a tárolás módját (<code>token_storage</code>); a másolt tokent tokencsere vagy visszavonás érvényteleníti (C4).	A DPAPI a gépről elvitt másolat ellen véd, a helyi rendszergazda vagy SYSTEM jogú kód ellen nem. Az <code>install.ps1</code> -gyel telepített vagy régebbi Setupról csak önfrissített gép a sima fájlt tartja meg, amíg az aktuális Setup nem fut. A lemeztitkosítás az IT feladata.
E2 · Root jogú gyűjtő macOS-en A nyomtatók válaszait feldolgozó gyűjtő egy hibáján át a támadó root jogosultsággal futtat kódot a Macen.	Az <code>install.sh</code> a macOS-gyűjtőt a rejtett, bejelentkezésre nem használható <code>_printerms</code> fiókkal futtatja (500 alatti rendszerazonosító, <code>/usr/bin/false</code> héj). A root tulajdonú <code>agent.json</code> fájlt csak olvassa, írni csak a saját <code>Data</code> könyvtárába tud. A frissítést és a távoli leszerelést külön root LaunchDaemonok végzik: csak root vagy e fiók fájljait fogadják el, a törölt útvonalakat root tulajdonú fájlokból veszik, frissítést csak saját root könyvtárban ellenőrzött másolatból telepítenek.	A meglévő Mac az <code>install.sh</code> újbóli futtatásakor vált át (a macOS-ügynök nem frissül magától); addig a gyűjtő root jogosultsággal fut. A root segédek kiemelt jogú kódok maradnak, a helyi rendszergazda az ügynököt módosíthatja. Windows, Linux és Docker alatt a gyűjtő eddig is rendszergazdai jog nélkül fut (05).
G1 · Felhőkapcsolat Egy módosított beállítás, egy átirányítás vagy egy közbeékelődő hálózati eszköz az eszköztokent és a mérési adatokat idegen kiszolgálóhoz juttatja.	A <code>server_url</code> csak a <code>printerms.com</code> tartomány címe lehet, különben a konfiguráció nem töltődik be; eltérni csak helyben, az <code>allow_custom_server_url</code> beállítással vagy a <code>DCA_ALLOW_CUSTOM_SERVER_URL=1</code> változóval lehet, a felhőből nem. Az ügynök az API átirányítását soha nem követi, legalább TLS 1.2-t használ, és a tanúsítványt az OS bizalmi tárával ellenőrzi. A megadott <code>proxy_url</code> (vagy <code>DCA_PROXY_URL</code>) minden felhőkérésre érvényes, és megelőzi a <code>HTTPS_PROXY</code> , <code>HTTP_PROXY</code> és <code>NO_PROXY</code> változókat. <code>strict_tls</code> módban csak a <code>proxy_url</code> számít, és a <code>server_url</code> kiszolgálójának tanúsítványláncában szerepelnie kell egy <code>server_spki_sha256</code> kulcsnak.	Alapértelmezésben nincs kulcsrögzítés, és <code>proxy_url</code> nélkül a környezeti proxyváltozók érvényesek. <code>strict_tls</code> mellett vállalati TLS-vizsgálat csak a vizsgáló tanúsítványkiadó kulcsának rögzítésével működik, és kulcscserekor a rögzítést frissíteni kell. A frissítési fájlok kiszolgálóját a rögzítés nem érinti, azokat az aláírás védi (A4). A régebbi ügynökverziók ezeket a szabályokat nem ismerik.
G2 · Biztonsági kapcsolat Aki sebezhetőséget talál az ügynökben vagy a PrinterMS felhőben, nem tudja, hová jelentse, ezért a hiba nyilvánosságra kerül, mielőtt a PrinterMS javíthatná, vagy el sem jut hozzá.	A <code>https://www.printerms.com/.well-known/security.txt</code> fájl (RFC 9116) megadja a bejelentési címet (support@printerms.com), a magyar és az angol nyelvet, és a Biztonság oldal „Sebezhetőség bejelentése” részére mutat. A szabály: a bejelentő bizalmasan, e-mailben jelez, a PrinterMS 5 munkanapon belül visszaigazol, és a részletek a javításig, de legfeljebb 90 napig nem kerülnek nyilvánosságra.	A bejelentések az ügyfélszolgálati postafiókba érkeznek; külön biztonsági cím és díjazott hibakereső program nincs. A fájl lejárat dátumát a PrinterMS évente megújítja.

A tűzfalszabály minden sornál független, ügyféloldali korlát marad.

Üzemeltetési ellenőrzés és eltávolítás

Jóváhagyáskor rögzítendő

A gazdagép és felelőse; a telepített verzió és kiadási SHA-256; a jóváhagyott nyomtató-IP-k/CIDR-ek; a felhős címlista helyi korlátozási módja; az engedélyezett protokollok; a felhős módosításra jogosultak; a leolvasási ütem; a frissítési mód; a helyi adatkönyvtár védelme; a felhőbeli megőrzés és az eltávolítás felelőse.

Kapcsolat, proxy és működés ellenőrzése

- Kiadás:** a telepítő aláírását és SHA-256 azonosítóját a jóváhagyott kiadással összevetni. A kiadóhoz tartozó aláírás és a hash ellenőrzése külön lépés.
- API-elérés:** `curl.exe -fsS https://api.printerms.com/healthz` Windows alatt, más rendszeren `curl`. Ez a tesztfolyamat DNS/TLS/elérését igazolja; a szolgáltatását a sikeres hitelesített heartbeat bizonyítja.
- Proxy:** javasolt a `proxy_url` megadása az `agent.json` fájlban (vagy `DCA_PROXY_URL` a szolgáltatás környezetében); ez elsőbbséget élvez. Nélküle a szolgáltatás saját környezetének `HTTPS_PROXY`, `HTTP_PROXY` és `NO_PROXY` változói érvényesek; `strict_tls` mellett az ügynök ezeket figyelmen kívül hagyja. A felhő TLS-ellenőrzése az OS bizalmi tárárt használja, kulcsrögzítés csak `strict_tls` esetén van (09, G1); vállalati TLS-vizsgálathoz a szolgáltatás számára megbízható gyökértanúsítvány szükséges. A nyomtatói SNMP/IPP nem megy a webproxyn át.
- Nyomtató:** egy jóváhagyott eszköz gyári számát, számlálóját és állapotát összevetni a PrinterMS-ben látott adattal. Tűzfal/EDR-naplóval ellenőrizni a tényleges célokat és gyakoriságot.
- Folytonosság:** ellenőrizni az újraindulást, az adatsor ürülését és a kimaradásjelzést. CPU-, RAM-, lemez- és forgalmi értéket a tényleges flottával mérni; univerzális terhelési garancia nincs.

Azonnali helyi leállítás internet nélkül

A következő műveletek adminisztrátori jogosultsággal állítják le a gyűjtőt és tiltják annak szokásos automatikus újraindulását. Nem törölnek adatot és nem vonják vissza a felhőtokenet.

Windows (admin terminál)	<code>sc.exe config printerms-agent start= disabled</code> <code>sc.exe stop printerms-agent</code> <code>sc.exe query printerms-agent - az elvárt állapot: STOPPED.</code>
Linux	<code>sudo systemctl disable --now printerms-agent</code>
macOS	<code>sudo launchctl disable system/com.printerms.agent</code> <code>sudo launchctl bootout system/com.printerms.agent</code>
Docker	<code>docker update --restart=no printerms-agent</code> <code>docker stop printerms-agent</code> ; orchestrator esetén a kívánt példányszámot/újraindítást ott is módosítani kell.

Futó karbantartás és külső telepítésvezérlő külön is kezelendő. Incidensnél hálózati izolálás is alkalmazható. Visszaengedés előtt egyeztesse a helyi és felhős konfigurációt.

Teljes eltávolítás és adattörlés

Windows: Beállítások → Alkalmazások → PrinterMS Agent → Eltávolítás. A natív eltávolító szerveroldali tokenvisszavonást követel meg; ha ez nem igazolható, a telepítést megőrzi/visszaállítja az újrapróbáláshoz. Offline azonnali tiltáshoz a fenti leállítás használható. A programkönyvtár kézi törlése ne előzze meg az eltávolítót.

Linux/macOS/Docker: a token felhőbeli visszavonása után a szolgáltatás/csomag vagy konténer, valamint a konfiguráció és tartós adatkönyvtár/kötet eltávolítandó. Linuxon a sima csomageltávolítás adatot hagyhat; a teljes takarítás a csomag és telepítési mód szerint történjen. A helyi eltávolítás után a korábbi felhőadatok külön törlési eljárás alá tartoznak.

Dokumentumok és kapcsolat

[Adatfeldolgozási megállapodás](#) · [Alfeldolgozói jegyzék](#) · [Adatkezelési tájékoztató](#) · [DCA-feltételek](#) · [Szolgáltatói adatok](#)
Támogatás és biztonsági esemény: support@printerms.com · Adatvédelem: privacy@printerms.com