

KYOCERA FLEET SERVICES BIZTONSÁGI TANULMÁNY

v1.7 2018. november

A KFS folyamatosan fejlődik, így lehetséges, hogy a rendszerben lévő új funkciók - előzetes értesítés nélkül - a jelen tanulmány csak egy későbbi verziójában lesznek elérhetőek.

1 BEVEZETŐ



A mai hálózatos irodai környezetben a nyomtatók és multifunkciós készülékek távoli menedzsmentje költséghatékonyabb, mint valaha. A fejlett szoftveres eszközök az interneten keresztül gyűjtik be a készülékek műszaki adatait. A szolgáltató egy számítógép, laptop vagy mobil eszköz segítségével valós idejű adatokat lát a flotta működéséről lokálisan vagy globálisan.

Miért olyan fontos a távoli eszköz menedzsment? A folyamatos adatáramlás kihasználása bizonyított módja a flotta üzemelésének optimalizálására és drasztikusan növelheti a munkacsoport termelékenységét. Ezenkívül az eszköz technikai adataiból gyűjtött információk lehetőséget biztosítanak a szolgáltatónak, hogy gyorsan reagáljon az ügyfél jelenlegi és jövőbeni igényeire.

Az internet széleskörű használatát megelőzően az eszközfigyelés drága megoldás volt; dedikált telefonvonalak és egyedi szerver alkalmazások használata volt szükséges. A 21. század felhő alapú üzleti megoldásai nélkülözik az igen költséges helyi installációkat, mivel igény szerint osztják meg az

erőforrásokat az interneten keresztül. A sokoldalú, megbízható és biztonságos felhő alapú megoldások ma már igen elterjedtek és mindennaposak, mint a Dropbox™, a Google Drive™, az Apple® iCloud®. Ezek a fájlmegosztó és tárhely szolgáltatások hozzáférést kínálnak az értékes információkhoz bárhol, bármikor.

A KYOCERA Fleet Services (KFS) implementálásával ügyfeleinknek ezt a csúcstechnológiás felhő platform használatát kínáljuk, ahol a kiejtett eszköz elemzések és vezérlések egyszerűsítik a flottamenedzsment minden aspektusát. De hogyan fog ezekből az információkból profitálni az Ön szervezete? Biztonságos a rendszer? Ez a tanulmány választ ad a hasonló (és sok más egyéb) kérdésre, hogy jól informált legyen és megalapozott döntést hozzon a KFS bevezetéséről a cégénél.

A készülékekről begyűjtött technikai adatok segítségével a szolgáltató gyorsan tud reagálni az ügyfél jelenlegi és jövőbeni igényeire.

2 MI A KFS ÉS HOGYAN MŰKÖDIK?



A KFS egy felhő alapú eszköz monitorozó és menedzsment rendszer, mely szolgáltatott szoftver (Software as a Service - SaaS) modell alapon működik. Ezzel az üzleti megoldás modellel nincs szükség semmilyen szoftveres vagy hálózati infrastruktúra beruházásra. Ehelyett a biztonságos felhő szolgáltatások biztosítják az eszközöket a KFS szolgáltatóknak, hogy központilag kezeljék az eszközöket a telepítéstől kezdve a konfiguráláson át a riportolásig és a hibaelhárításig. A KFS hatékony eszköztára proaktív menedzsmentet biztosít a KYOCERA és a nem KYOCERA márkájú eszközöknek egyaránt bármilyen számítógép vagy okostelefon segítségével, amennyiben rendelkezik internet böngészővel. A kifinomult biztonsági protokolloknak és szabályoknak köszönhetően a KFS kommunikációja tökéletesen védett.

PROAKTÍV SZERVIZ MODELL

A KFS implementálásával „reaktív” helyett “proaktív” szerviz modell kialakítására nyílik lehetőség. A proaktív modell kulcsa a KFS email küldő funkciója, mely tájékoztatja a szerviz technikust az eszközön történő technikai eseményekről, rendszerhibákról, tonerszintről, számláló adatokról (az email küldést a készülék indítja). Az email-ben leírt esemény gyors reagálást és megoldást biztosít. Például ahelyett, hogy a felhasználó felhívna a szervizt egy hiba miatt (reaktív), az email értesítés alapján a szerviz technikus hívja fel a felhasználót (proaktív). Az

Számos esetben a szervizhívások megoldhatóak telefonon keresztül, minimalizálva az ügyfél munkafolyamatainak megzavarását és az állásidőt.

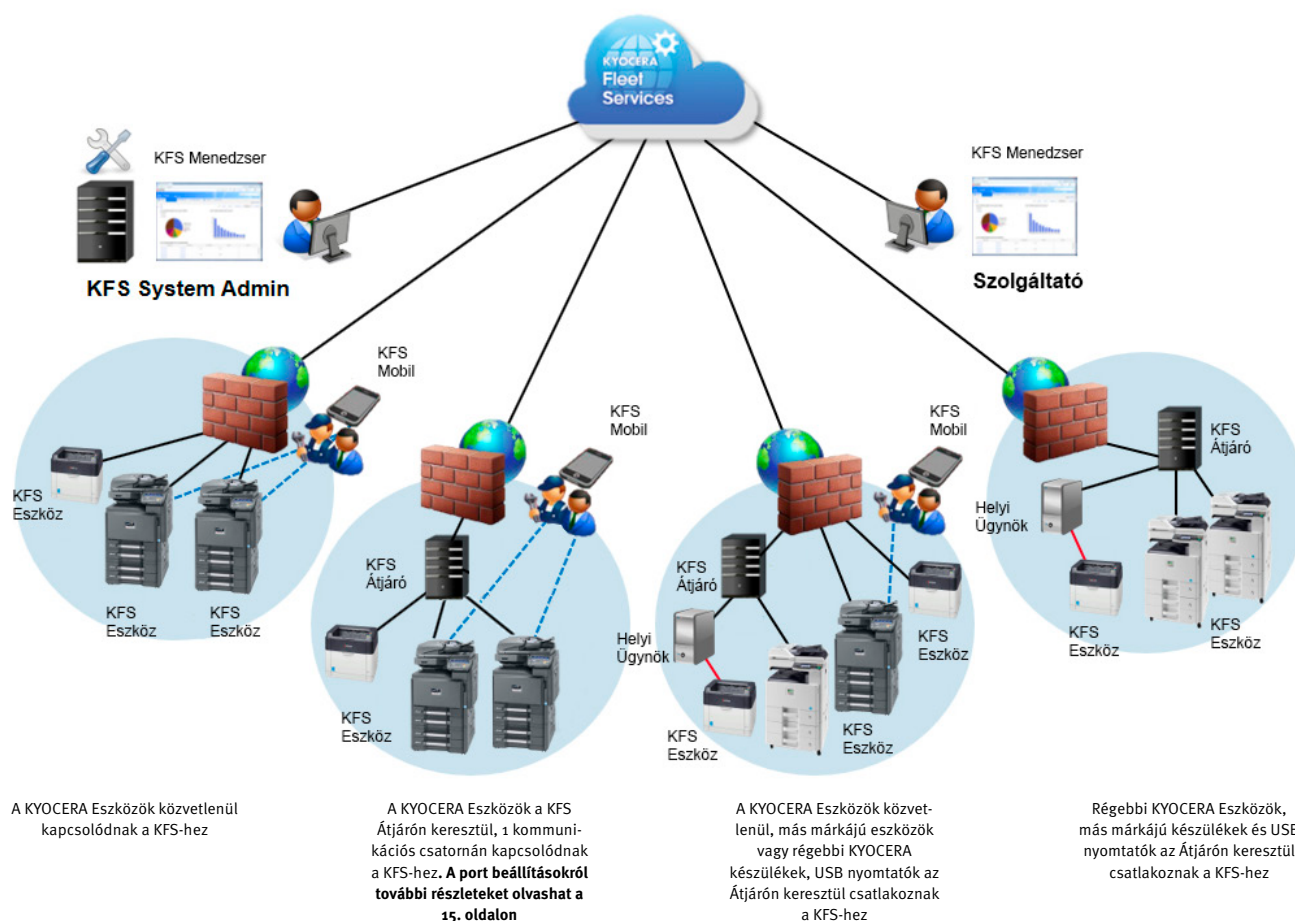
értesítés lehetőséget ad arra is, hogy a technikus a szükséges cserealkatrészekkel felkészülve érkezzen a helyszínre.

A humán erőforrások jobb kihasználásával a szolgáltató maximalizálhatja az eszközök rendelkezésre állását, csökkentheti az ügyfélnél a munkafolyamatok megszakadását, csökkentheti a helyszíni hibajavítások számát; számos esetben a szervizhívások megoldhatóak telefonon keresztül, minimalizálva az ügyfél munkafolyamatainak megzavarását és az állásidőt. Minél több eszköz és felhasználó van csatlakoztatva a rendszerhez, annál több információ áll rendelkezésre, így téve még kifinomultabbá a prediktív képességeket, ezzel segítve a vállalati hatékonyságot és a szolgáltatás szintű reakcióidő javulását.

A KFS négy fő komponensből áll – KFS Menedzser, KFS Eszköz, KFS Átjáró és KFS Mobil. Bár mind a négy komponens önálló feladatot lát el a KFS rendszerben, mindnek egy fő célja van... információt és eszközöket szolgáltatni a flotta problémamentes üzemeltetéséhez. Ezért ezek a komponensek lehetővé teszik a szolgáltatóknak, hogy optimalizálja a készülékek működését.

A KFS használatával számos gyártó eszközeinek széles paláttáját monitorozhatja. KYOCERA eszközökön a kiegészítő távoli karbantartás funkciók használata is lehetséges. Ezzel a KYOCERA a lehető legjobb üzleti megoldást tudja szállítani a vállalatok számára.

A KFS eszközállapot és használati adatokat gyűjt a készülék és a KFS Menedzser között lévő biztonságos kapcsolaton keresztül. A KFS Menedzser a KYOCERA Fleet Services gerince, ami a Microsoft® Azure® felhő rendszerben fut. A KFS Átjáró Windows-os környezetben telepíthető akár egy PC-re vagy egy szerverre az ügyfél informatikai környezetében. Az Átjárón keresztül lehetőség van egyetlen kommunikációs pont kialakítására is, ahogyan az 1. ábrán is látszik. A KFS Mobil egy mobil alkalmazás, mely a szolgáltató a szerviz technikusának telefonjára vagy tabletjére telepíthető.



1. ábra: Rendszer térkép – kapcsolódási lehetőségek a KFS-hez

KFS MONITOROZÁS

Az intuitív webes felület segítségével centralizált felügyeletet biztosít a fő rendszer funkciókhoz, az eszközök kihasználtságának monitorozásához, a hatékonyság növeléséhez **KYOCERA és más márkák** esetén.

- > Számláló állások és tulajdonságok
- > Grafikus és lista riportok
- > Toner szint ellenőrzés
- > Valós idejű monitorozás
- > Rendelési rendszer támogatás

KFS MENEDZSMENT

Az alábbi funkciók kizárólag **KYOCERA készülékek esetén** érhetőek el és a gyors távoli ügyféltámogatás révén növelik az elégedettséget.

- > Felhasználók, eszközcsoportok rögzítése, kezelése
- > Konfigurációs beállítások
- > Részletes készülék információk
- > Karbantartás / diagnosztika / hibaelhárítás
- > Készülék újraindítása (reboot)
- > Távoli firmware frissítés

1. táblázat: Főbb előnyök és funkciók



3 HOGYAN GARANTÁLJUK A BIZTONSÁGÁT?

Az IDC¹ legfrissebb előrejelzése szerint 2025-re a globális adatmennyiség a tízszeresére, 163 zetabyte-ra nő. Emellett a nyilvános felhőben tárolt adatok is a duplájára, 26%-ra nőnek, melyben egyre nagyobb arányban generálnak adatokat a vállalkozások. Ugyanakkor a becslések szerint egy átlag személy közel 4800 alkalommal lép kapcsolatba a csatlakoztatott eszközökkel naponta, ami 18 másodpercenként 1 interakciót jelent. Ebben az egyre növekvő adatintenzitású világban ezért rendkívül fontos az értékes információk védelme. Ezért a KFS számos robosztus biztonsági funkciót alkalmaz, melyek biztosítják a kommunikációt a KFS komponensek és az eszközök között.

BIZTONSÁGOS MICROSOFT® AZURE® HOSZTING KÖRNYEZET ÉS SZABÁLYOZÁSI MEGFELELÉS

A KFS Menedzser a Microsoft Azure²-ban van hosztolva, amely egy felhő alapú platform és kiemelten biztonságos szerver infrastruktúrát biztosít a KFS alkalmazások menedzselésére, a rosszindulatú kísérletek kivédésére, mint a distributed denial-of-service (DDoS) és a domain name system (DNS) támadások. Az Azure védelmét képezi annak folyamatos monitorozási folyamata és a folyamatosan fejlesztett behatolás tesztelése. Úgy tervezték, hogy ne csak a külső támadásoknak álljon ellen, hanem más Azure felhasználóktól érkező támadásoknak is. Belső DNS-t használ a belső virtuális gépek (VM) neveinek védelmére. A VM nevek a felhőszolgáltatáson belüli privát IP címekre oldódnak fel, folyamatosan fenntartva az adatvédelmet a felhőszolgáltatások között, még azonos előfizetés esetén is. A többféle biztonsági réteg mellett a Microsoft Azure teljes izolációt biztosít minden más hálózattól; a forgalom csak az ügyfél által konfigurált útvonalon folyik.

Az Azure a Microsoft iparágvezető adatvédelmi elkötelezettsége miatt került kiválasztásra. A Microsoft volt az első nagy felhő szolgáltató, amely bevezette az új nemzetközi felhő biztonsági standardot az ISO 27018-at. A Microsoft megfelel a nemzetközileg elismert információbiztonsági ellenőrzéseknek és az iparág specifikus szabványoknak, mint az ISO 27001, HIPAA, FedRAMP, SOC 1 és SOC 2, valamint az olyan ország specifikus szabványoknak, mint az ausztrál CCSL (IRAP), a brit G-Cloud és a szingapúri MTCS.

Független auditorok rendszeresen tanúsítják, hogy a Microsoft betartja ezeket az előírásokat az Azure infrastruktúra fizikai és virtuális vonatkozásainak tekintetében. Ennek eredményeként a KFS-t folyamatosan diagnosztizálják a webes alkalmazások tipikus sérülékenységeire, mint a privilege escalation, directory traversal, code injection, cross-site scripting, stb., valamint az alkalmazott tesztekkel feltárt sérülékenységek és más forrásokból származó jelentések is segítenek az alkalmazást biztonságban tartani.

2017 májusában a KYOCERA teljesítette a [Cloud Security Alliance \(CSA\) STAR Self-Assessment](#) önértékelését, mely az iparág leghatékonyabb programja a felhő biztosítására, mely magában foglalja az átláthatóságot, a szigorú auditok alapelveit és a szabványok harmonizációját. 2017 novemberében a KYOCERA befejezte az információbiztonsági rendszerének a tanúsítását (ISMS). Ez az önértékelés lekövetése az ISO 27001 információ biztonsági és az ISO 27017 felhő információ biztonsági szabványok szerint, mely magában foglalja harmadik fél által végzett tanúsítást is.

A KYOCERA folyamatosan figyelemmel kíséri a legújabb biztonsági trendeket és sebezhetőségi információkat. A KYOCERA a KFS fejlesztésekor követte az "Open Web Application Security Project (OWASP)" útmutatást. Szigorúan ellenőrizzük a lehetséges sebezhetőségeket így biztosítva a lehető legnagyobb biztonságot. A program kiadása előtt a biztonsági diagnosztika teszteket a KYOCERA mellett egy független szolgáltató is elvégzi.

1- D. Reinsel, J. Gantz, J. Rydning, "Data Age 2025: The Evolution of Data to Life-Critical", IDC biztonsági tanulmány, 2017 Április.

2- További információért olvassa el a Microsoft Azure Network biztonsági tanulmányát: <https://docs.microsoft.com/en-us/azure/security/abstract-azure-network-security> vagy látogassa meg a <http://azure.microsoft.com> weboldalt.



4 A KFS HASZNÁLATA ELŐTT

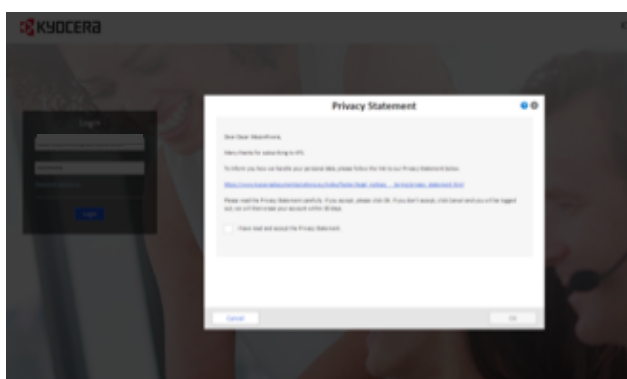


A KYOCERA eddig is kiemelt fontossággal kezelte az adatvédelmi jogszabályok betartását, azonban 2018 májusa óta az EU Általános Adatvédelmi Rendeletének (“GDPR”) hatálybalépésétől még ennél is nagyobb figyelmet szentel a területnek. A GDPR szigorította az adatkezelők és adatfeldolgozók kötelezettségeit és a szabályszegések bírságtételeit is növelte. Ez a KYOCERA és az ügyfeleinek munkájára és adatkezelési folyamataira is hatással van.

A KFS szoftver tulajdonosa a japán székhelyű KYOCERA Document Solutions Inc. (“KDC”). A KFS szoftver a felhőben fut, a szerverek az Európai Unió területén Amszterdamban, Hollandiában vannak. A KFS szoftver tulajdonosaként a KDC be tud jelentkezni a KFS szerverre és hozzáfér a felhasználói fiókok tulajdonosainak személyes adataihoz (név, e-mail cím, készülék IP cím). A KDC kizárólag a szolgáltatások működtetéséhez, támogatás nyújtásához vagy a felhasználó

kérése esetén használja a személyes adatokat. A KDC további adatfeldolgozókat használhat a KFS szolgáltatások ellátása érdekében. Az adatfeldolgozók listája megtekinthető a KYOCERA www.kyoceradocumentsolutions.eu weboldalon.

A KFS szolgáltatás tekintetében a KYOCERA adatfeldolgozóként vesz részt az adatkezelő nevében, aki az ügyfél. Az adatkezelő az a vállalat, amely felelős az adatkezelés céljának meghatározásáért, az adatfeldolgozó az a vállalat, amely kezeli a személyes adatokat az adatkezelő nevében. A teljes megfelelési biztosítása érdekében a KYOCERA a KFS felhasználóktól kéri az Adatkezelési Feltételek elfogadását. A KYOCERA adatkezelőként is kezelhet személyes adatokat pl. a szolgáltatásainak fejlesztése céljából. Erre az adatkezelésre a KFS Adatkezelési Nyilatkozat érvényes. Mindkét dokumentum elérhető a KYOCERA www.kyoceradocumentsolutions.eu weboldalon.



Privacy Statement

Last modified: 11 October 2017

We are KYOCERA Document Solutions Europe B.V., Bloemlaan 4, 2132 NP, Hoofddorp, the Netherlands and all subsidiaries in Europe, Middle-East and Africa. A complete list of the subsidiaries can be found [here](#).

In this privacy document we explain to you how we process your personal data.

First, we explain per Kyocera service for what purpose and on what legal ground(s) we process your personal data and who we involve. After, we explain on what legal basis we transfer your personal data to other countries, what your rights are towards us processing your personal data and how you can contact us.

- SERVICE - KYOCERA FLEET SERVICES
- SERVICE - WEBSITE CAMPAIGNS
- YOUR RIGHTS
- INTERNATIONAL TRANSFERS
- EXERCISING YOUR RIGHTS AND CONTACTING US
- CHANGES TO THIS DOCUMENT

2. ábra: Személyes adatok kezelése – a felhasználó beleegyezésének kérése. A teljes adatkezelési nyilatkozat elérhető a KDE EU weboldalon az a következő linken: https://www.kyoceradocumentsolutions.eu/index/footer/legal_notices_terms/privacy_statement.html



5 HOGYAN BIZTOSÍTJA A KFS AZ ADATVÉDELMI JOGAIT?

A KFS nem gyűjt, tárol vagy továbbít nyomtatási folyamatokban tárolt információt. A KFS kizárólag a flotta menedzsmenthez, karbantartáshoz szükséges készülék adatokat kezel biztonságos módon, nem azonosít és nem is továbbít személyekhez vagy csoportokhoz köthető adatokat amíg fel nem kéri rá az ügyfelek. A több-bérlős architektúra (multi-tenancy) alkalmazása miatt a viszonteladó és az ügyfelei adatai más viszonteladó vagy ügyfél által nem elérhetők.

A TÁROLT ADATOK VÉDELME

A KFS komponensekben, mint a KFS Menedzser, KFS Eszköz, KFS Átjáró és a KFS Mobil az adatok titkosítva vannak tárolva. A KFS Mobilban tárolt szenzitív adatok tartalmazzák a felhasználó KFS menedzser jelszavát, a frissítő token-t a KFS-el való biztonságos kommunikációs csatorna felállításához és a jelszót a proxy szerver hitelesítéshez. Ezek a szenzitív információk titkosítva vannak tárolva, így védve azokat az ártó szándékú külső támadásoktól.

Titkosító algoritmus: Advanced Encryption Standard (AES)

Kulcs hosszúsága: 128-bit, 256-bit

Fontos: A készülék adatok kizárólag olyan információkat tartalmaznak, melyek a flottakezeléshez és a karbantartáshoz szükségesek. Nem tartalmaznak személyes adatokat (pl. címjegyzék) vagy az ügyfél képfeldolgozási adatait (nyomtatásból, másolásból, faxolásból vagy szkennelésből). Az ilyen adatok feldolgozásához az ügyfél engedélye szükséges a kezelőpanelen keresztül.

Rendszerkomponens	Kulcs hosszúság	Kulcs generálás és kezelési metodika
KFS Menedzser	256-bit	Minden környezethez külön kulcs generálódik, melyek beállításra kerülnek a szerverekhez. A kulcsok a konfigurációs menedzsment szoftverben vannak eltárolva (CMS), melyhez kizárólag a telepítési mérnök fér hozzá.
KFS Átjáró (PC/Box Common)	128-bit	A kulcs a KFS Átjáró első indításakor automatikusan generálódik. A kulcsok az alkalmazás helyi adatbázisában van tárolva, a hozzáférési kulcs a helyi adatbázishoz (Apache Derby) a programon belül van menedzselve.
KFS Mobil (Android)	256-bit	A kulcsok automatikusan generálódnak az applikáció első indításakor a telepítés után. A kulcsok az applikációtól függő adatbázisban vannak eltárolva.
KFS Mobil (iOS)	128-bit/256-bit	A kulcsok előzetesen generálódnak és beágyazásra kerülnek az applikációba (azonos minden eszköz esetén).
KFS Eszköz	128-bit/256-bit (modellfüggő)	A kulcsok az eszközön alapuló egyedi számként generálódnak az egyes készülékek indításakor a KYOCERA Document Solution saját algoritmus alapján és a készülék memóriájába kerülnek tárolásra.

2. táblázat: A kulcsok hosszának generálása és kezelése.

ADAT KOMMUNIKÁCIÓ

A KFS a kommunikációs adattartalmat titkosítja HTTPS protokoll segítségével, akár a felhasználó kezeli az adatokat a KFS Menedzseren keresztül, akár a komponensek között történik adatcsere. A HTTPS védi a KFS kommunikációs adatfolyamait a módosítástól, maszkolástól, megcsapolástól mivel minden KFS komponens egyaránt titkosított. A KFS titkosított adatokat küld és fogad az interneten keresztül és a helyi hálózaton (LAN).

> KFS kommunikáció az interneten keresztül

A KFS hálózati kommunikációt az XMPP szerver és a KFS Menedzser kezeli a felhőben. Az XMPP protokoll HTTPS protokollt használ az adattovábbításhoz. A KFS Menedzser XMPP protokollt használ az XMPP szerverrel való kommunikációhoz a felhőben, vagy a KFS Átjáró/KFS Eszköz és az XMPP szerver között a tűzfalon keresztül.

> KFS kommunikáció a helyi hálózaton

A KFS Átjáró és a készülékek közötti kommunikáció HTTPS web szolgáltatáson keresztül zajlik. A KFS Átjáró és a készülék biztonságos kommunikációja SNMPv3 használatával valósul meg, ami titkosítja a hálózaton küldött SNMP csomagokat. A helyi hálózaton zajló kommunikáció alhálózati maszkok, IP címek és hosztnevek tartományával van vezérelve. A hálózaton csak szándékos és vezérelt kommunikáció történik.

> Kommunikáció a KFS komponensek között

Az egy-az-egyben biztonságos kommunikációhoz a KFS Mobil és a készülék között beállítható titkosított Bluetooth, Wi-Fi Direct vagy USB.

> Extensible Messaging and Presence Protocol (XMPP)	> a KFS Menedzser és az XMPP szerver között - az XMPP szerver és a KFS Átjáró/KFS Eszköz között
Hyper Text Transport Protocol Secure (HTTPS)	- a böngésző kliens UI és a KFS Menedzser között - a böngésző kliens UI és a KFS Átjáró között - a KFS Menedzser és az XMPP szerver között - az XMPP szerver és a KFS Átjáró/KFS Eszköz között
Simple Network Management Protocol (SNMPv1/v2)	a KFS Átjáró és a készülék között
Bluetooth Wi-Fi Direct USB	a KFS Mobil (USB csak Android-hoz érhető el jelenleg) és a KFS Eszköz között

3. táblázat: Adat protollok és kommunikáció.

ADAT HOZZÁFÉRÉS

Mint számos más SaaS megoldás, a KFS is a több-bérlős architektúrán alapszik (multi-tenant system), hogy több dealer és viszonteladó is használni tudja a rendszert és "Csoport menedzsment" koncepciót használ az adathozzáférések kezeléséhez. A KFS-hez való hozzáférést a felhasználó csoportjának egységként való kezelése és a csoportba bejegyzett felhasználók és eszközök hozzáférési jogosultságainak megadása jelenti. Az információkat szigorúan védik ezek a hozzáférési jogok. Éppen ezért egy dealer nem fér hozzá másik dealer adataihoz, vagy annak ügyfeleihez.

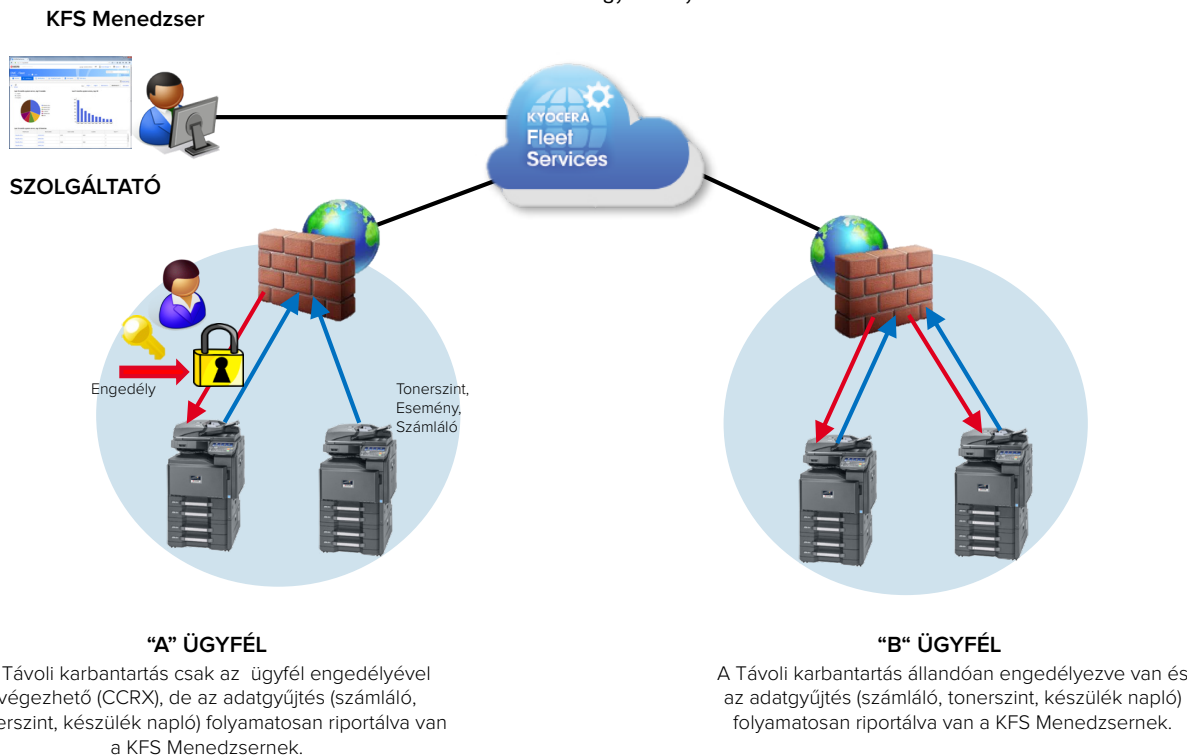
KAPCSOLATI MÓD

A Kapcsolati mód funkció a KFS-ben lehetőséget ad a felhasználóknak, hogy meghatározzák a készülék kapcsolódási módját a KFS szerverhez. Két beállítás lehetséges: Manage és Monitor. A beállítás elérhető az Átjáróhoz és az Ügynökhöz. A felhasználó elérheti a beállítást: az Átjáró UI-n, az Eszköz panelen, CCRX, Eszköz Regisztrációs és Diagnosztikai Eszközzel (DRD Tool) és a Mobil alkalmazással.

> **Monitor:** A KFS Eszköz/Átjáró kommunikációja a KFS szerverrel korlátozott. ("A" Ügyfél a lenti ábrán).

> **Manage:** A KFS Eszköz/Átjáró kommunikációja a KFS szerverrel XMPP-n keresztül állandó ("B" Ügyfél a lenti ábrán).

Ez azt jelenti, hogy "Monitor" beállítás esetén távoli karbantartás addig nem végezhető a szolgáltató által, amíg egy Manager jogosultsággal rendelkező személy az ügyfél részéről engedélyt nem ad a műveletre és és át nem kapcsolja a funkciót "Manage" módba. A készülék automatikusan visszavált "Monitor" módba egy bizonyos idő után. Ez az idő beállítható 1 órás időközökkel.



3. ábra: Példa a csoport beállítására és a kapcsolati mód beállítására.

Connection mode

- ☒ Manage - Remote maintenance and Data collection
☒ Automatically switch to Monitor in :
24 hours
☐ Monitor - Data collection

expire

Connection mode

- ☐ Manage - Remote maintenance and Data collection
☐ Automatically switch to Monitor in :
hours
☒ Monitor - Data collection

4. ábra: Command Centre (CCRX) példa a beállításokra.

ADATTOVÁBBÍTÁS

A 4. táblázat mutatja a készülékektől begyűjtött adatok mennyiségét és a kommunikáció gyakoriságát. Például a készülék információk (számláló, tonerszint, naplók) naponta egyszer kerülnek kiküldésre a KFS Menedzsernek.

Megjegyzés: A kapcsolat fenntartási funkció (Keep-alive) percenként fut, hogy biztosítsa az XMPP kapcsolatot a KFS Menedzser és a KFS Eszköz/KFS Átjáró között. A keep-alive funkció által generált kapcsolat adatmennyisége kb. 1.300 Kbyte/nap, de ez függ a csomag méretén (packet size). A készülékektől begyűjtött adatok nagysága kb. 100 Kbyte/nap. A becsült napi kommunikáció adatmennyisége kb. 1.400 Kbyte.

Adatkommunikáció típusa	Adatküldés gyakorisága	Adatkommunikáció mérete/nap	Adatkommunikáció teljes mérete/nap
> Számláló > Tonerszint > Készülék napló fájl	Naponta egyszer. Megjegyzés: a számláló/tonerszint max. napi négyszer küldhető el; az alapértelmezés napi egy alkalom.	80 Kbyte	1.400 Kbyte
> Értésítés	Riasztási eseményenként.	20 Kbyte	
> Keep-alive	Percenként.	1.300 Kbyte	
> Készülék beállítás > Pillanatkép > Készülék státusz > Karbantartási mód > Adat lehívás > USB Naplók > Mentés	A távoli karbantartási művelet alatt.	0 Kbyte Megjegyzés: > Karbantartási művelet nélkül nincs adatforgalom. > Az adatmennyiség függ a készülék típusától és a művelet tartalmától.	

4. táblázat: A kommunikáció típusai és az adatfolyamok.





FELHASZNÁLÓI FIÓKOK KEZELÉSE

A KFS Menedzserben a felhasználókhoz 5 féle jogosultsági szint rendelhető a feladattuktól függően.

1. **System Administrator:** Menedzseli a teljes KFS rendszert. Minden csoporthoz és felhasználóhoz hozzáférése van. Minden monitorozó, karbantartó és hibafeltáró művelethez hozzáfér.
2. **Manager:** Kezeli a felhasználókat, szerviz feladatokat, riportolást a hozzá delegált csoportokban és alcsoportokban. Külön jogosultsággal feltölthet és publikálhat firmware-eket.
3. **Service:** Regisztrálhat készülékeket a rendszerben. Minden karbantartási művelethez hozzáfér.
4. **Analyst:** Jogosultsága van riportokat futtatni, de nem futtathat karbantartási műveleteket.
5. **Customer:** Időzíthet és generálhat riportokat és üzeneteket. Láthatja a készülék tulajdonságokat. Nem fér hozzá a napló adatokhoz. Műveletek, mint a Készülék konfigurálása, szintén nem elérhető.

Megjegyzés: Mikor egy felhasználó belép a KFS Menedzserbe, minden esetben azonosítva és hitelesítve van. Ha az azonosítás és a hitelesítés sikeres, a felhasználó hozzáfér a KFS Menedzserhez a hozzá rendelt jogokkal.

Jelszó beállítás

Mikor a KFS Menedzserben először kerül létrehozásra egy felhasználói fiók, a felhasználó egy automatikus e-mailt kap. Az e-mail tartalmazza a felhasználói azonosítóját, az automatikusan generált jelszavát és egy linket a szolgáltatáshoz. A generált jelszó átmeneti, 7 napig érvényes. A felhasználónak az első bejelentkezéskor meg kell változtatnia a jelszavát. A jelszó megváltoztatása után az email-ben küldött link érvénytelenné válik. Ez a biztonsági funkció segít megővni a felhasználói fiókok sértetlenségét.

AZONOSÍTÁS ÉS HITELESÍTÉS

A KFS használatához a felhasználónak be kell jelentkeznie a regisztrált felhasználói azonosítójával és a jelszavával; jogosulatlan felhasználó nem férhet hozzá a KFS-hez. A belépési információk rögzítve és naplózva vannak, auditálás esetén elérhetőek ezek az információk. További beléptetési biztonsági funkciók:

> Fiók zárolási politika

Hogy a KFS védve legyen a jelszótörési támadások ellen, a felhasználói fiók zárolásra kerül, ha három egymás utáni alkalommal a jelszó megadása sikertelen. A fiók automatikusan feloldásra kerül 30 perc elteltével.

> Jelszó politika

A jogosulatlan hozzáférések megakadályozása végett a gyenge jelszavak használata nem megengedett a rendszerben, a felhasználóknak erős jelszavakat kell használniuk. A jelszónak legalább nyolc (8) karakter hosszúságúnak kell lennie, tartalmaznia kell legalább egy (1) számot (0-9), kisbetűt és nagybetűt, valamint speciális karaktert is.

FELADAT KORLÁTOZÁS

A szolgáltató által a KFS Menedzseren keresztül futtatott műveletek némelyike az ügyfél előzetes engedélyéhez köthető. Például a kijelző kép rögzítése (Panel Screenshot) és az adatlekérés (Data Capture) nem végezhető el az ügyfél engedélye nélkül. Az engedélyezési üzenet megjelenik a készülék kijelzőjén, melyt az ügyfélnek el kell fogadnia, hogy a műveletet végre lehessen hajtani.

Megjegyzés: A műveletek és a hozzá kapcsolódó adatok titkosítva vannak a HTTPS protokoll használatával. A KFS Menedzser képes megszakítani egy műveletet a KFS Eszköznek küldött stop parancs alkalmazásával a biztonságos XMPP kommunikációs csatornán keresztül.

Adat	A funkciók elvégzéséhez gyűjtött adatok és attribútumok
Készülék értesítés/Log	Rendszerhiba esetén a készülék egy esemény információt küld a KFS Menedzsernek, mely azonnal tájékoztatja a felhasználót. > Rendszerhiba > Esemény (pl. papírelakadás, alacsony tonerszint) > Fogyasztás > Számláló
Adat beállítás	A felhasználó kérésére távolról be lehet állítani a készüléket. A beállítások mentésre kerülnek a KFS Menedzserben, majd kiküldésre kerülnek a készülékre, amikor az használaton kívül van. Az alábbi információk kerülnek begyűjtésre: > Hálózati beállítások pl. bővített WSD > Rendszer beállítások pl. dátum/idő, időzóna > E-mail beállítások pl. SMTP, E-mail küldési beállítások > Nyomtatási beállítások pl. Eco nyomtatás > Másolási beállítások pl. eredeti kép, kifutó megelőzése > FAX beállítások pl. folyamatos szkennelés, FAX TX felbontás > Alap beállítások pl. szkennelési felbontás
Pillanatkép	A KFS Menedzser a távoli diagnosztikához a következő adatokat gyűjti. > Státusz > Szervíz státusz > Esemény napló > Karbantartási riport > USB Log > FAX riport
Készülék státusz	A készülék státuszának távoli lekérdezéséhez. > Panel üzenet > Riasztások listája
Karbantartási beállítások	Optimális karbantartási műveletek végzése az ügyfél telephelyén. Begyűjthető a KFS Menedzserből, megváltoztatható és visszaküldhető a készülékre. > Készülék beállítás
Adat lekérés	Begyűjthető, mikor a készülék kijelzőjén megjelenő jóváhagyó üzenet elfogadásra került. A szerviztechnikus megadhat egy max. 7 napos időintervallumot (alapbeállítás – 1 nap) a lekért adatok eltávolítására. > Ügyfél nyomtatási adatok
Igény szerinti USB Log	Igény szerinti USB Log-ok lekérése lehetséges az ügyfél telephelyén. A készülék zárolásra kerül néhány percre (3-4 perc) az adatok legyűjtéséig. A művelet után a készülék automatikusan újraindul. Amint a készülék újraindult, az USB log automatikusan letöltődik a felhasználó számítógépére a KFS Menedzserből. > USB Log-ok
Mentett adat	A szerviztechnikus be tud importálni a készülékbe egy másik készülékről mentett adatot. A mentett adat letöltése csak a készüléken megjelenő kérés jóváhagyása után lehetséges. A mentett adatban esetleg előforduló személyes adatok nem kerülnek tárolásra a KFS Menedzserben. A mentett adat titkosított. A funkció használatához megfelelő jogosultság szükséges. A mentett adatok importálása / exportálása rögzítésre kerül a rendszernaplóban. > Címjegyzék > Munkamenet fiók

KFS komponens	Információ (KFS-en belüli kommunikáció és azonosítás)
KFS Menedzser	> KFS felhasználók hitelesítési adatai. > A KFS Eszközök által használt hozzáférési azonosítók (KFS Átjáró és KFS Mobil). > A biztonságos kommunikációhoz használt szerver tanúsítványok a KFS Menedzser és a különböző ügynökök vagy kliensek között, mint a webböngészők, KFS Eszközök, KFS Átjárók és a KFS Mobil, illetve a KFS Menedzser belső komponensei. > A KFS Eszközök/KFS Átjárók MAC címei. > Hálózati információk, mint a regisztrált eszközök hoszt neve, IP címe, melyek a távoli menedzsment/karbantartás funkció használatához szükségesek. > A KFS Menedzserben/KFS Átjárón a készülék felderítés közben megadott SNMP hitelesítő adatok (pl. SNMPv1/v2 közösségi név, SNMPv3 felhasználó név és jelszó, stb.). > Mobil eszköz (okostelefon vagy tablet) gyári száma, melyre a KFS Mobil telepítve lett [ha a gyári szám nem nyerhető ki a mobil eszközéből, az IMEI száma lesz használva erre a célra].
KFS Device	> A készülék MAC címe, melyen a KFS Eszköz fut. > A készüléken vagy máshol megadott proxy hitelesítési információ. > A KFS Menedzserhez proxy szerveren keresztül csatlakozó Átjáró/Eszköz. > A KFS Menedzser által generált és a KFS Eszközre letöltött hitelesítési token.
KFS Átjáró	> A KFS Átjáróba belépéskor a rendszergazda által megadott hitelesítési információk. > A KFS Átjáróba belépéskor a szerviztechnikus által megadott hitelesítési információk. > A gép MAC címe, amin a KFS Átjáró telepítve lett (Windows-os KFS Átjáró esetén a PC, KFS Átjáró IB esetén a linux box). > A KFS Átjáró által használt azonosítási kód, mellyel regisztrálja magát a KFS Menedzserben [a kódot a KFS Átjáró az automatikus készülék felderítés és regisztráció esetén is használja]. > A KFS által használt proxy hitelesítési információk. > A KFS Menedzserhez proxy szerveren keresztül csatlakozó Átjáró/Eszköz. > A KFS Menedzser által generált és a KFS Átjáróra letöltött hitelesítési token. > A KFS Menedzserben/KFS Átjárón a készülék felderítés közben megadott SNMP hitelesítő adatok (pl. SNMPv1/v2 közösségi név, SNMPv3 felhasználó név és jelszó, stb.). > A KFS Átjáró által a készülékekkel történő kommunikációhoz használt hitelesítő adatok.
KFS Mobil	> Mobil eszköz (okostelefon vagy tablet) gyári száma, melyre a KFS Mobil telepítve lett [ha a gyári szám nem nyerhető ki a mobil eszközéből, az IMEI száma lesz használva erre a célra]. > A KFS Menedzser által generált hitelesítési token, mely letöltésre kerül a KFS Mobil alkalmazásba > A KFS Mobil felhasználó által megadott hitelesítési információ a KFS Menedzserbe való belépéshez > Proxy hitelesítési információt használ a KFS Mobil és a párosított KFS Eszköz a KFS Menedzserhez való csatlakozás közben a proxy szerveren keresztül.

6. táblázat: A KFS komponensek által használt információk.

AUDIT LOG

A Quocirca³ ajánlása szerint a flottakezelő rendszer bevezetésének egyik legnagyobb előnye a folyamatos monitorozás, mely elengedhetetlen a nyomtatási infrastruktúra irányításához. A KFS audit naplókat (log) rögzít számos eseményről, melyhez csak az engedélyezett felhasználók férnek hozzá. Audit napló készül az alábbi eseményekről:

Audit naplók - KFS Manager

- > Sikeres/sikertelen felhasználó azonosítás és hitelesítés
- > KFS Menedzser verzió váltás
- > Adatbázis mentés
- > Adatbázis helyreállítás
- > Csoport vagy felhasználó hozzáadása/szerkesztése/törlése
- > KFS Eszköz/KFS Átjáró/KFS Mobil regisztrálása/felfüggesztése/törlése
- > Biztonsági beállítások konfigurálása
- > Inaktív felhasználó munkamenetének megszakítása
- > Felhasználói jelszó visszaállítása e-mail-ben
- > Felhasználó lista importálása/exportálása
- > Feladat törlése/archiválása
- > Rendszer esemény törlése/archiválása
- > Eszköz napló exportálása
- > Audit naplók törlése/archiválása
- > Adatgyűjtés letöltése
- > Mentési adatok importálása/exportálása

Audit naplók - KFS Átjáró

- > Sikeres/sikertelen felhasználó azonosítás és hitelesítés
- > KFS Átjáró helyi adminisztrátor jelszó visszaállítása
- > Eszköz visszaállítási beállítások konfigurálása
- > Biztonsági beállítások konfigurálása
- > Inaktív munkamenetek megszakítása

Ezen eseményekhez rögzítve van az idő/dátum és az eredmény (siker/hiba). Módosítás vagy adatszivárgás esetén az audit naplók felhasználhatók a nyomozáshoz és segítenek lekövetni az esetleges illetéktelen hozzáférést. A működési naplók mentése az ellenőrzési nyomvonalak karbantartását szolgálják.

3- További információért olvassa el a Quocirca piaci előrejelzését a nyomtatási biztonságról: An Imperative in the IoT Era: <http://quocirca.com/wp-content/uploads/2018/06/Quocirca-Print-Security-Jan-2017-Report-Excerpt.pdf>

PORT BEÁLLÍTÁSOK

Az Intranet tűzfalon

- > A 443-as TCP porton (HTTPS) engedélyezni kell a kimenő forgalmat. Ezen a porton kommunikál a KFS Eszköz és a Windows-os KFS Átjáró a KFS Menedzserrel.
- > Ha a tűzfal a kimenő forgalmat fehérlista (whitelist) alapján engedélyezi, a KFS Menedzser webservereinek hoszt nevét fel kell venni a listára.
- > A webserverek neveit az alábbi 7. táblázat tartalmazza.

Server type	Host neve	IP cím	Érvényes
User Web	fs-eu.kyocera.biz	191.233.91.217	
Device Rest	rfs-eu.kyocera.biz	104.46.60.117	
XMPP Servers	fs-eucso1.kyods.com	52.233.166.114	10-jan-18
		52.233.152.139 (back-up)	10-jan-18
Remote Panel	fs-eurso01.kyocera.biz	40.115.1.211	10-nov-18
	fs-eurso02.kyocera.biz	40.113.113.42	10-nov-18

7. táblázat: KFS Web szerverek az EU régióban.

A számítógépen, melyen a Windows-os KFS Átjáró fut

- > A 443-as TCP porton (HTTPS) engedélyezni kell a kimenő forgalmat. Ezen a porton kommunikál a Windows-os KFS Átjáró a KFS Menedzserrel. Szintén ezen a porton keresztül kerül kiküldésre HTTPS-en a régebbi modellek regisztrációja, melyek nem támogatják még a WSDL KYOCERA kiterjesztést (KM-WSDL), illetve a fájl küldése funkció IPPS-en.
- > A 8443-as TCP porton (HTTPS) engedélyezni kell a bejövő forgalmat. Ez szükséges a Windows-os KFS Átjáró web UI eléréséhez ha a hálózaton egy másik számítógép internet böngészőjén keresztül kell használni.
- > A 161-es UDP porton engedélyezni kell a kimenő forgalmat az eszközök felé. Ezen a porton keresztül zajlik a készülék adatok begyűjtése SNMP-n keresztül.
- > A 80-as TCP porton (HTTP) engedélyezni kell a kimenő forgalmat. Ezen a porton keresztül kerülnek kiküldésre a Windows-os KFS Átjáró parancsai a régebbi KYOCERA készülékek regisztrációjához, melyek nem támogatják a KM-WSDL-t vagy a HTTPS-t.
- > A 9090-es (HTTP) és/vagy a 9091-es (HTTPS) TCP porton engedélyezni kell a kimenő forgalmat. Ezen a porton keresztül küldi a Windows-os KFS Menedzser parancsai a KFS Eszközhöz KMWSDL-en keresztül a készülék regisztrációjakor.
- > A Windows-os KFS Átjáró telepítésekor a 8442-es TCP port (vagy a telepítéskor megadott alternatív port) automatikusan megnyitásra kerül a Windows tűzfalon a bejövő forgalom engedélyezésére a készülékek felől. Ez szükséges a firmware frissítés funkció használatához. A bejövő forgalom engedélyezése automatikusan törlődik a KFS Átjáró eltávolításakor.
- > A 9100-as TCP porton (vagy egy alternatív porton, mely meg lett adva a fájl küldése funkcióhoz) engedélyezni kell a kimenő forgalmat a KFS Átjáró fájl küldése funkciójához - raw port nyomtatás (RAW).

- > A Windows-os KFS Átjáró telepítésekor a 8081-es TCP port (HTTPS) automatikusan megnyitásra kerül a Windows tűzfalon a bejövő forgalom engedélyezésére a készülékek felől. Ez szükséges a KFS Átjáró 1 pontos kommunikáció funkciójának használatához. A bejövő forgalom engedélyezése törlésre kerül az Átjáró eltávolításakor.
- > Az 1 pontos kommunikáció beállítása az Átjárón egyszerű. Ahogy a telepítés a PC-n kész és a regisztráció a KFS szerveren megtörtént, be kell állítani a proxy-t, amennyiben az ügyfél használ proxy-t. Ha nem, a check box aktiválásával a telepítés kész. A KFS-ben már regisztrált készülékek esetén is megváltoztathatók a proxy beállítások a 8081-es porton.

A számítógépen, melyen a Helyi Ügynök fut

A Helyi Ügynök egy program, melyet olyan PC-re kell telepíteni, melyhez USB-n keresztül van nyomtató kötve, így az Átjáró megtalálja az adott eszközt.

- > A 445-ös TCP porton engedélyezni kell a bejövő forgalmat a Helyi Ügynök KFS Átjárón keresztüli telepítéséhez. A porton keresztül kerülnek átküldésre a fájlok a Helyi Ügynök telepítéséhez/frissítéséhez SMB-n.
- > A Windows Management Instrumentation (WMI) engedélyezése szükséges a Helyi Ügynök telepítéséhez vagy frissítéséhez a Windows-os KFS Átjáróból.
- > Ha a WMI vagy a WinRM engedélyezése ellenkezik a helyi biztonsági előírásokkal, letiltva lehet hagyni. Ebben az esetben a Helyi Ügynököt manuálisan kell telepíteni, nem a Windows-os KFS Átjáróból.

Forrás	Célállomás	Protokoll	Port	Szolgáltatás
MFP / nyomtató	KFS Menedzser	TCP	443	HTTPS : flotta adatok küldése a KFS-nek
Átjáró Windows-hoz	KFS Menedzser	TCP	443	HTTPS : flotta adatok küldése a KFS-nek
Kliens PC	KFS Menedzser	TCP	443	HTTPS : hozzáférés a UI-hoz
Kliens PC	Átjáró Windows-hoz	TCP	443	HTTPS : hozzáférés a UI-hoz
Átjáró Windows-hoz	MFP / nyomtató	UDP	161	SNMP
		TCP	443	IPPS
		TCP	9100	RAW (a fájlküldés funkcióhoz)
		TCP	8442	HTTP (a firmware frissítés funkcióhoz)
		TCP	80	HTTP
		TCP	443	HTTP
		TCP	9091	SOAP HTTPS-en : eszköz konfiguráció
		TCP	8081	1 pontos kommunikáció
Átjáró Windows-hoz	Helyi Ügynök	UDP	161	SNMP
		TCP	445	SMB
		TCP	5985	WinRM

8. táblázat: Port beállítások.

RENDSZER JAVASLATOK

Rendszer komponens	Operációs rendszer	Böngésző	.NET Framework	Java runtime
Menedzser	-	Internet Explorer 11 Edge Firefox 40 vagy újabb (*1) Chrome 47 vagy újabb (*1) Safari 8 vagy újabb (*1)	-	-
Átjáró (Windows)	Windows 7 [32-bit/64-bit] Windows 8/8.1 [32-bit/64-bit] Windows 10 [32-bit/64-bit] Windows Server 2008 R2 [64-bit] Windows Server 2012 R2 [64-bit] Windows Server 2016 [64-bit]	Internet Explorer 11 Edge Firefox 40 vagy újabb (*1) Chrome 47 vagy újabb (*1)	-	JRE 7 [32-bit] JRE 8 [32-bit] JRE 7 [64-bit] JRE 8 [64-bit]
Helyi Ügynök	Windows 7 [32-bit/64-bit] Windows 8/8.1 [32-bit/64-bit] Windows 10 [32-bit/64-bit] (*3)	-	.NET Framework 3.5 (*2)	-

RENDSZER JAVASLATOK

Mobil (Android)	Android 4.1 vagy újabb	-	-	-
Mobil (iOS)	iOS 8.0 vagy újabb	-	-	-
DRD (Device Registration and Diagnostics) Eszköz regisztrációs és diagnosztikai program	Windows 7 [32-bit/64-bit] Windows 8/8.1 [32-bit/64-bit] Windows 10 [32-bit/64-bit] Windows Server 2008 R2 [64-bit] Windows Server 2012 R2 [64-bit]	-	.NET Framework 4	-
DCT (Data Collection Tool) Adatgyűjtő program	Windows 7 [32-bit/64-bit] Windows 8/8.1 [32-bit/64-bit] Windows 10 [32-bit/64-bit] Windows Server 2008 R2 [64-bit] Windows Server 2012 R2 [64-bit]	-	.NET Framework 4	-

(*1) Javasoljuk, hogy minden esetben az elérhető legújabb hivatalos verziót használja.

(*2) Legalább Windows 8/8.1 szükséges a “.NET Framework 3.5 (beleértve a .NET 2.0 és 3.0)” engedélyezéséhez a Windows funkciókban.

(*3) Nem domain-be léptetett környezetben a KFS Gateway Local Agent távoli telepítése Windows rendszer esetén a cél számítógép regisztrációs kulcsának módosítása szükséges lehet, ahogy az alábbi linken elérhető leírásban szerepel, hogy a fájlrendszer adminisztrátori megosztása engedélyezett legyen. Bővebb információt a KFS Átjáró Kezelési Útmutatójában talál.

<https://support.microsoft.com/en-us/kb/942817>

9. táblázat: Javasolt rendszerkiépítések összesítése.



A KYOCERA

A KYOCERA Document Solutions Inc. a KYOCERA Corporation leányvállalata, mely fennállásának 50. évfordulóját ünnepelte 2009-ben. A KYOCERA Document Solutions egyike a világ vezető irodai dokumentumkezelő megoldásokat szállító vállalatainak. Termékeinek és szolgáltatásainak széles palettája magába foglalja az Ecosys nyomtatókat, a megbízható multifunkciós eszközöket, a kiváló minőségű kellékanyagokat és a szoftveres- és MDS megoldások portfólióját.

© 2017 KYOCERA Document Solutions Europe B.V.



GLOBAL-UNION Kft.

1172 Budapest, Rétifarkas u. 16.

Tel: +36 (1) 273-0100

Email: mds@globalunion.hu