KONICA MINOLTA

Biztonságtechnikai tanácsok

Service Location Protocol, sérülékenység

CVE-2023-29552

Verzió: 1.3
Dátum: 2023. május 3.

Tartalomjegyzék

1 Módosítási napló

Verzió	Dátum	Módosítás
1.0	2023.04.26.	Első változat
1.1	2023.04.28.	Kárenyhítési folyamat hozzáadása az IT6-hoz és az eszköz kézikönyv linkekhez
1.2	2023.05.02.	Az SLP-t és CVSS pontszámot nem használó alkalmazások listájának hozzáadása
1.3	2023.05.03.	Dispatcher Paragon+ és Dispatcher Pheonix hozzáadása

2 Háttér

A közelmúltban a Bitsight és a Curesec kutatói felfedezték, hogy a CVE-2023-29552 néven azonosított Service Location Protocol (SLP) protokollal visszaélve magas amplifikációs faktorú DoS-támadásokat lehet végrehajtani hamisított forráscímek felhasználásával. Az SLP lehetővé teszi egy nem hitelesített távoli támadó számára, hogy tetszőleges szolgáltatásokat regisztráljon. A sérülékenységet kihasználó támadók az eseteket felhasználva akár 2200-szoros faktorú, masszív szolgáltatásmegtagadásos (Denial-of-Service (DoS)) támadásokat indíthatnak, amely az egyik legnagyobb támadást jelentheti. Az SLP egy olyan protokoll, amelyet 1997-ben hoztak létre az RFC 2165 révén, hogy dinamikus konfigurációs mechanizmust biztosítson a helyi hálózatok alkalmazásai számára. Az SLP lehetővé teszi, hogy a hálózaton lévő rendszerek megtalálják egymást és kommunikáljanak egymással. Ehhez az elérhető szolgáltatások jegyzékét használja, amely olyan dolgokat tartalmazhat, mint a nyomtatók, fájlkiszolgálók és egyéb hálózati erőforrások. Az SLP úgy működik, hogy egy rendszer regisztrálja magát egy jegyzéket kezelőnél, amely a rendszer szolgáltatásait elérhetővé teszi a hálózat többi rendszere számára. Az SLP-t biztosító daemonok az alapértelmezett 427-es porthoz vannak kötve, mind UDP, mind TCP esetén. Az SLP-t nem arra tervezték, hogy a nyilvános internet számára elérhető legyen.

CVE ID	Érintett funkció	Lehetséges Hatás	CVSSv3.1 pontszám	Ellenintézkedés
CVE-2023-29552	Service Location Protocol	szolgáltatás megtagadása	8.6	Kárenyhítés alább

Hivatkozás: [Service Location Protocol Vulnerability (Bitsight)]

Mivel az SLP a legtöbb Konica Minolta készülékben megtalálható, szeretnénk felhívni a figyelmét az alábbi biztonságtechnikai tanácsokra. Kérjük, tanulmányozza a Konica Minolta termék státusz című részt a készülékre gyakorolt hatásról és az esetlegesen felmerülő károk enyhítéséről.

3 Konica Minolta termék státusz

A CVE-2023-29552 biztonsági rés magát a Service Location Protocol (SLP) protokollt érinti. Azok az eszközök, amelyeken ez a protokoll ki van kapcsolva, vagy engedélyezve van, de nem érhető el közvetlenül a nyilvános internetről (pl. tűzfal védi), nincsenek közvetlen veszélyben. Azonban azokon az eszközökön, amelyeken a protokoll engedélyezve van, és közvetlenül elérhetőek a nyilvános internetről, nagy kockázatnak vannak kitéve. Ezt a biztonsági rést kihasználva a támadó szolgáltatásmegtagadásos támadást hajthat végre az áldozat eszközén vagy kiszolgálóján

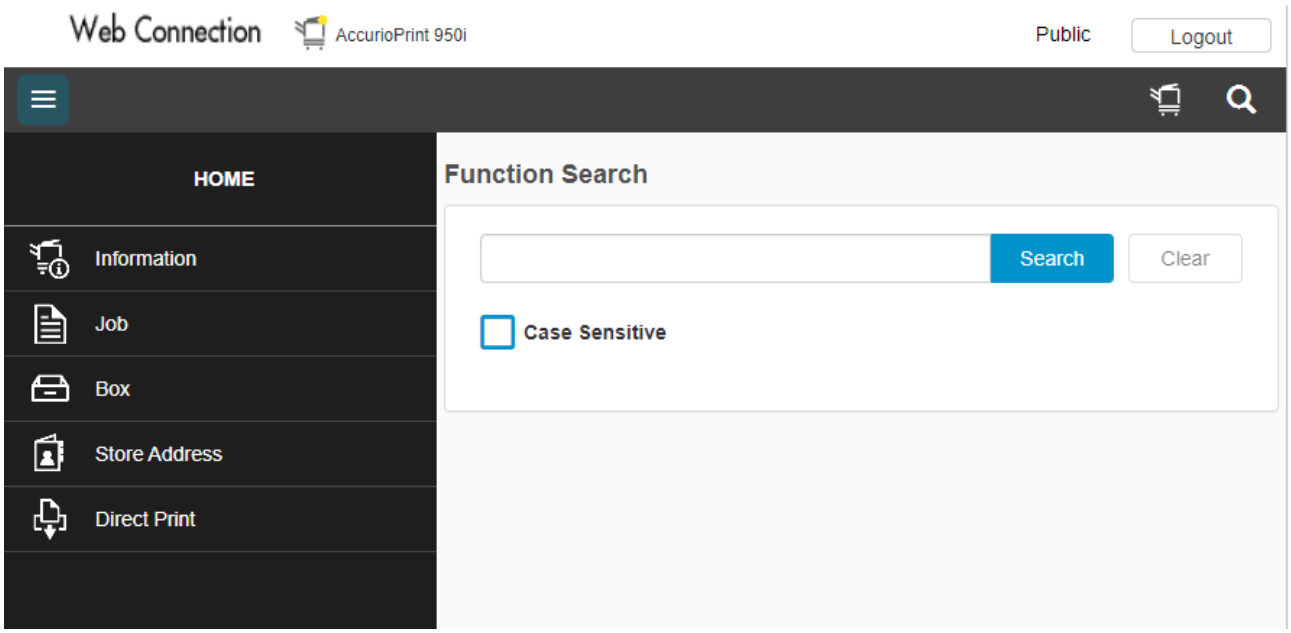
4 Kárenyhítés

A CVE-2023-29552 elleni védekezés érdekében az SLP-t le kell tiltani minden olyan rendszernél, amely nem megbízható hálózatokon fut, például közvetlenül az internetre csatlakozik. Ha ez nem lehetséges, akkor a tűzfalakat úgy kell beállítani, hogy a 427-es UDP és TCP porton keresztül érkező forgalmat szűrjék. Ez megakadályozza, hogy a külső támadók hozzáférjenek az SLP-szolgáltatáshoz. További védekezési lépésként javasoljuk, ha az eszköz nem megbízható hálózatra kerül, cserélje le az alapértelmezett rendszergazda jelszavát egy biztonságosabb, összetettebb jelszóra. Ez biztosítja, hogy egy potenciális támadó ne tudjon bejelentkezni egy védtelen eszközre, hogy azon engedélyezze a sérülékeny protokollt. Irodai nyomtatási és termelési nyomtatási eszközeinken az SLP beállítás általában a hálózati beállításokon keresztül konfigurálható, rendszergazda módban. A beállítás az MFP kijelzőjén, a webfelületen vagy a távoli panelen keresztül érhető el. Az alábbiakban felsoroljuk azokat az alkalmazásokat, amelyek nem használják az SLP-protokollt:

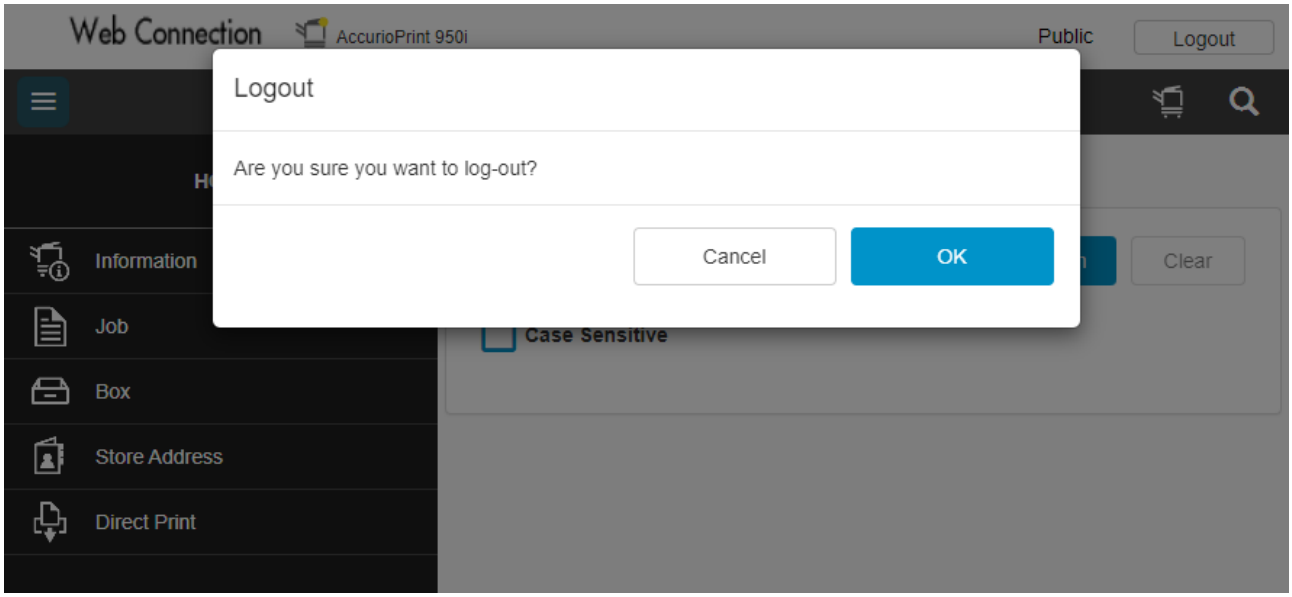
- Box Operator
- CS Remote Care adatgyűjtő (CSRC DCA)
- CS Remote Care Relay tool
- RSA Edge telepítő
- Data administrator
- FleetRMM
- Font Management segédprogram
- HDD BackUp segédprogram
- HDD TWAIN illesztőprogram
- IWS telepítési eszköz
- Naplókezelő segédprogram
- PageScope Enterprise Suite
    - Net Care eszközkezelő
    - Account menedzser
    - Hitelesítési menedzser
    - Saját nyomtatáskezelő
    - Saját panelkezelő
    - Eszköz Plug-in modulok
- Print status notifier
- ReTWAIN Illesztőprogram (valós idejű mód)
- Távoli telepítési eszközök (RDT)
- Eszközök az LK-114-hez
    - ManagerPort
    - InstallerCreateTool
    - SetupTool
- OpenAPI SDK
- bizhub Remote Panel (Távoli panel szerver)
- CS Remote Care (szerver modulok)
- CS Remote Analysis (szerver modulok)
- YSoft SafeQ 6
- Dispatcher Paragon
- Dispatcher Paragon+
- Dispatcher Phoenix

Az alábbi példa az i-Series-ben használt IT6 vezérlőn alapul:

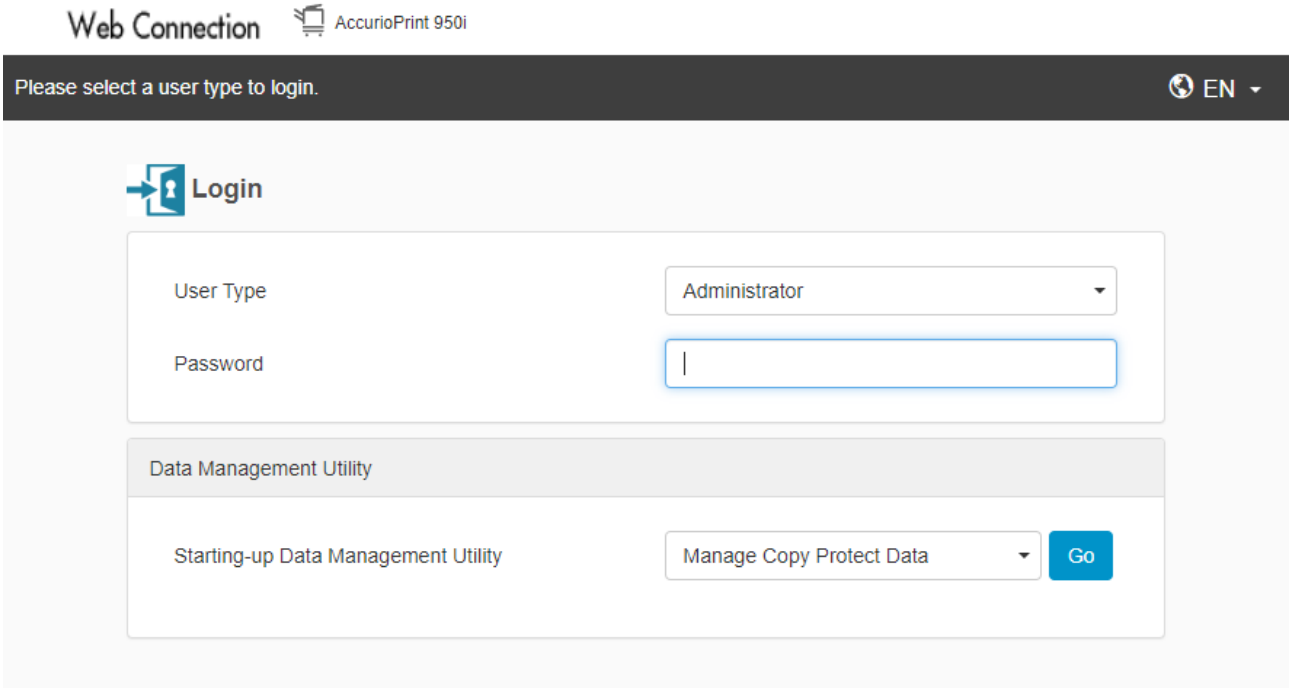
1. Először lépjen be a készülékbe úgy, hogy beírja az IP-címet a webböngészőbe.



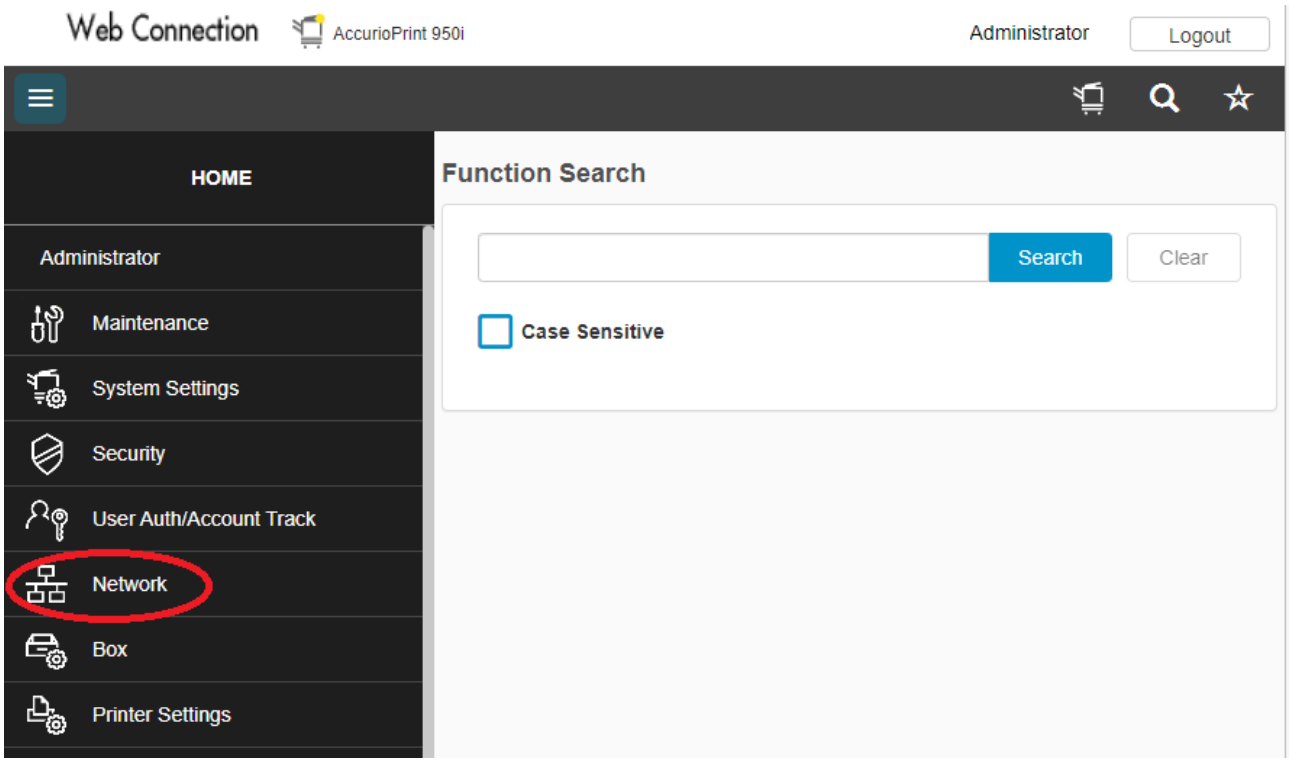
2. Kattintson a kijelentkezés (logout) gombra a Public User mode-ból való kilépéshez.



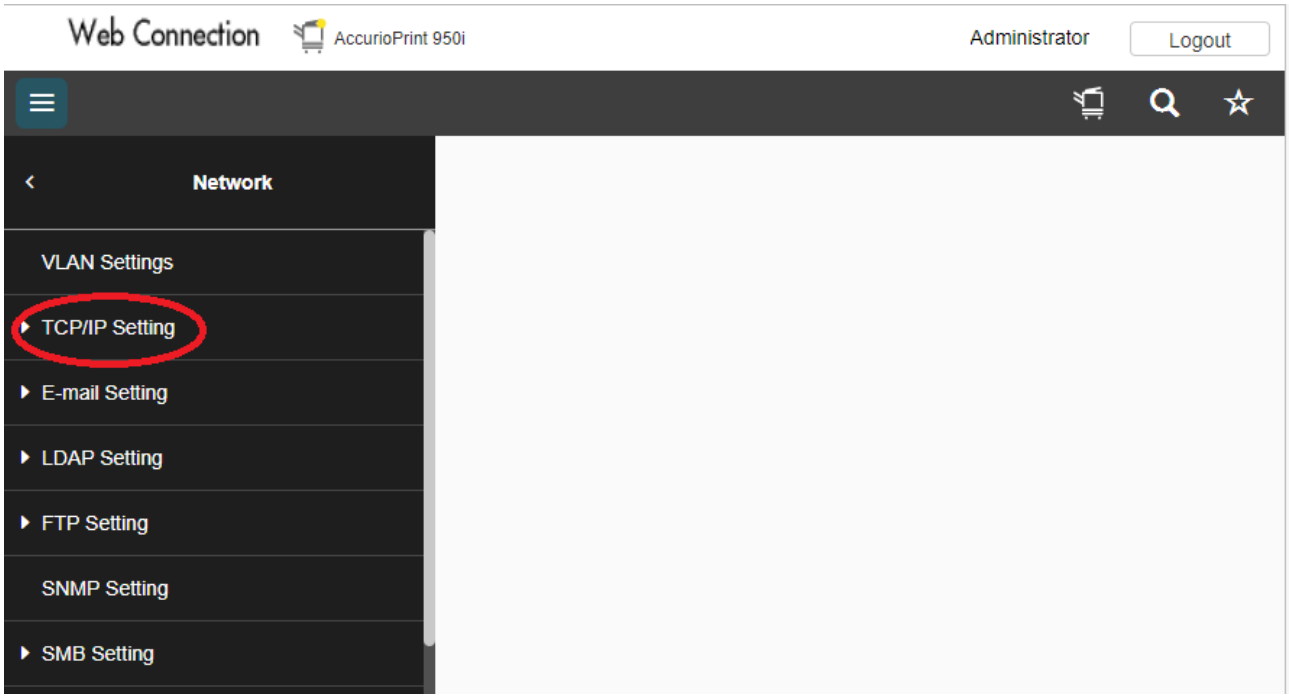
3. Ezután válassza a Rendszergazda felhasználói típust (User Type: Administrator), és adja meg a jelszót.



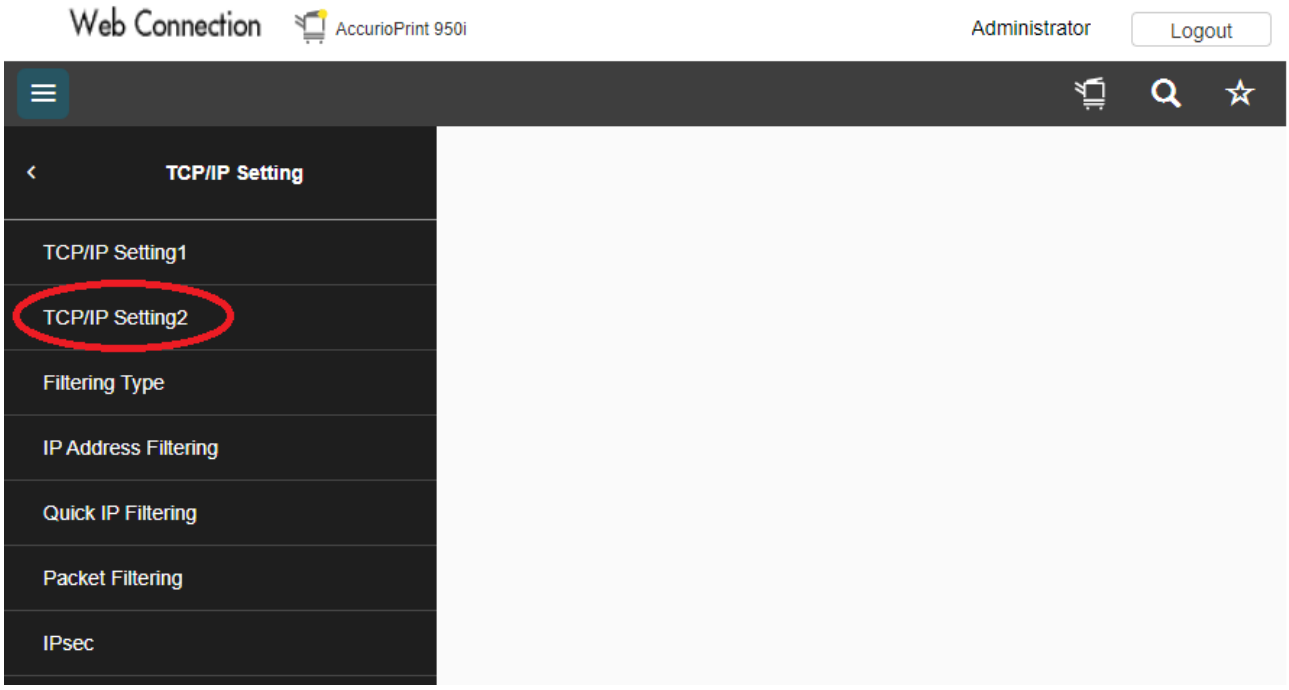
4. Bejelentkezés után válassza a Hálózat (Network) menüpontot.



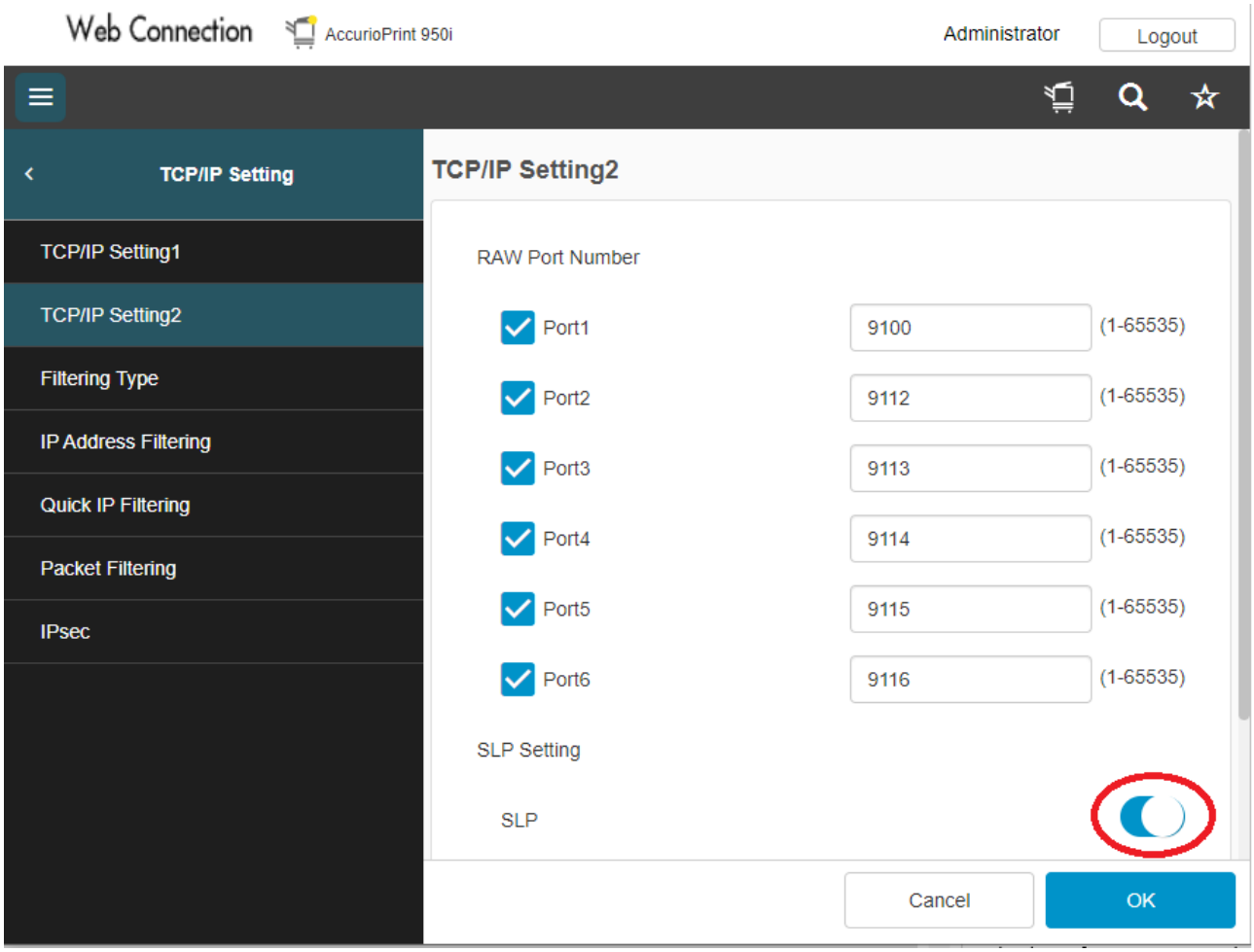
5. Itt válassza a TCP/IP Setting beállításokat.



6. Ezután válassza a TCP/IP Setting2 lehetőséget.



7. Végül állítsa az SLP beállítási kapcsolót kikapcsolt állapotba, és nyomja meg az OK gombot a mentéshez.



Az SLP-beállítás alternatívaként olyan flottakezelési megoldásokon keresztül is konfigurálható, mint például a Remote Deployment Tools (RDT) vagy a FleetRMM. További információért forduljon a helyi Konica Minolta képviseletéhez. Más Konica Minolta eszközök és nyomtatásvezérlők esetében, kérjük, tanulmányozza az alábbi felhasználói kézikönyveket:

- **Konica Minolta Online Manuals**
- **Konica Minolta Download Centre**

Konica Minolta Magyarország Üzleti Megoldások Kft., 1117 Budapest, Galvani u. 4. · Magyarország
www.konicaminolta.hu