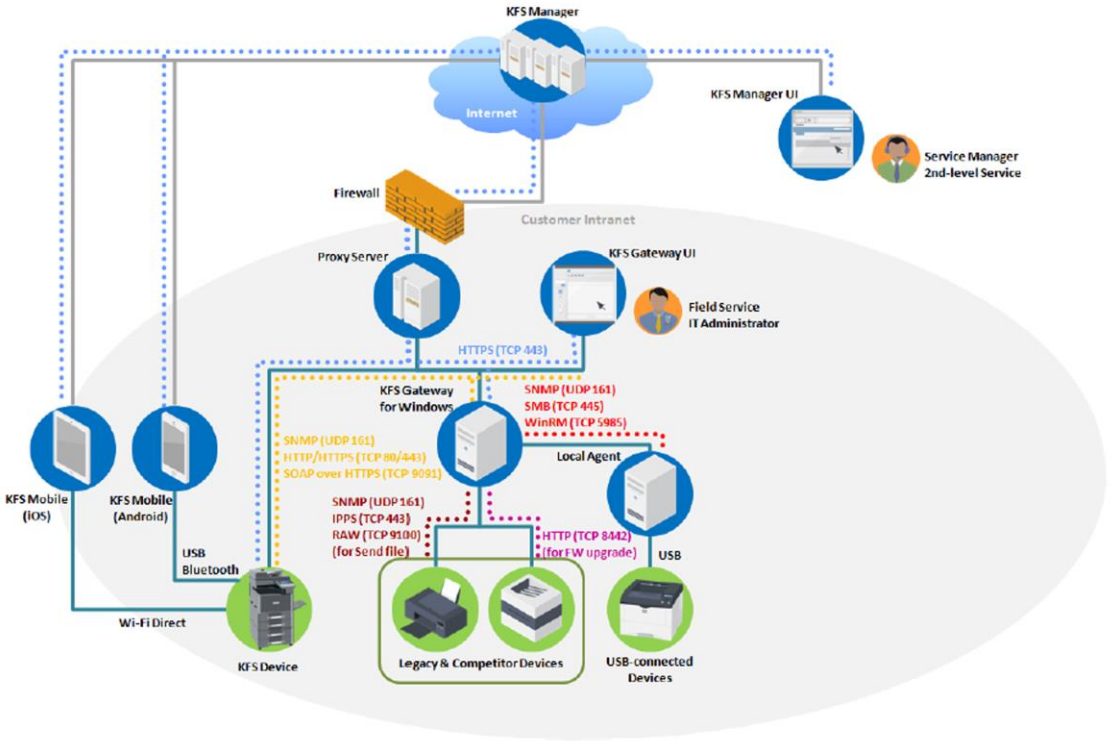
KYOCERA FLEET SERVICES
PORT INFORMATION

Bei **KYOCERA Fleet Services (KFS)** müssen Benutzer keine nicht-standardisierte Ports öffnen.
KFS verwendet für die Kommunikation nur standardisierte Ports.
Daher besteht keine Notwendigkeit, sich um die Sicherheit zu sorgen;
Wenn jedoch die Sicherheit nach wie vor ein Problem ist, wird der Einsatz eines Proxies empfohlen.

Port Information

Für die unterschiedlichen Funktionen werden verschiedene Ports verwendet, wie unten gezeigt:



Intranet Firewall

- **TCP 443** (HTTPS) muss geöffnet sein, um ausgehenden Datenverkehr zuzulassen. Dieser Port wird für KFS-Geräte und KFS-Gateway (für Windows und IB) verwendet, um eine Verbindung zum KFS-Manager herzustellen.
- Wenn Ihre Firewall den ausgehenden Datenverkehr durch eine Ziel-Whitelist beschränkt, sollten die Hostnamen der Webserver in KFS Manager hinzugefügt werden.
    - Die Namen der Webserver hängen davon ab, in welchem Azure-Rechenzentrum KFS Manager gehostet wird. Diese Informationen werden von der Kyocera-Zentrale in Ihrer Region bereitgestellt.

PC mit NetGateway (Standardwerte)

- **TCP 443** (HTTPS) muss geöffnet werden, um ausgehenden Datenverkehr zuzulassen. Dieser Port wird für die Verbindung vom NetGateway zum KFS Manager verwendet. Der Port 443 wird verwendet, um eine sichere Verbindung zur Geräte-Homepage über HTTPS herzustellen.
- **TCP 9797** (HTTPS) sollte geöffnet werden, um eingehenden Datenverkehr zuzulassen. Dies ist erforderlich, wenn Sie eine Verbindung zur NetGateway-Webseite herstellen möchten.
- **TCP 80** (HTTP) sollte geöffnet werden, um ausgehenden Datenverkehr zuzulassen. Dieser Port wird für für die Verbindung vom NetGateway zur Geräte-Homepage verwendet.
- **TCP 9090** (HTTP) **und/oder 9091** (HTTPS) sollte geöffnet werden, um ausgehenden Datenverkehr zuzulassen. Dieser Port wird für NetGateway verwendet, um Daten vom Gerät anzufordern.
- **UDP 161** muss geöffnet werden, um ausgehenden Datenverkehr zu Geräten zuzulassen. Dieser Port wird zum Erfassen des Gerätestatus und der Eigenschaften über SNMP verwendet.
- **TCP 8081** muss offen sein, um **S**ingle **P**oint **o**f **C**ommunication über den Stone Proxy zu ermöglichen.

PC mit KFS Gateway for Windows

- **TCP 443** (HTTPS) muss geöffnet werden, um ausgehenden Datenverkehr zuzulassen. Dieser Port wird verwendet, um eine Verbindung zum KFS Manager herzustellen. Der Port wird auch zum Senden von Steuerbefehlen über HTTPS verwendet, wenn ältere KFS-Gerätemodelle registriert werden, die die Kyocera-Erweiterung von WSDL (KM-WSDL) nicht unterstützen. Derselbe Port wird auch für die Funktion zum Senden von Dateien über IPPS verwendet.
- **UDP 161** muss geöffnet werden, um ausgehenden Datenverkehr zu Geräten zuzulassen. Dieser Port wird zum Erfassen des Gerätestatus und der Eigenschaften über SNMP verwendet.
- **TCP 80** (HTTP) sollte geöffnet werden, um ausgehenden Datenverkehr zuzulassen. Dieser Port wird für KFS Gateway für Windows verwendet, um Steuerbefehle zu senden, wenn ältere Modelle von KFS-Geräten registriert werden, die weder KM-WSDL noch HTTPS unterstützen.
- **TCP 9091** sollte geöffnet werden, um ausgehenden Datenverkehr zuzulassen. Dieser Port wird für KFS Gateway für Windows verwendet, um zum Zeitpunkt der Geräteregistrierung Steuerbefehle über KM-WSDL an KFS-Gerät zu senden.
- **TCP 8442** (oder ein zum Zeitpunkt der Installation angegebener alternativer Port) wird automatisch in der Windows-Firewall geöffnet, um eingehenden Datenverkehr von Geräten zuzulassen. Dies ist erforderlich, wenn Sie die Firmware-Aktualisierungsfunktion über KFS Gateway für Windows verwenden möchten. Die so erstellte eingehende Regel wird gelöscht, wenn KFS Gateway für Windows deinstalliert wird.
- **TCP 9100** (oder ein alternativer Port, der als Parameter für eine Sendedatei-Aufgabe angegeben werden soll), sollte für ausgehenden Datenverkehr geöffnet werden, wenn Sie die Funktion zum Senden von Dateien über Raw (Raw Port Printing) über KFS Gateway für Windows verwenden möchten.
    - Die obigen Einstellungen sind bei Auslieferung in KFS Gateway für IB vorkonfiguriert.

PC mit installiertem Local Agent (über USB verbundene Drucker)

- **TCP 445** sollte für eingehenden Datenverkehr geöffnet sein, wenn Sie die Funktion von KFS Gateway für Windows zum Installieren oder Aktualisieren des lokalen Agenten verwenden möchten. Dieser Port wird zum Übertragen von Dateien verwendet, die für die Installation oder das Upgrade des lokalen Agenten über SMB erforderlich sind.
- Windows Management Instrumentation (WMI) sollte aktiviert sein, wenn Sie die Funktion von KFS Gateway für Windows zum Installieren oder Aktualisieren des lokalen Agenten verwenden möchten.
- **TCP 5985** wird für eingehenden Datenverkehr geöffnet, wenn Sie Windows Remote Management (WinRM) aktivieren. Dies ist erforderlich, wenn Sie die Funktion von KFS Gateway für Windows zur Installation oder Aktualisierung des lokalen Agenten verwenden möchten.
    - Ausführliche Anweisungen zum Aktivieren von WMI und WinRM finden Sie im KYOCERA Fleet Services Gateway-Benutzerhandbuch.
    - Wenn die Aktivierung von WMI oder WinRM gegen die Sicherheitsrichtlinie Ihrer Site verstößt, sollten Sie sie deaktiviert lassen. In diesem Fall müssen Sie Local Agent manuell und nicht von KFS Gateway für Windows installieren.