OMECORP GENESIS BUSINESS SYSTEMS

(918) 664-2588 or (800)520-7755
5125 S. Garnett Rd. Ste. F
Tulsa, OK 74146
Empowering. Connections.

Trusted -Since- 1975

KFS WHITE LIST

For all new MFP and Printer instalation the following IP’s and ports need to be availible.

KFS Web Servers after XMPP Server Address Unification

Server Type	**Host Name**	**IP Address**
User Web	fs-us.kyocera.biz	23.102.187.77
Device Rest	rfs-us.kyocera.biz	23.101.190.57
XMPP Servers	**fs-uscs01.kyods.com**	**13.65.249.118**
		13.65.249.143 ***As a backup**

On the Intranet Firewall

- TCP port 443 (HTTPS) must be opened to allow outbound traffic. This port is used for KFS Device and KFS Gateway for Windows to connect to KFS Manager.
- If your firewall restricts outbound traffic by a destination whitelist, the host names of Web servers in KFS Manager should be added in it.

- The names of the Web servers vary depending on which Azure data center KFS Manager is hosted. This information is provided by the Kyocera headquarters in your region.

On the Machine Hosting KFS Gateway for Windows

- TCP port 443 (HTTPS) must be opened to allow outbound traffic. This port is used for KFS Gateway for Windows to connect to KFS Manager. The port is also used to send control commands by HTTPS when registering older models of KFS Device that don’t support the KYOCERA extension of WSDL (KM-WSDL). The same port is used for the Send File feature over IPPS, too.
- TCP port 8443 (HTTPS) should be opened to allow inbound traffic. This is necessary if you wish to use the Web UI of KFS Gateway for Windows from a browser running on another PC in the LAN.
- UDP port 161 must be opened to allow outbound traffic to devices. This port is used to collect device status and properties over SNMP.
- TCP port 80 (HTTP) should be opened to allow outbound traffic. This port is used for KFS Gateway for Windows to send control commands when registering older models of KFS Device that don’t support either KM-WSDL or HTTPS.

- TCP port 9090 (HTTP) and/or 9091 (HTTPS) should be opened to allow outbound traffic. This port is used for KFS Gateway for Windows to send control commands to KFS Device over KMWSDL at the time of device registration.
- When KFS Gateway for Windows is installed. TCP port 8442 (or an alternative port specified at the time of installation) is automatically opened in Windows Firewall to allow inbound traffic from devices. This is necessary if you wish to use the Firmware Upgrade feature via KFS Gateway for Windows. The inbound rule thus created will be deleted when KFS Gateway for Windows is uninstalled.
- TCP port 9100 (or an alternative port to be specified as a parameter of a Send File task) should be opened for outbound traffic, if you wish to use the Send File feature over raw port printing (RAW) via KFS Gateway for Windows.
- When KFS Gateway for Windows is installed, TCP port 8081 (HTTPS) is automatically opened in Windows Firewall to allow inbound traffic from devices. This is necessary if you wish to use the feature of KFS Gateway for Windows to consolidate outgoing network traffic from KFS Device as a single point of communication. The inbound rule thus created will be deleted when KFS Gateway for Windows is uninstalled.