

POSTBASE ADVANCED NETWORK SETUP

Security Certificates and Firewall Rules for Networking PostBase

FP Mailing Solutions
140 N. Mitchell Ct. #200
Addison, IL 60101-5627
Tel: 800-341-6052
Fax: 800-341-5141



In some cases you may have problems connecting a PostBase meter with the customer's local network. After trying all possible settings in the connectivity menu, the machine may still show an error message:

“Connection to the FPI is impossible, please check your connection settings”.

Local computer networks are all individual and different. Some customers (e.g. credit institutions and public authorities) may have especially high security standards. One special security feature that may cause an issue is the firewall. In some organizations there can be a firewall independent of the Windows firewall, and sometimes both are active.

Security Certificates

Public Security Certificates

Depending on the configuration of those firewalls, a certification check is set up by the administrator. Certificates are used to establish a secure https data connection on port 443. This public certification can be bought from commercial organizations like VeriSign, Thawte, Symantec, and GeoTrust. These public certificates have an advantage as they are updated automatically on all certificate servers.

FP Security Certificates

Service providers like FP can also issue their own security certificates, which may cause problems on the customer's network. Since the corresponding certificate required to check or validate the FP certificate is unknown to the customer's firewall, the transfer of data between PostBase and the FP server is blocked resulting in a connection error.

To solve this problem, network administrators can download the FP Security Certificate files and embed the FP certificates into their local area network (proxy server/firewall). The files are available on the [FP PostBase Support](#) web page.

Firewall Rules

Local network administrators may also have to configure their firewalls by adding the following rules/exceptions to accommodate FP connections.

The PostBase machine attempts to resolve the following IP addresses:

50.201.5.193
50.201.5.194
193.29.243.32
193.29.243.33

IP ADDRESSES & CONNECTION TYPES

SUBDOMAIN	PROTOCOL	IP ADDRESS	CONNECTION TYPE
N/A	N/A	193.29.243.32	Not currently in use, but may activate as backup to 193.29.243.33
ins.franco typ.com	mutual SSL	193.29.243.33	Used by installer software
ins2.franco typ.com	mutual SSL	193.29.243.33	Used by installer software
5ins.franco typ.com	mutual SSL	193.29.243.33	Used by PostBase Mini installer software*
5ins2.franco typ.com	mutual SSL	193.29.243.33	Used by PostBase Mini installer software*
mausa.franco typ.com	mutual SSL	50.201.5.194	Communication with FPI (TDC) PVD
mausa2.franco typ.com	mutual SSL	50.201.5.194	Communication with FPI (TDC) PVD
busa.franco typ.com	HTTP & SSL	50.201.5.193	Remote diagnostics on PSD or HTTPS failure
busa2.franco typ.com	HTTP & SSL	50.201.5.193	Remote diagnostics on PSD or HTTPS failure
mabusa.franco typ.com	mutual SSL	50.201.5.194	Communication with Repository
mabusa2.franco typ.com	mutual SSL	50.201.5.194	Communication with Repository

*Applies to **PostBase Mini** only, not to PostBase 20, 30, 45, 65, or 85.