Erweiterte FAQ für PostBase-Frankiersysteme

Datenaustausch/Konnektivität/Betriebs-Software

Welches Betriebssystem wird bei unseren Frankiermaschinen der PostBase-Modellreihe eingesetzt?

Wir setzen bei unseren Frankiermaschinen auf Integrity OS, was als eines der sichersten Betriebssystemen der Welt gilt. Integrity OS wurde mit der Sicherheitseinstufung EAL 6+ von der National Information Assurance Partnership zertifiziert.

Wie sieht die Bug- bzw. Update/Patch- Historie aus?

In unregelmäßigen Abständen, derzeit ca. 1x pro Jahr, wird für jede Modell-Variante von Seiten FP eine neue Version der Betriebssoftware auf unserem Update-Server zur Verfügung gestellt. Diese beinhaltet dann in der Regel neue Features oder Bugfixe.

Die Frankiermaschine erhält beim regulären Portoladeprozess eine Information, dass eine neue Softwareversion zum Download zur Verfügung steht. Der Benutzer kann manuell an der Maschine die Funktion „Remote Service“ (PostBase Classic) oder „Synchronisieren“ (PostBase Vision) aufrufen, um die neue Softwareversion zu downloaden. Ansonsten wird die Maschine beim Ausschalten und einer gleichzeitig vorhandenen aktiven Datenverbindung dass Softwareupdate automatisch durchführen. Die neue Software-Version wird dann beim nächsten Neustart in der Maschine installiert.

Updates können ausschließlich auf dem o.a. Wege vorgenommen werden - es gibt keine Möglichkeit, die Software-Version des Frankiersystems z.B. über den Anschluss eines PCs, USB-Stick oder ähnliches upzudaten.

Ist es möglich, die Maschine für allgemeines Surfen im Internet zu verwenden?

Nein, das ist nicht möglich! Die Maschine verfügt über kein eigenes Webinterface und es kann kein Browser auf dem System ausgeführt werden.

Besteht Kommunikationsbedarf zu anderen Geräten (z.B. Anschluss an einen PC, für weitere Verarbeitungen?)

Der Betrieb aller PostBase-Frankiersysteme ist komplett ohne Zusatzgeräte möglich. Allerdings wird ein PC/Laptop mit Windows10-Betriebssystem oder höher benötigt, um Komfortfunktionen bei einigen Modell-Varianten, z. B. die Einrichtung von individuellen Kurzwahlen, Benutzerbeschränkungen oder detaillierte Listen- und Berichts-Funktionen, zu nutzen.

Kann der Zugriff auf administrative Einstellungen des PostBase-Systems eingeschränkt werden?

Diese Möglichkeit besteht, erfordert aber zur Konfiguration die Zusatzsoftware "PostBase-Navigator" für die PostBase-Varianten Mini, 30/45/65/100 und ONE oder die Einrichtung über das Kunden-Portal MyFP für die PostBase Vision, Fusion und M2 zu erreichen unter https://www.myfrancotyp.com. Im „Auslieferungszustand“ sind alle administrativen Einstellungen frei zugänglich. Mit Hilfe der o. a. Lösungen können PIN-geschützte Benutzer-Rollen mit beschränkten Zugriffsrechten eingerichtet werden.

Ist es möglich, die Navigator-Software (für PostBase Mini, 30/45/65/100, ONE) auch über eine LAN-Verbindung mit der Maschine zu nutzen?

Nein! Grund sind in erster Linie Sicherheitsanforderungen der Deutschen Post AG. Der PC, auf dem die Navigator-Software installiert wird, muss zwingend per USB mit dem Frankiersystem verbunden sein.

Wie erfolgt die Synchronisierung der Daten zwischen MyFP-Portal und den PostBase Vision / Fusion / M2 Frankiersystemen?

Um die im MyFP-Portal vorgenommenen Einstellungen in die PostBase Vision zu übertragen, benötigt das Frankiersystem eine aktive Internetverbindung über Port 443 (https). MyFP-Portal bietet auch diverse Auswertungs- und Berichts-Funktionen (siehe MyFP-Portal). Die benötigten Verbindungen sind immer ausgehend und werden entweder manuell oder automatisch durch die Maschine initiiert. Alle Verbindungen sind verschlüsselt und durch eine Mutual-SSL-Authentification abgesichert.

Besteht die Möglichkeit, über das Internet „von außen“ auf die PostBase-Frankier-Systeme zuzugreifen?

Nein! Es besteht nicht die Möglichkeit, per Remote auf die Systeme zuzugreifen. Die Maschine ist lediglich mittels Ping im internen Netzwerk zu erreichen.

Ist ein Virenschutz auf den PostBase-Frankier-Systemen installiert?

Nein! Wir sehen dafür auch kein Erfordernis. Neue Software-Versionen und Software-Komponenten (z.B. Tariftabellen oder Klischees) gelangen grundsätzlich und ausschließlich über eine gesicherte Verbindung mit den FP-Servern in die Maschine. Ein Zugriff durch Dritte auf die Maschinen-Software ist deshalb nicht möglich.

Wie stellt Francotyp-Postalia dann den Virenschutz für die PostBase-Frankiersysteme sicher - z.B. durch VPN, Virenscanner, Firewall?

Die Maschinen kommunizieren per http (Port 80) und https (Port 443) Protokoll mit den zentralen FP-Servern. Dabei wird die Kommunikation kryptografisch verschlüsselt. Die unverschlüsselte und nicht kundenspezifische Kommunikation über Port 80 wird nur zur Abfrage der Serververfügbarkeit über den von Ihnen eingestellten DNS-Server verwendet. Die Sicherheit dieser Kommunikation wird im Rahmen der Zulassung der Frankiermaschinen von der Deutschen Post AG zertifiziert.

Kann ein Proxy-Server in den PostBase-Systemen eingerichtet werden?

Ja, das ist möglich. Für die Nutzung, müssen die Proxy-IP und der verwendete Port manuell im PostBase-System eingetragen werden. Bei Nutzung der Proxyserver-Funktion ist zu beachten, dass wir die IP des Proxys oder die URL hinterlegen können, aber kein automatisches Konfigurations-Script verarbeitet werden kann. Es werden Proxy-Server ohne Authentifikation unterstützt. Bei Bedarf kann die PostBase auch ‘basic’ oder ‘digest’ Authentifikations-Methoden unterstützen, (Benutzung eines Benutzernamen und Passwort; „digest“ benutzt eine MD5 checksum).
Die Maschine benötigt eine Mutual-SSL-Authentication, um mit den FP-Servern zu kommunizieren. NTLM wird als Authentifikations-Methode nicht unterstützt !

Ich möchte die Internetverbindung der Maschine, an der Firewall auf die Kommunikation mit dem Server von Francotyp-Postalia beschränken. Welche Ziel-URL‘s sind dafür frei zu geben?

Folgende Kommunikations-Adressen sind in der Firmware der PostBase-Systeme fest (nicht änderbar) hinterlegt, antworten nicht auf Ping-Anfragen und können auch nicht im Browser geöffnet werden.:

Model	IP-Adressen	URL
PostBase Mini	193.29.243.134	5ins.francotyp.com (wird von der Installationssoftware verwendet)
	193.29.243.134	5mabdeu.francotyp.com
	193.29.243.132	5mabdeu2.francotyp.com
	193.29.243.132	5madeu.francotyp.com
	193.29.243.134	5madeu2.francotyp.com
PostBase Classic / 100 / ONE	193.29.243.134	ins.francotyp.com (wird von der Installationssoftware verwendet)
	193.29.243.134	mabdeu.francotyp.com
	193.29.243.132	mabdeu2.francotyp.com
	193.29.243.132	madeu.francotyp.com
	193.29.243.134	madeu2.francotyp.com
PostBase Vision / Fusion / M2	193.29.243.134	vins.francotyp.com (wird von der Installationssoftware verwendet)
	193.29.243.134	vmabdeu.francotyp.com
	193.29.243.132	vmabdeu2.francotyp.com
	193.29.243.132	vmadeu.francotyp.com
	193.29.243.134	vmadeu2.francotyp.com

Unsere Server benutzen eine Mutual SSL Authentication. Bitte deaktivieren Sie einen Paketfilter für diese Verbindung. Jegliche Veränderungen unserer Datenpakete führen zum Abbruch der Datenverbindung und zu einer Fehlermeldung.

Wie kommunizieren die PostBase Maschinen mir der FP-Infrastruktur ?

Für Nachrichten zwischen dem PostBase-System und der FP postalischen Infrastruktur wird fast immer das HTTPS-Protokoll verwendet.
Die Nachrichten werden ausschließlich mit TLS (Transport Layer Security) Version 1.2 gesichert. Standardmäßig wird der Port 443 verwendet, der jedoch von den Benutzern geändert werden kann.
Das HTTP-Protokoll kann in sehr seltenen Fällen verwendet werden, wenn die Sicherheitseinrichtung eines Systems defekt ist. Dies verhindert, dass eine sichere TLS-Sitzung aufgebaut werden kann. In diesem Modus ist nur eine sehr eingeschränkte Auswahl an Diagnosediensten verfügbar und es werden keine postalisch sensiblen Daten übertragen.
Das System unterstützt keine Dienste, bei denen es als Netzwerkserver fungiert.
CMP wird für die Netzwerkdiagnose (z. B. Ping) unterstützt. Die Protokolle UDP und TCP/IP v6 werden nicht unterstützt, ebenso wenig FTP und Telnet.
Beim Herstellen von HTTP- oder HTTPS-Verbindungen stellen PostBase-Systeme immer eine Verbindung zur FP postalischen Infrastruktur her, indem sie eine von mehreren Standard-URLs verwenden, die in der Anwendungsfirmware fest codiert sind. Es werden mehrere URLs verwendet, um betriebliche Flexibilität zu ermöglichen und für Eventualitäten gerüstet zu sein.

Im Normalfall werden die Nachrichten zwischen dem Mailing-System und den FP-Servern über das HTTPS-Protokoll übertragen, das durch den TLS-Mechanismus (Transport Layer Security) gesichert ist. SSL wird nicht unterstützt. Die TLS-Sitzung verwendet die folgenden Sicherheitsmechanismen

Mechanism	Implementation
Protokoll	TLS 1.2 (only)
Cipher suite	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (also known as ECDHE-RSA-AES128-SHA256)
Schlüsselaustausch / Authentifizierung	Mutual authentication using elliptic-curve Diffie-Hellmann, RSA
Verschlüsselungsmethode	AES 128 CBC
Integrität der Daten	SHA-256

Darüber hinaus wird die Sicherheit sensibler Daten zwischen dem Sicherheitsgerät und der FP postalischen Infrastruktur durch eine sichere End-zu-End-Sitzung gewährleistet, die von der TLS-Sitzung umschlossen wird.

Zertifikate

In einigen Fällen haben Kunden nach der Ausführung des Verbindungsassistenten immer noch Probleme, ein PostBase-System mit ihrem internen Netzwerk zu verbinden. Es kann eine Meldung ähnlich der unten stehenden angezeigt werden:

"Verbindung zum FPI ist nicht möglich, bitte überprüfen Sie Ihre Verbindungseinstellungen"

Lokale Computernetzwerke sind alle individuell und unterschiedlich, und einige Kunden haben besonders hohe Sicherheitsstandards. In solchen Situationen können mehrere Firewalls im Einsatz sein - zum Beispiel eine Windows-Firewall und eine weitere innerhalb der Organisation. Häufig versuchen Firewalls, die für HTTPS-Verbindungen (Port 443) verwendeten Sicherheitszertifikate zu überprüfen. Insbesondere erwarten sie oft ein Zertifikat, das von einem der bekannten, seriösen Aussteller wie Symantec und GeoTrust unterzeichnet wurde.
Dienstanbieter, die eine Public-Key-Infrastruktur wie FP betreiben, können auch ihre eigenen Zertifikate ausstellen, was FP auch macht. Der Betrieb von FP wird von mehreren Postbehörden und anderen unabhängigen Prüfstellen reguliert und regelmäßig kontrolliert, so dass der Zertifizierungsstelle von FP in gleicher Weise vertraut werden kann. FP beglaubigt keine Zertifikate Dritter.
Die gesamte Kommunikation mit den Systemen von FP wird daher von der FP-eigenen Zertifizierungsstelle zertifiziert. Dies bedeutet, dass Systemadministratoren je nach den eingerichteten Sicherheitsmechanismen die Sicherheitszertifikate von FP in ihr eigenes lokales Netzwerk importieren müssen.
Sollte Sie das Sicherheitszertifikat benötigen, melden Sie sich bitte bei unserem Support (support@francotyp.com)

Welche Datenvolumen fallen bei den Daten-Verbindungen der PostBase-Frankier-Systeme an?

Für die gängigsten Dienste beim Betrieb des Frankiersystems fallen die u.a. Datenvolumen an: Portoladungen – ca. 50 kB; Aktualisierung von Tariftabellen (neue Portowerte) – ca. 32 kB; Download von Werbeklischees – durchschnittlich ca. 16 kB pro Klischee; Diagnoselisten, postalische Zusatz-informationen – ca. 2 MB; Firmware-Update – ca. 30 - 40 MB

Ich möchte unser PostBase-Frankiersystem mit festen IP-Adressen versehen. Dies würde ich gerne über IP-Adress-Reservierung auf unserem DHCP Server umsetzen woher bekomme ich vorab die dafür erforderliche MAC-Adresse des Gerätes?

Die individuelle MAC-Adresse wird für jedes PostBase-Frankiersystem erst im letzten Produktionsschritt in die Onboard-Netzwerkkarte der PostBase geschrieben. Anschließend wird die Maschine verpackt -die MAC-Adresse ist Bestandteil der Informationen mit den Serien-Nummern des Karton-Aufklebers und damit von außen lesbar. Die Belieferung Ihres Auftrags erfolgt dann vom Fertigwaren-Lager unserer Produktionsstätte. Die für Sie relevante MAC-Adresse steht deshalb erst bei Übergabe der Sendung an den Logistik-Dienstleister fest. Es ist uns daher nicht möglich ihnen die MAC-Adresse vorab mitzuteilen. Sie können diese aber sofort nach dem Eintreffen der Maschine in ihrem Haus vom Kartonaufkleber übernehmen.

Welche Übertragungsfrequenz werden für die WLAN-Funktion in der PostBase Vision / Fusion / M2 verwendet ?

Eine WLAN-Schnittstelle ist bei der PostBase Vision / Fusion / M2 vorhanden. Sie ist eine transparente Alternative zu der Ethernet-Verbindung. Dazu sind zwei Antennen in das Mailingsystem eingebaut.

WLAN-Verbindungen entsprechen den folgenden Standards:
IEEE 802.11 b/g/n, auch bekannt als WiFi 4.
Für die WLAN-Kommunikation wird nur das 2,4-GHz-Band verwendet. Die folgenden Datenraten werden unterstützt:

- 1, 2, 5,5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbit/s nach IEEE 802.11 b/g
- MCS-Index 0-15 (bis zu 144 Mbit/s) unter IEEE 802.11 n

Ähnlich wie die kabelgebundene Ethernet-Verbindung unterstützt die WLAN-Verbindung TCP/IP mit IP v4.

Wenn sowohl Ethernet- als auch WLAN-Verbindungen verfügbar sind, wird immer nur eine verwendet. Die kabelgebundene Ethernet-Verbindung hat immer Vorrang. Wenn eine kabelgebundene Ethernet-Verbindung verfügbar wird, während das System die WLAN-Verbindung verwendet, schaltet das System sofort auf die Kabelverbindung um.

Kanal	Frequenz (MHz)	Countries	Kanal	Frequenz (MHz)	Countries	Kanal	Frequenz (MHz)	Countries
1	2412	All	6	2437	All	11	2462	All
2	2417	All	7	2442	All	12	2467	Not USA
3	2422	All	8	2447	All	13	2472	Not USA or CAN
4	2427	All	9	2452	All	14	2484	Only JPN (802.11b)
5	2432	All	10	2457	All			

WLAN Authentifizierung in der PostBase Vision / Fusion / M2

Es wird nur WPA-Personal mit einem Pre-Shared Key unterstützt. Weder WPA-Enterprise noch Wi-Fi Protected Setup (WPS) werden unterstützt.

WLAN Verschlüsselung (PostBase Vision / Fusion / M2)

Der verwendete WLAN-Verschlüsselungsmodus hängt von dem gewählten WLAN-Sicherheitsprotokoll ab. Der WiFi-Zugangspunkt definiert immer die verfügbaren Sicherheitsprotokolle. Wenn das Netzwerk anhand einer Liste eingerichtet wird, wird das Protokoll mit dem Zugangspunkt ausgehandelt. Wenn das Protokoll manuell eingestellt wird, wird die verwendete Methode im Mailing-System vom Benutzer definiert. Die folgenden Protokolle sind verfügbar:

Security protocol	Encryption
Open	None
WPA	WEP or TKIP
WPA-2	CCMP (based on AES)

Beachten Sie, dass zusätzlich zur WLAN-Verschlüsselung die Nachrichten zwischen dem Mailing-System und dem Gateway-Server auch durch eine HTTPS-Sitzung geschützt werden

WLAN Signalstärke (PostBase Vision / Fusion / M2)

Die Signalqualität ist entscheidend, wenn ein Frankiersystem über eine WLAN-Verbindung angeschlossen wird. Eine schlechte Signalqualität kann zu hohen Fehlerraten und entsprechend niedrigen Datenübertragungsraten führen. Dies ist besonders wichtig beim Herunterladen von Software-Updates und Portotariftabellen. FP rät davon ab, Geräte mit WLAN-Verbindung in der Nähe von anderen Geräten zu betreiben, die Mikrowellen im 2,4-GHz-Band erzeugen, wie z. B. Mikrowellenherde.
Beim Verbindungsaufbau versucht das Frankiersystem immer, eine Verbindung zu dem Access Point oder Repeater herzustellen, der die beste Signalqualität für die jeweilige SSID (Verbindungsname) aufweist. Die Zugangspunkte und Repeater sollten so platziert werden, dass eine optimale Signalqualität gewährleistet ist.
Idealerweise sollten sich die Systeme in einem Abstand von 3 m zu einem Zugangspunkt oder Repeater befinden, dessen Signalstärke nicht absichtlich verringert wurde.

Es dürfen keine Fremdgeräte in unser Firmen-Netzwerk eingebunden werden oder wir haben keinen Internet-Anschluss. Welche anderen Möglichkeiten gibt es, die Datenverbindungen für die PostBase-Frankiersysteme zu ermöglichen?

Für diese Fälle bieten wir ein optionales LTE-Kit für PostBase-Frankiersysteme an. Das LTE-Kit für PostBase-Frankiersysteme stellt eine komfortable Alternative zur direkten Einbindung der PostBase-Modelle in das Netzwerk des Kunden über den integrierten LAN- oder WLAN-Anschluss dar.

Wir empfehlen diese Lösung immer dann, wenn eine Netzwerkeinbindung des Frankiersystems aus technischen oder „politischen“ Gründen nicht möglich ist. Das LTE-Kit kann mit eigener Kunden-SIM-Karte oder einer von FP überlassenen SIM-Karte (bei Abschluss eines entsprechenden Vertrags) betrieben werden. Die SIM-Karten von FP nutzen dabei das Mobilfunknetz der Deutschen Telekom.

Meine MAC-Adresse wird mit sechs Nullen in meinem Windows-Server- System aufgefüllt. Warum ist das so?

Die PostBase-Frankiersysteme verwenden normal eindeutige MAC-Adressen mit einer Länge von 6Bytes – gemäß Definition für Ethernet-Protokolle. Der DHCP-Server verwendet nicht eins-zu-eins diese MAC-Adressen, sondern eindeutige ID‘s.

Diese eindeutigen ID‘s (in der englischen Version des Microsoft DHCP-Servers als „Unique ID“ bezeichnet) sind ein DHCP-Parameter, welcher im RFC2132 Section 9.14 als „Client-Identifier“ beschrieben ist. (http://tools.ietf.org/html/rfc2132#section-9.14)

Für die PostBase-Frankiersysteme wird als eindeutige ID die MAC-Adresse des Ethernet-Adapters aufgefüllt (gepadded) und mit sechsmal dem Zeichen „0“ verwendet. Die MAC-Adresse eines Ethernet-Adapters hat eine Länge von 6 Byte. Um diese MAC-Adresse darzustellen, werden bei hexadezimaler Darstellung 12 Zeichen benötigt. Ergänzt um die sechsmal „0“ ergibt sich eine Länge von 18 Byte + 2 Byte Overhead = 20 Byte. Diese Eindeutige ID dürfte sogar ein voll qualifizierter Domänen-Name sein.

Ansonsten wird vom Inhalt nur verlangt, dass er eindeutig ist, und dies wird von der PostBase dadurch erfüllt, dass garantiert wird, dass die MAC-Adresse bereits eindeutig ist. Die PostBase Frankiermaschine verhält sich somit völlig standardkonform.

Haben Sie zusätzliche Fragen?

Sollten Sie weitere Fragen haben, kontaktieren Sie uns bitte unter der Rufnummer: 030 / 220 660 540
Oder senden Sie uns Ihre Frage per E-Mail an: support@francotyp.com
Unter https://fp-francotyp.de/pages/download-bereich finden Sie alle Benutzerhandbücher unserer Frankiersysteme.