International Financial System

Cloud Client Installation and Configuration Guide

version 4.50 and later

Last updated: 16 September 2026

Contact

Postal Technology Centre - Universal Postal Union Weltpoststrasse 4, 3015 Bern - Switzerland

Phone: +41 31 350 31 11

Service Desk Portal: https://support.upu.int

UPU UNIVERSAL POSTAL UNION

This document and the associated software contain proprietary information of the Universal Postal Union (UPU) and are provided under a specific agreement with eligible postal entities stipulating restrictions on use and disclosure. This document and the associated software are protected by law, including, as applicable, copyright laws.

This document and the associated software may not be, partly or as a whole, copied, disassembled, decompiled, modified or reverse-engineered without the express written permission from the UPU.

References in this publication to UPU products, applications, or services do not imply that the UPU intends to, or can make the said software, products, applications, or services, or parts thereof, available in all UPU member countries. Furthermore, no reference to a UPU software, product, application, or service is intended to state or imply that only UPU software, products, applications, or services may be used. Evaluation and verification of operation in conjunction with other products, applications, or services, except those expressly designated by the UPU, are the responsibility of the user.

Any references to particular designations of countries or territories shall not imply any endorsement or judgement by the UPU as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries. Moreover, any references to names of specific companies or products (whether or not indicated as registered) shall not imply any intention to infringe proprietary rights, nor shall it be construed as an endorsement or recommendation on the part of the UPU.

The UPU shall not be liable for any loss or damage arising from, or directly or indirectly connected to, the use of, reference to, or reliance on the associated software or any other UPU product, application, or service, including, but not limited to, any liability arising from negligent misuse, errors, disclosure, undue transfer, loss or destruction of data that may occur.

Any trademarks mentioned or referred to in this document and the associated software are the property of their respective owners.

The information in this document, including uniform resource locators (URLs) and other website references, is subject to change without notice.

Nothing in or relating to this notice shall be deemed or interpreted as a waiver, express or implied, of the privileges and immunities enjoyed by the UPU as an intergovernmental organization and specialized agency of the United Nations.

Copyright © 1996-2026 Universal Postal Union. All rights reserved.

PTC
PostalTechnologyCentre
UNIVERSAL POSTAL UNION

Table of contents

About this document 4
Intended audience 4
How to use this manual 4

Introduction 5
Overview 5
Terminology 5
IFS Components 5
Security in IFS 6
IFS Cloud unsupported in virtualized environments 6

Hardware and software requirements 8
IFS Cloud client requirements 8
Firewall requirements 8
Supported peripherals 9
PTC Enroll Mobile and IFS Mobile 9

Prerequisites 10
Workstation requirements 10
Mobile device requirements 10
Install the PTC Enroll app and enroll your desktop or mobile device 10
Install IFS Mobile 14
Install VMware Horizon Client 15

Accessing IFS Cloud 17
Access IFS Cloud from a workstation 17
Access IFS Mobile 18

About this document

Intended audience

This manual is intended for use by IFS administrators who are responsible for configuring IFS Cloud clients. IFS Cloud clients refer to any workstation or mobile device accessing IFS that runs in the Cloud.

How to use this manual

This manual applies to any IFS applications that run in a Cloud environment, e.g. IFS Cloud.

Before you install and configure your IFS Cloud clients, you must have a basic understanding of how a Cloud environment works.

For information on:

- the basic IFS Cloud concepts, see"Introduction" on the next page
- the hardware and software requirements for your workstation or mobile device, see"Hardware and software requirements" on page 8
- the relevant IFS components and enrollment application to install on a workstation or mobile device, see "Prerequisites" on page 10
- how to access IFS Cloud from a workstation or mobile device, see"Accessing IFS Cloud" on page 17

You may not copy, rewrite or redistribute this document in any form. To do so is a violation of international copyright laws. However, the Postal Technology Centre welcomes your input. For queries or service requests, you can raise them at https://support.upu.int.

Introduction

Overview

IFS Cloud is IFS hosted in a Cloud environment, which can be accessed from a trusted workstation or IFS Mobile.

Terminology

The following terms are used throughout this guide.

IFS Cloud client: Any workstation or mobile device that accesses the IFS Cloud components.

PTC Enrollment solution: A suite of enrollment applications developed by the PTC which reuses the existing PTC Certificate Authority (CA) infrastructure to manage the process of client enrollment for any PTC website or web API. For workstations or mobile devices to use IFS Cloud, they must first be enrolled using the relevant PTC Enrollment application: PTC Enroll Client for workstations and PTC Enroll Mobile for mobile devices. The PTC Enrollment web application manages all enrollment requests.

IFS Components

IFS consists of several distinct software components and supported peripherals.

The following table contains a complete list of IFS components.

	Software components	Description
Database repositories	IFS Production Database	Repository of the IFS production data
	IFS Archive Database	Repository of the IFS archive data
Windows Services	IFS Communication Server	Interfaces with local systems
	IFS Gateway Server	Connection to the UPU EDI network (POST*Net-Finance)
Web Services	IFS API Server	Web Services used to provide operational functions to the local system
	IFS Management Console	The IFS application used for administration and configuration
Applications	IFS Mobile App	App used to provide operational functions on the mobile device
	IFS Web Server	Web application used to provide operational functions via the intranet,

	Software components	Description
		accessed through the IFS Web Client, a browser front-end

Security in IFS

IFS Cloud includes a number of security measures that limit access to IFS application components. It is only available to authorized client workstations and mobile devices.

Only client workstations with valid certificates, credentials and execution rights delivered by the PTC are authorized to connect to IFS Cloud. Similarly, only mobile devices installed with a valid certificate delivered by the PTC are authorized to connect. The table below lists the security measures for client workstations and mobile devices accessing IFS Cloud components.

Client type	IFS component accessed	Security measure
Workstation	IFS Web	Two-way SSL authentication to validate server and client identities
	IFS Management Console	Active Directory (AD) implementation and account management by the PTC
		VMware Horizon Client
Mobile device	IFS API Server	Web server certificate installed on the IFS API Server to secure access to it
		Mobile device certificates are issued and revoked by PTC Enrollment via the PTC-hosted Certificate Authority (CA)

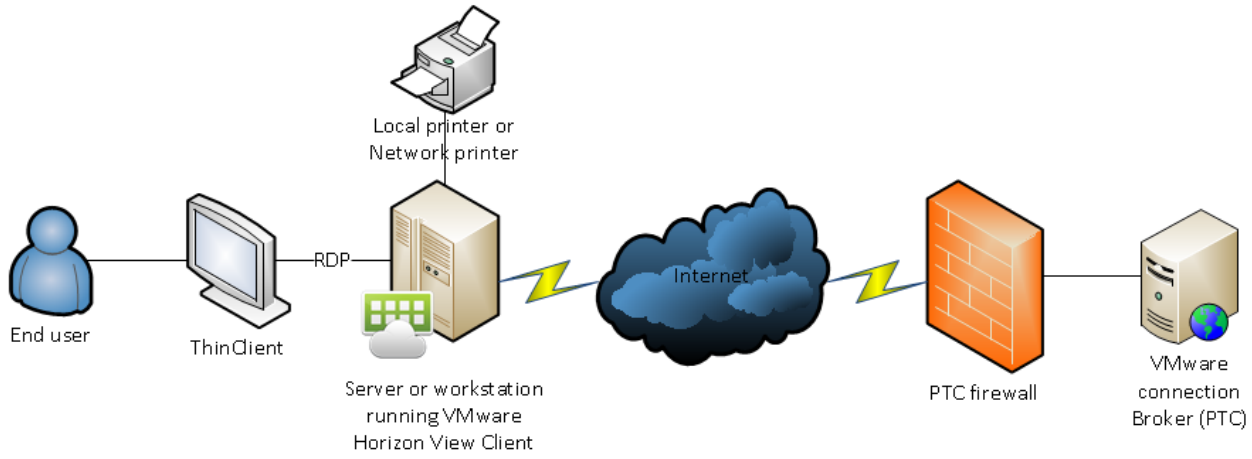
IFS Cloud unsupported in virtualized environments

IFS Cloud is unsupported in a virtualized environment. Locally mapped peripherals do not work when connecting remotely, such as through Remote Desktop.

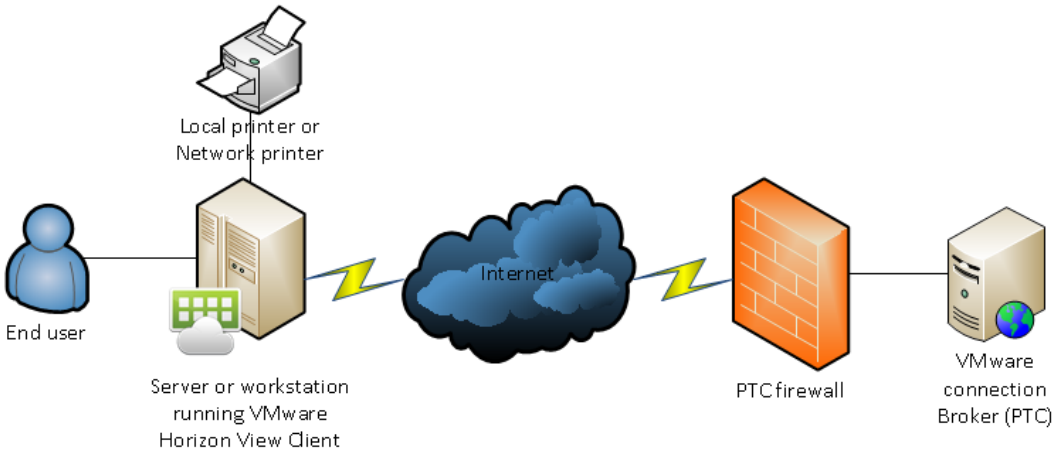
The following diagram illustrates the supported and unsupported scenarios:

- Scenario 1 is the unsupported scenario whereby the user connects to the workstation through a remote connection
- Scenario 2 is the supported scenario whereby the user connects to the workstation directly

Scenario 1 - peripherals (= printers, ...) are not available in IFS Cloud



Scenario 2 – peripherals (= printers, ...) are available in IFS Cloud



Hardware and software requirements

This chapter describes the PTC's recommended minimum hardware and software requirements for IFS Cloud clients.

IFS Cloud client requirements

Except for a compliant browser and the relevant application for enrollment, there is no specific hardware or software requirement for workstations connecting to IFS Cloud. However, business managers accessing the IFS Management Console component must have the VMware Horizon Client installed on their workstation, see "Install VMware Horizon Client" on page 15.

For mobile devices, the only requirement is the installation of PTC Enroll Mobile and IFS Mobile.

Refer to "Prerequisites" on page 10 for details on these components.

Firewall requirements

This section describes the firewall requirements to ensure that a successful connection to IFS Cloud is established.

Communication ports

You must open all the ports listed below to connect to cloud.ptc.post and cloud-preprod.ptc.post.

Port	Transport Protocol
443	TCP
4172	TCP
4172	UDP
8443	TCP
8443	UDP

For improved security, port opening can be restricted to a single IP address of the PTC servers.

Supported peripherals

IFS supports the following peripheral devices.

Laser printers

Hardware	
Document printer	Requires a Windows driver

Receipt printers

Hardware	
Small form factor printer	Requires a Windows driver Print width between 50 and 200 mm

PTC Enroll Mobile and IFS Mobile

Hardware	
Screen size	Minimum 4.3 inch; 7 inch or larger recommended
Network access	Wi-Fi/GPRS (mobile data)
Options	For printing (requires custom development): • Bluetooth • Native printing configuration
Software	
Operating systems	Android 14.0 and 15 (API level 34 and 35) Android 6.0 or later (minimum API level 23)
PDF reader	Any PDF reader software (for IFS Mobile App only)

Mobile device requirement

The mobile device must not be rooted and the screen lock function must be configured with at least a pattern, a PIN, or a password.

Prerequisites

Before you can access IFS Cloud, your workstation or mobile device must already have the required components and must be enrolled.

Workstation requirements

1. Install the **PTC Enroll Client** application and enroll your workstation by submitting a certificate request and downloading a valid certificate.
2. Ensure that your workstation has a compliant browser to access IFS Web.
3. If you are accessing the IFS Management Console, install the VMWare Horizon Client. See "Install VMware Horizon Client" on page 15.

Mobile device requirements

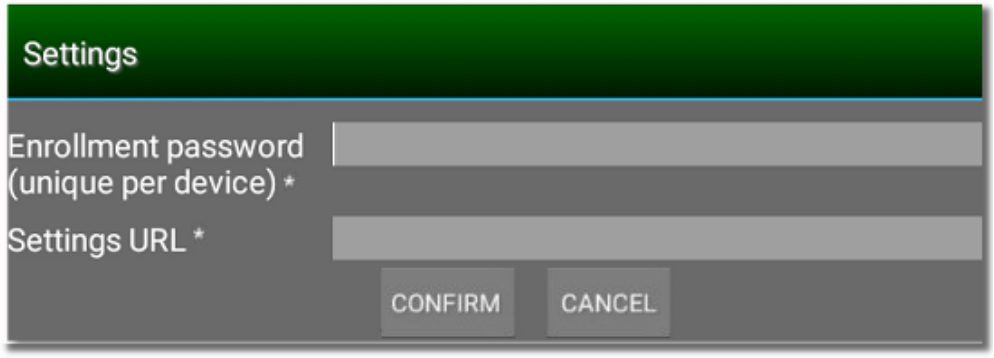
1. Install **PTC Enroll Mobile** and enroll your mobile device by submitting a certificate request and downloading a valid certificate.
2. Install IFS Mobile to access IFS from your device.

Install the PTC Enroll app and enroll your desktop or mobile device

If you are using a desktop to access IFS Cloud, refer to the PTC Enroll Client User Guide at: https://www.upu.int/en/Postal-Solutions/Technical-Solutions/Products/PTC-Enrollment for detailed information on installing PTC Enroll Client and enrolling your desktop workstation.

If you are using a tablet or a mobile device to access IFS Cloud, follow the procedure below to install the PTC Enroll app and enroll your mobile device.

1. On the Google Play Store, search for the PTC Enroll app and install it: https://-play.google.com/store/apps/details?id=ptc.enroll.
2. When the installation process ends, tap **OPEN**. The **Settings** window is displayed.



3. Specify values for the following:

   Enrollment password: Set a unique password for your device; this password is used to authorize installed PTC applications to access the certificate of the mobile device. The

password must be at least eight characters long, containing a combination of letters, numbers and special characters. Keep the password safe and secure, and do not share it with any unauthorized personnel.

Settings URL: Type or paste the URL provided to your organization by the PTC in this field. The pre-production settings URL has the format:

http://enroll.preprod.ptc.post/MobileXXX/settings.xml where XXX is the three-letter operator code, for example, FRA.

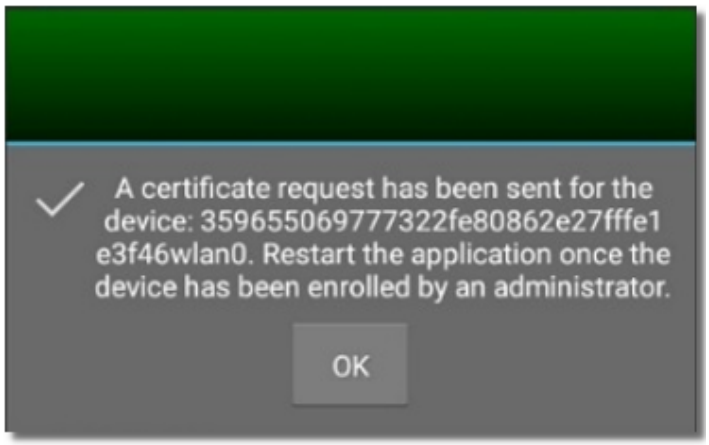
Similarly, the production settings URL for PTC Enroll would be http://enroll.ptc.post/MobileXXX/settings.xml

4. Tap **CONFIRM**. The Certificate Request window appears. The information collected in this screen helps the enrollment manager to identify the enrollment request. PTC Enroll Mobile displays the country based on the value defined in the Settings file. You must fill in values for all the fields in the screen, as follows.

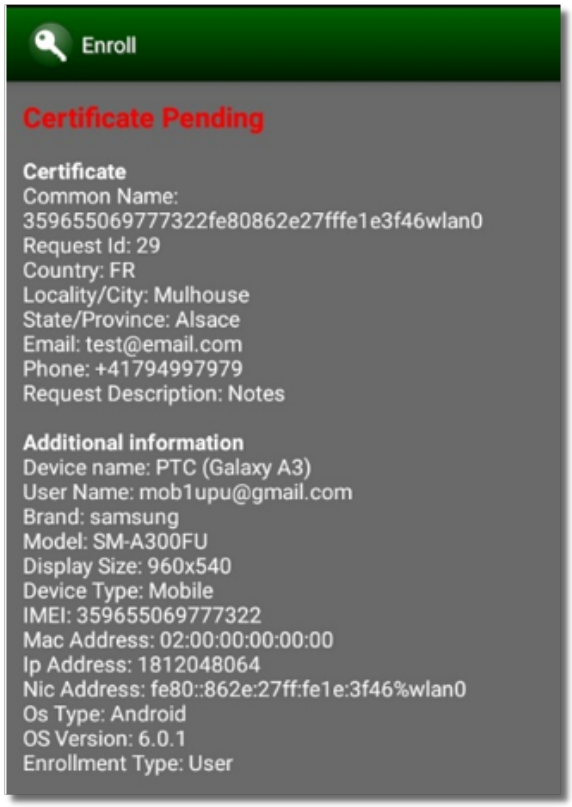
   - Country
   - State/Province
   - Locality/City
   - Email
   - Phone
   - Request Description (Enter information about the request to help the PTC Enrollment Manager identify and approve it easily.)



5. Click **SUBMIT**. PTC Enroll Mobile displays a confirmation message.

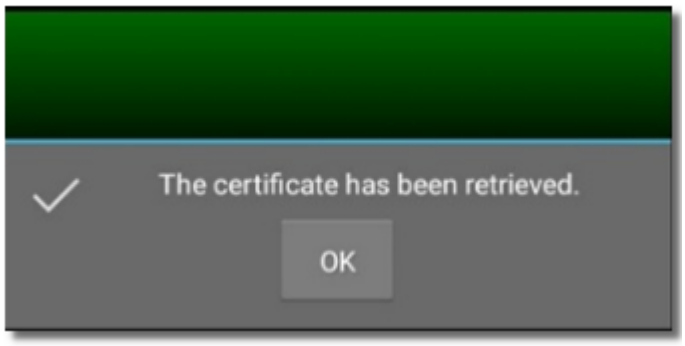


6. Click **OK**. Details of the certificate request submitted are displayed.



7. Communicate the **Request id** to the Enrollment Manager. Often, the enrollment manager for the web workstations and mobile devices is the same. It may take sometime for the Enrollment Manager to approve the request from the PTC Enrollment web application.

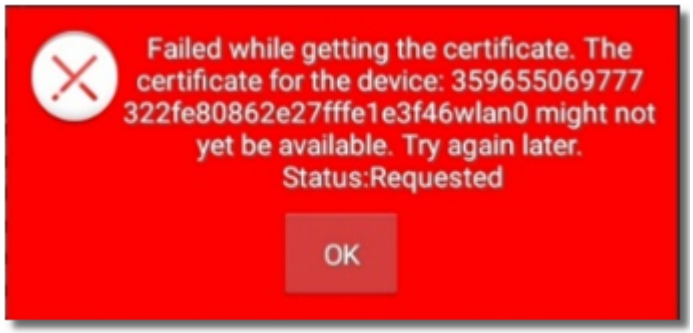
8. After the enrollment has been approved, launch PTC Enroll Mobile. PTC Enroll Mobile retrieves the certificate and installs it.



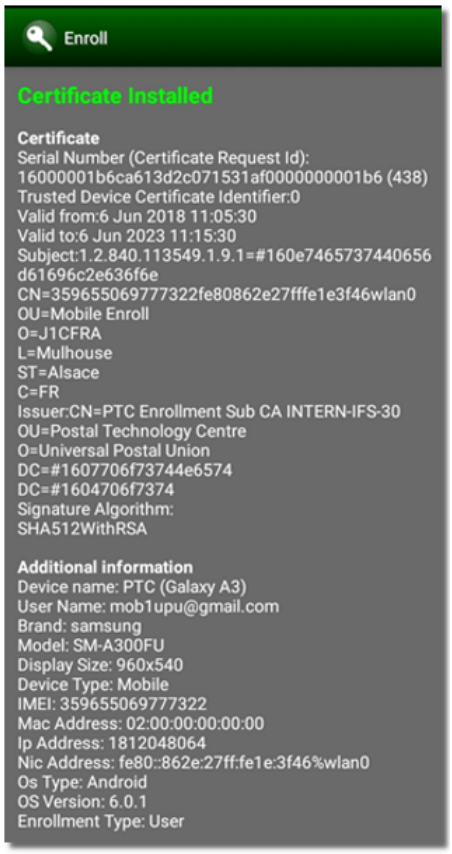
If the enrollment is rejected, PTC Enroll Mobile displays a rejection message.



However, if the certificate has not been issued yet, PTC Enroll Mobile displays a message asking you to check again later.



9. Click **OK**. PTC Enroll Mobile displays the details of the retrieved certificate.



Your certificate is now installed. You are now ready to install or use PTC mobile applications from this device.

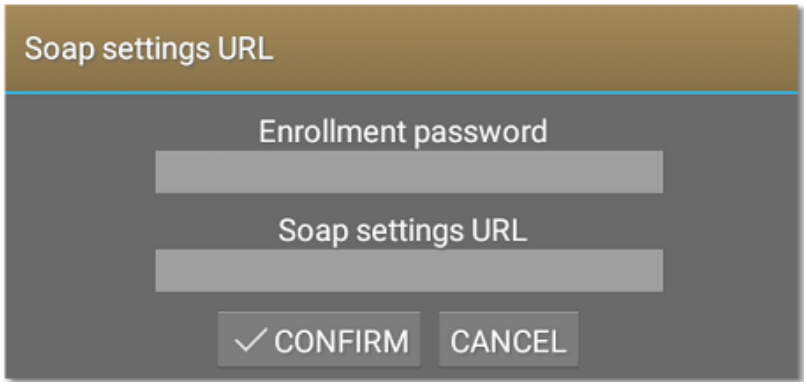
Install IFS Mobile

1. Download the IFS Mobile app (test or production copy) from the Google Play Store.

   Test: https://play.google.com/store/apps/details?id=org.universalpostalunion.ifs.preprod

   Production: https://play.google.com/store/apps/details?id=org.universalpostalunion.ifs.prod

2. When the installation process ends, launch the IFS Mobile app. You will be prompted to enter enrollment information.



3. Specify values for the following:

   Enrollment password - Type the password you created during the PTC Enroll set up.

Soap settings URL - Type or paste the URL provided to your organization by the PTC in this field. For the pre-production environment, an example is: http://XXX.-preprod.ifs.post/J1CXXX_IFSMobile/soap_settings.xml, where XXX is your operator code, for example, FRA.

Similarly, for the production environment, the settings URL to be typed should have the format http://XXX.ifs.post/J1CXXX_IFSMobile/soap_settings.xml.

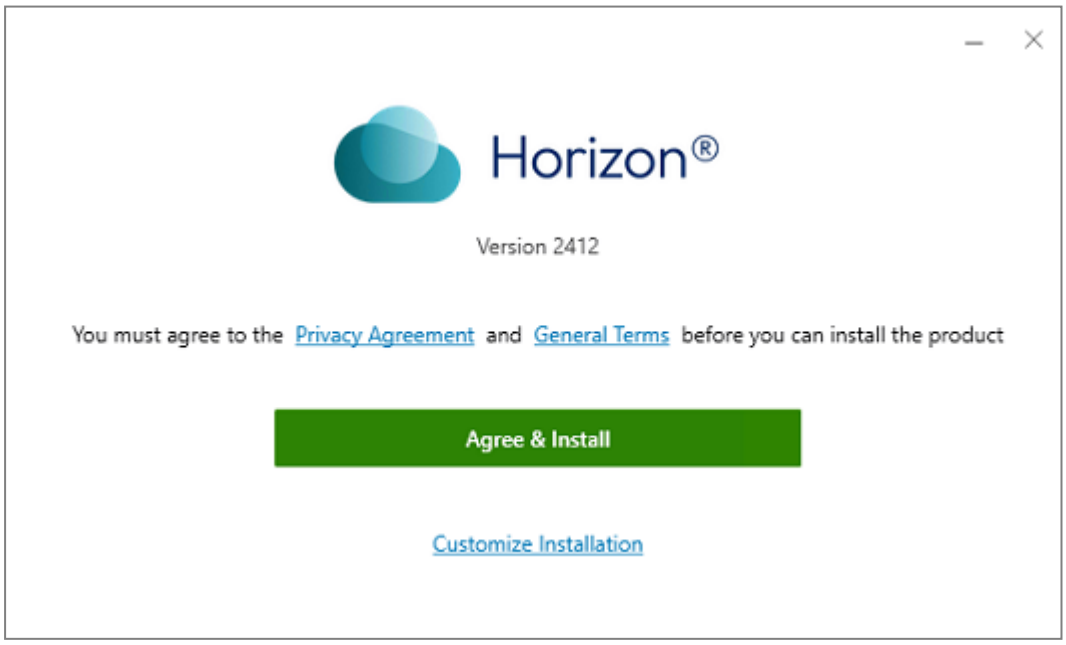
4. Tap **CONFIRM**. You have just completed the installation and configuration of IFS Mobile on the enrolled device.

Install VMware Horizon Client

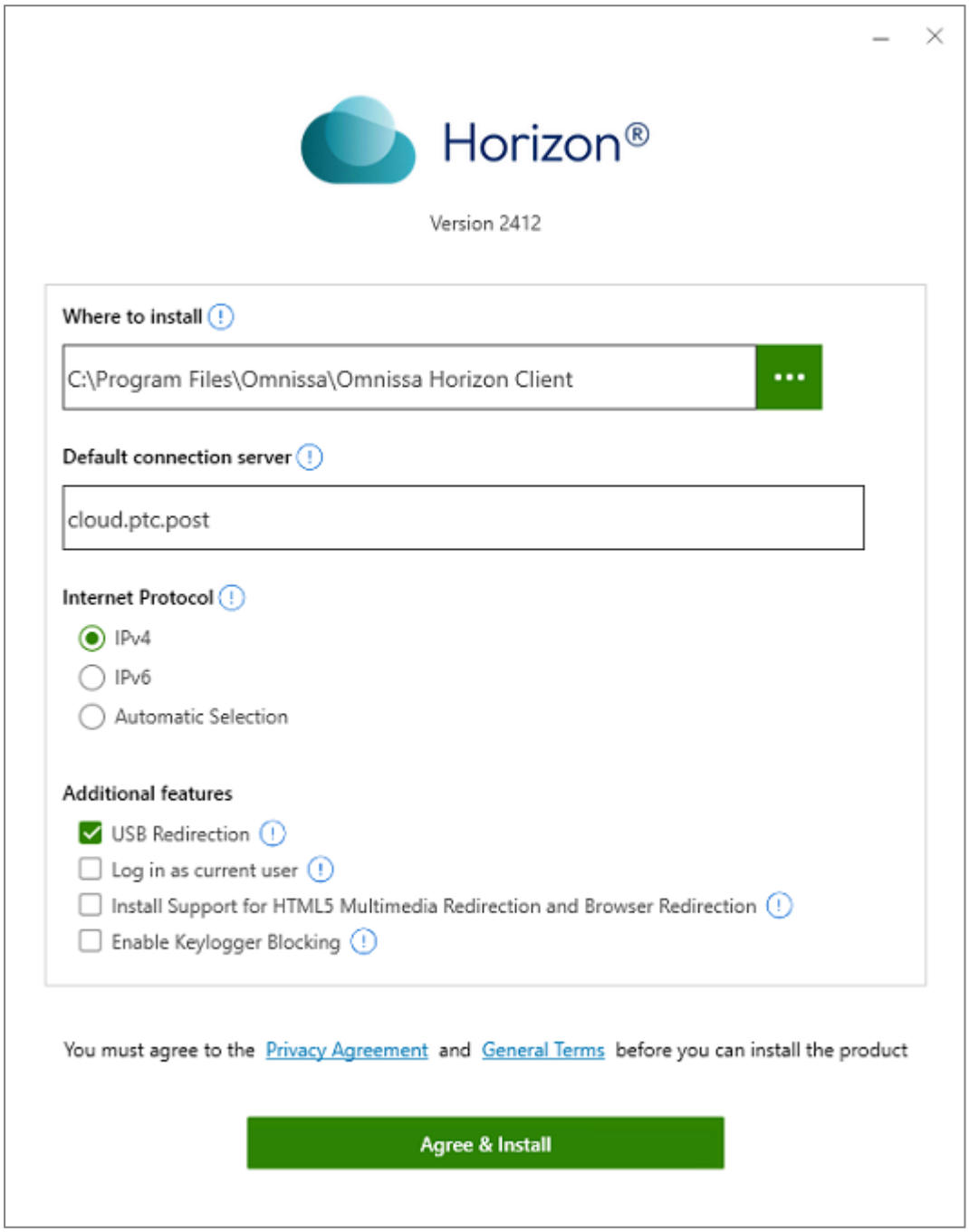
Install VMware Horizon Client only if you are accessing the IFS Management Console component from your workstation.

The PTC recommends installing VMware Horizon Client version 2412.

1. Access the VMWare Horizon Client Downloads page using the following link: https://-customerconnect.omnissa.com/downloads/info/slug/virtual_desktop_and_apps/omnissa_horizon_clients/8.
2. Click on the **Select Version** field and select **2412** from the drop-down list. The PTC recommends installing this version.
3. Double-click the downloaded file to start the installation process.
4. Click **Agree & Install** to install the application with default settings or click **Customize Installation**.
   a. If you choose **Agree & Install**, skip steps 5 to 6.
   b. If you choose **Customize Installation**, proceed to step 5.



5. If you choose **Customize Installation**, set the following values:
   a. **Default connection server** - type cloud.ptc.post for the Production server, cloud-pre-prod.ptc.post for the Pre-production server
   b. **Internet Protocol** - leave the default selection IPv4 as is
   c. **Additional features** - choose only USB Redirection



6. Click **Agree & Install** to start the installation process.
7. Click **Launch** to launch the application.
8. Click **Finish** to complete the installation. You are prompted to restart your computer for the changes to take effect.

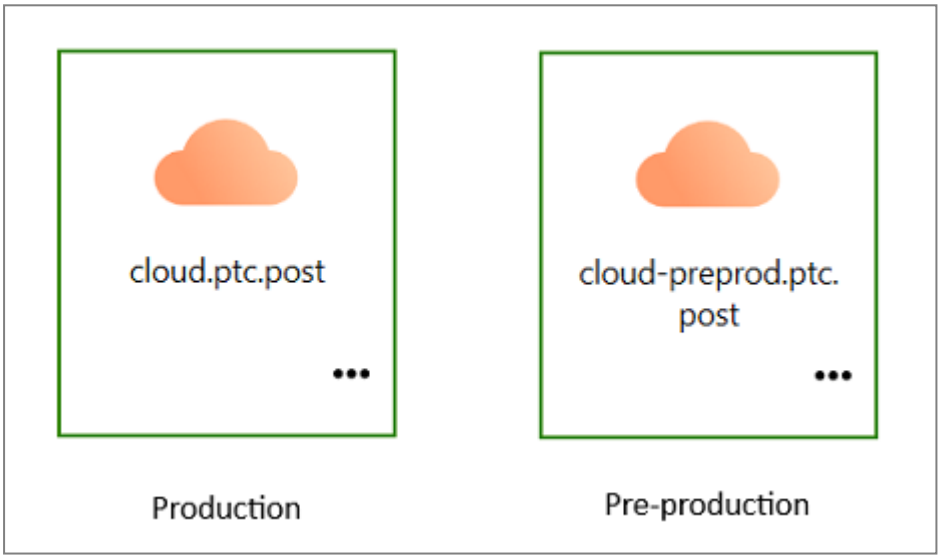
Accessing IFS Cloud

Access IFS Cloud from a workstation

You must have already enrolled your workstation before accessing IFS Management Console or IFS Web. See the PCT Enroll Client User Guide, accessible at https://www.upu.int/en/Postal-Solutions/Technical-Solutions/Products/PTC-Enrollment for details.

Access IFS Management Console

1. Start the VMware Horizon Client and double-click the relevant server icon: cloud.ptc.post for Production or cloud-preprod.ptc.post for Pre-production.



2. The application prompts you to log in. Enter the credentials below:
   - User name: XXX-UserName (where *XXX* is your operator code)
   - Password: your existing IFS Cloud password
   - Domain: Depending on the environment you are accessing, this field displays CLOUD for the Production environment, PPROD for the Pre-production environment



3. To perform administrative functions in IFS Cloud Management Console, double-click the icon below and enter your login credentials. IFS may request you to change your password if it is your first time to log in, or if your password does not comply with the password settings defined for your organization. You can change your password by logging in to IFS Web and selecting the **Change password** function from the **Administration and configuration** menu.



Access IFS Web

1. Open your browser and enter the IFS Cloud URL provided to you by the PTC.
2. Log into IFS. IFS redirects you to the **Change password** screen if it is your first time to log in, or if your password does not comply with the password settings defined for your organization. You must change your password to access IFS.

Access IFS Mobile

You must have already enrolled your mobile device to use IFS. See the PTC Enroll Mobile User Guide, accessible at https://www.upu.int/en/Postal-Solutions/Technical-Solutions/Products/PTC-Enrollment for details.

1. Open the IFS Mobile app on your mobile device.
2. Log into IFS. IFS prompts you to change your password if it is your first time to log in, or if your password does not comply with the password settings defined for your organization.