# Cegid Notilus Technical Prerequisites

## Public & International Organizations (PIO) - v10

Distribution: public document

Version: June 2025

cegid

# About this document

This document describes the technical prerequisites associated with the **Cegid Notilus Public & International Organizations (PIO)** solution in SaaS (Software as a Service) mode published, hosted and operated by Cegid.

This document covers the technical prerequisites relating to workstations, network and telecommunications aspects as well as peripherals. Compliance with these prerequisites is essential for the proper functioning of these solutions.

Cegid cannot be held liable in the event of a malfunction of the solution linked to their non-compliance.

In the case of using other Cegid solutions, the Customer must ensure that they respect the recommendations common to the entire proposed offer. For personalized advice, contact your Sales Engineer.

If users are distributed across distinct geographic sites, it is up to the client to check the latency tests from each of the user sites identified.

| | |
|---|---|
| Last update | 02 June 2025 |

# TABLE OF CONTENT

# 1. Provision of Cegid Notilus

The **Cegid Notilus Public & International Organizations** (PIO) solution is an application available in SaaS mode, entirely hosted and operated by Cegid.

# 2. Access to the application

The application access URL is made up of the application hosting domain, prefixed with the application name.

This name can contain a maximum of 15 characters and is subject to current standards (RFC 3986).

The final URL for accessing the application must be decided before the first installation of the application, subject to availability and validation by the Cegid teams.

# 3. Workstation

## 3.1. Browsers

Navigation on the Cegid Notilus platform is carried out only in HTTPS via the TLS 1.2 protocol.

Cegid Notilus requires a modern web browser to function properly:

- Users accessing the product can use the two latest versions of Chrome, Firefox, and Edge (Blink/Chromium engine).
- Browsers must be configured with sufficient cache memory (minimum 128 MB).
- The browser must allow the opening of tabs and pop-ups from the application and the sites it includes (e.g., the online booking portal).

The Cegid Notilus application must be configured as a trusted site.

## 3.2. Screen resolution

The minimum screen resolution for Cegid Notilus (PIO) is 1440 by 900, dpi 100%.

The recommended screen resolution is 1920 by 1080, dpi 100%.

## 3.3. Email client

To communicate emails, Cegid Notilus requires an HTML 5 compatible client.

The links must be active and allow access to the Cegid Notilus website.

## 3.4. PDF reader

Cegid Notilus offers several extractions in PDF format. A PDF reader such as Acrobat Reader 21 or higher is required to view them.

## 3.5. Spreadsheet

Cegid Notilus' standard spreadsheet extractions are in CSV, XLS, or XLSX format. Therefore, you must have a spreadsheet program capable of reading Excel 2007 .XLSX/.XLS files.

Extraction compatibility is guaranteed for Microsoft Excel 2010 and later.

## 3.6. Online ticketing reservation module

Self-Booking Tools (SBT) platform accessed by Cegid Notilus and Notilus Travel Hub (Goelett, Cytric...) must be set as trusted sites.

The browser must accept cookies.

## 3.7. Available languages

The following languages are available in standard:

- French
- English

# 4. TECHNICAL POINTS

## 4.1. Encapsulation

For security reasons, Notilus cannot be encapsulated in a third-party application (I-FRAME).

Accessing Cegid Notilus requires opening a browser window.

## 4.2. Network equipment

Network equipment (proxy, reverse proxy, load balancer, WAF, etc.) between the user workstation and the Cegid Notilus web server must not alter each user's individual session information.

Dynamic pages must not be cached and must remain individualized. Flows between the user workstation, tablet, or mobile phone and the web server must not be altered.

The application's web services are not designed to support reverse proxies.

Cegid cannot be responsible for configuring the client's network equipment.

## 4.3. Network protocols

The client's network configuration must allow each user to quickly access the hosting center (in less than 100 milliseconds).

The protocol used is HTTPS for the web application and SFTP for file transfers.

We do not offer VPN tunneling between our infrastructure and that of our clients.

## 4.4. Messaging

Cegid Notilus emails are sent from our email delivery service provider to your users with the following addresses formats: "@notilus-pio.cegid.cloud" or "@notilus-common-services.cegid.cloud".

## 4.5. Data encoding

The data entered and imported must correspond to the ISO/IEC 8859-1 (Latin 1) encoding.

Characters specific to other encodings, including ISO/IEC 2022 and Unicode, are not supported by the application.

# 5. AUTHENTICATION OPTIONS

## 5.1. Connection methods to the web version

*Local authentication*

Login and password credentials are managed by Cegid Notilus. This information is entered upon entering Cegid Notilus.

- Passwords are secured using ARgon2Id hashing.
- Users can be required to enter complex passwords.
- Passwords expire automatically, with a configurable period between 30- and 90-days following registration.
- A history of the previous 3 to 5 passwords ensures regular renewal.

Unsuccessful attempts to access the application are recorded; the application locks accounts that experience too many failed login attempts.

In the event of unsuccessful attempts, the application requests Recaptcha validation (Version 2) in addition to the entry.

Upon initial login, an account activation process via email is required.

*SAMLv2 Identity Federation*

Cegid Notilus can be connected to a compatible IdP via the SAML transport protocol in IdP-initiated or SP-initiated mode.

The encryption of authentication tokens between Cegid Notilus and the IdP is SAML V2. The Client is responsible for setting up the IdP configuration.

## 5.2. Mobile version connection methods

*Entering credentials*

The "I know my credentials" option allows you to connect to the mobile application by entering the customer code (indicated in the URL of your Cegid Notilus application) and using the credentials of the web version.

*Using the QR code*

The "I flash my code" option allows you to authenticate yourself on the mobile application by first connecting to the Notilus application via a computer and scanning the QR code proposed in the user profile.

# 6. Cegid Notilus Mobile Application (PIO)

## 6.1. Delivery method

**The Cegid Notilus PIO mobile application** is available on the Google Play store and Apple store. This is the only delivery method for the mobile application.

The delivery of the mobile application to the employees of each client is the responsibility of the client.

For optimal operation of the Mobile version, the web application must always be up to date with new version releases.

## 6.2. Operating System

- Android
- iOS

Compatible OS versions are listed in the Google Play and App Stores.

## 6.3. Authorisation and photo taking

**The following authorisations must be granted:**

- Access to the camera
- Access to files and multimedia content
- Notifications

The way of creating expenses in mobility is based on receipts scanning using photos and an AI engine to fulfil and categorize expenses.

To access data, the Cegid Notilus application uses standard HTTPS access.

The push notification feature requires a connection to the Cegid Notilus Mobile Hub.

## 6.4. Device and application

The device must have a touchscreen of at least 4 inches.

# 7. DEMATERIALIZATION WITH PROBATIVE VALUE

## 7.1. Electronic document management

Documents uploaded to the Cegid Notilus EDM cannot exceed the size limit of 3 MB per document. Standard storage (excluding probative value) of supporting documents for expenses is carried out for a maximum period of 48 months, without exceeding the end date of the Contract; it will not be possible to retrieve a document beyond the 48 months of the standard storage contract or beyond the end of the Contract.

Only JPG/JPEG, PNG, BMP, GIF and PDF document formats are accepted. Dangerous extensions such as .EXE, .JS, .BIN, .BAT, .VBS, etc. are prohibited.

Users of the Cegid Notilus mobile application can directly scan their supporting documents from their smartphone with it.

WARNING: PDF must not contain forms, be encrypted or signed. Only PDFs containing only text and/or images are allowed.

## 7.2. Secure dematerialization & archiving with probative value

The integrity of the documents is guaranteed by an "eIDAS" server stamp, the European equivalent of the General Security Reference (RGS), issued by a certified trusted third party. The conservation of the documents is ensured within an Electronic Archiving System (EAS), for a period of Ten (10) years. The files are automatically purged upon expiry (anniversary date).

Only JPG/JPEG, PNG and PDF document formats are accepted to constitute the archive document in PDF/A format, containing the metadata and supporting documents for each expense report.

**END OF TECHNICAL PREREQUISITES WHICH COMPRISE 8 PAGES**