Cegid Notilus Technical Prerequisites

Public & International Organizations (PIO) - v10

Distribution: public document

Version: June 2024

cegid

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	18 June 2024

SUMMARY

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. User 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 latest two versions of Chrome, Firefox and Edge (Blink/Chromium engine).
- Browsers must be configured with sufficient cache memory (minimum 128 MB).
- The browser must accept the opening of tabs, as well as "pop-up" windows from the application and the sites it includes (for example, the online reservation portal).

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

3.2. Screen resolution

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

Recommended screen resolution is 1920 by 1080, 100% dpi.

3.3. Email client

To use the active emails offered in Cegid Notilus, the email client must be compatible with emails in HTML format.

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

Standard spreadsheet extractions from Cegid Notilus are in CSV, XLS or XLSX format. It is therefore necessary to have a spreadsheet capable of reading Excel 2007 .XLSX / .XLS files.

Extraction compatibility is ensured for Microsoft Excel 2010 and higher.

3.6. Online ticketing reservation module

The reservation sites used via Cegid Notilus and Notilus Travel Hub (Goelett, Cytric, etc.) must be configured as trusted sites.

The browser must accept cookies.

3.7. Languages available

Cegid Notilus Public & International Organizations is available as standard in French and English.

4. TECHNICAL POINTS

4.1. Encapsulation

For security reasons, the Cegid Notilus application cannot be encapsulated in a third-party application.

Access to Cegid Notilus requires opening a browser window.

4.2. Network equipment

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

Dynamic pages should not be cached and should remain individualized. The flows between the user station, the tablet or the mobile phone and the web server must not be altered.

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

The configuration of the customer's network equipment cannot be the responsibility of Cegid.

4.3. Network protocols: TCP/IP

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

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

We do not offer the establishment of a VPN tunnel between our infrastructures and those of our customers.

Cegid Notilus emails are sent from our email sending service provider to your users.

4.4. Data encoding

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

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

5. Connection modes to Cegid Notilus

5.1. Basic Authentication

Username/password pairs are managed by the application.

During the first connection, an account activation process by email is mandatory.

Password management

- Passwords are hashed with Argon2Id.
- It is possible to require users to enter complex passwords.
- Password expiration is automatic, the period can be configured between 30 and 90 days following declaration.
- Storing the previous 3 to 5 passwords ensures regular renewal.

Unsuccessful attempts to access the application are recorded, the application locks accounts experiencing too many connection failures.

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

5.2. SAML authentication

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 type.

Setting up the IDP configuration is the responsibility of the customer.

6. Cegid Notilus Mobile Application (PIO)

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

6.1. Operating systems

The Cegid Notilus mobile application is available for smartphones using Android and IOS systems. Compatible OS versions are presented in the Google Play and App Store stores.

6.2. Device and application

The device must have a minimum 4-inch touch surface.

The application can be downloaded from the Google Play and App Store application stores.

The "push notification" functionality requires connection to the Cegid Notilus Mobile Hub.

6.3. Data access

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

7. Dematerialization with Probative Value

The following formats are compatible with the process of dematerialization of documents with probative value:

- JPG/JPEG
- PNG
- PDF
- BMPs
- GIFs

PDFs must not contain forms, be encrypted, or signed.

Only PDFs containing only text and/or images are allowed.