



MERCADO IBÉRICO DEL GAS

Frequently Asked Questions (FAQs) About the Workstation Setup for the MIBGAS Platform

Date: 27/09/2024

Version 1.3

CONTENTS

1	INTRODUCTION	2
2	HELPFUL LINKS	3
3	ANSWERS TO COMMON QUESTIONS	4
3.1	CAN I CONTINUE LOGGING ON WITH INTERNET EXPLORER?	4
3.2	WHERE CAN I MANAGE INSTALLED CERTIFICATES?	4
3.3	WHERE CAN I FIND THE FORTIFY APPLICATION OR ITS LOG?	4
3.4	HOW DO I START FORTIFY BY DEFAULT WITHOUT ADMINISTRATION PRIVILEGES?	5
3.5	HOW DO I RESTART THE FORTIFY APPLICATION?	5
3.6	KNOWN ERROR OR WARNING MESSAGES	6
3.6.1	THE BROWSER DISPLAYS, “THE FORTIFY APPLICATION MUST BE ACTIVE”	6
3.6.2	THE BROWSER DISPLAYS, “THE CONNECTION TO THIS SITE IS NOT SECURE”	6
3.6.3	POP-UP WINDOW BLOCKING	7
3.6.4	AMQP PORT BLOCKED	10
3.6.5	JAVASCRIPT: “EADDRINUSE: ADDRESS ALREADY IN USE”	11
3.6.6	“UNCAUGHT EXCEPTION” MESSAGE AFTER INACTIVITY / SIGNING A TRANSACTION	12
3.6.7	“ERROR TO HANDLE” OR “REFERENCEERROR” MESSAGES	12
3.6.8	THE DOWNLOAD CENTER/TRADING CLIENT WON’T OPEN	13
3.6.9	OPENWEBSTART DISPLAYS THE ERROR, “NO SUITABLE JVM WAS FOUND...”	14
3.6.10	PROBLEM RELATED TO “WEBSITE’S SECURITY CERTIFICATE” WHILE ACCESSING THE SYSTEM	15
3.6.11	DELAY DURING SIGNED TRANSACTION	16
3.7	ADDITIONAL ERRORS NOT FOUND IN THIS DOCUMENT	17



1 INTRODUCTION

This guide contains frequently asked questions following setting the client workstation up to access the MIBGAS Platform, following the directions for initial access via the Edge browser.

The answers provided below do not replace setting the station up properly as discussed in the next section. They do offer a complement to address known problems quickly.



2 Helpful links

All the information needed to set the station up can be found in our repository, [Iberian Gas Market: MIBGAS Spot: Information system: Technical documentation](#) for reference during troubleshooting:

- » Workstation setup guide for accessing the MIBGAS Platform with the Edge browser
- » Frequently Asked Questions (FAQs) About the Setup for the MIBGAS Platform
- » MIBGAS installer for web access with the Edge browser

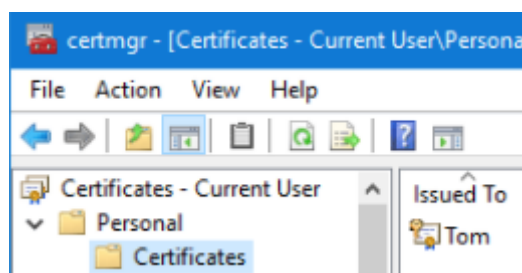
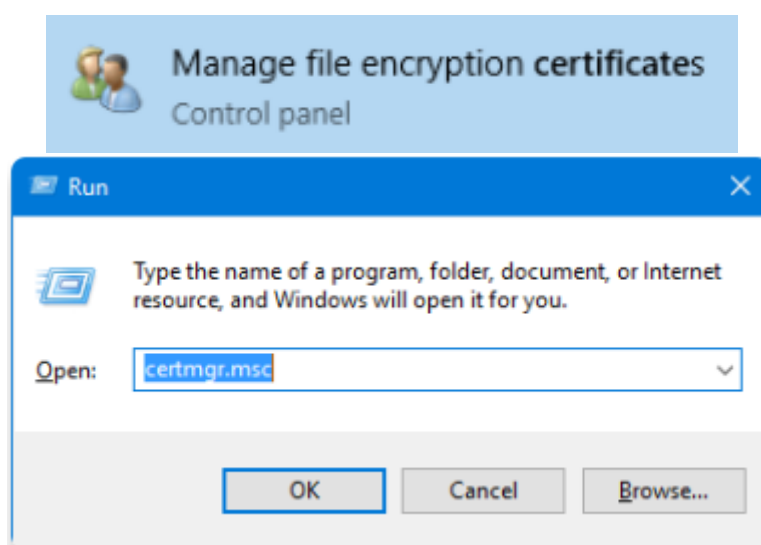
3 Answers to common questions

3.1 Can I continue logging on with Internet Explorer?

As of September 27, 2022, access via Internet Explorer to the gas market platforms will no longer be supported.

3.2 Where can I manage installed certificates?

You can check, import, or delete the digital certificates installed in the Windows certificate store on the computer from Control Panel > Manage user certificates [certmgr]> Certificates - Current user > Personal > Certificates, or from the browser's Security options.



3.3 Where can I find the Fortify application or its log?

During the Installer execution, the Fortify application is installed by default in the path C:\Fortify\Fortify.exe, where C: is the operating system drive.

While running, it can be found in the notification area on the Windows taskbar, among the icons for running programs or within the drop-down menu of hidden icons. It should appear as a blue shield:



You can check the Fortify log by enabling it before accessing the private platform: to do this, right-click on the Fortify icon and go to *Settings > Manage Log > Enable*.

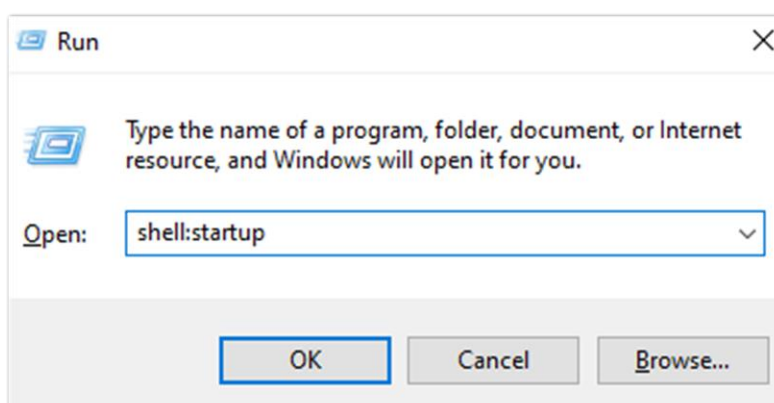
Once it is enabled, log back in for the log to begin registering.

3.4 How do I start Fortify by default without administration privileges?

If you do not want to have to run Fortify after every time you restart the computer, the application can be started if a shortcut to “fortify.exe” is placed in the startup applications folder. The Startup Applications destination folder is in the following path by default:

C:\Users\YourUser\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

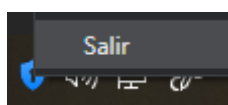
It can also be called up from Run (Windows + R) > Shell:startup.



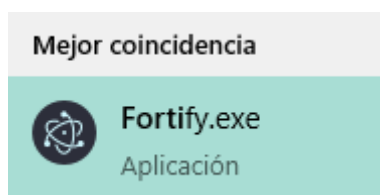
Note: performing this step in a session with administration privileges, contrary to the indications offered, would provoke the error indicated in point 3.6.5 of this guide.

3.5 How do I restart the Fortify application?

If you want to restart the application, right-click on the icon shown in section 3.3 and select Exit:

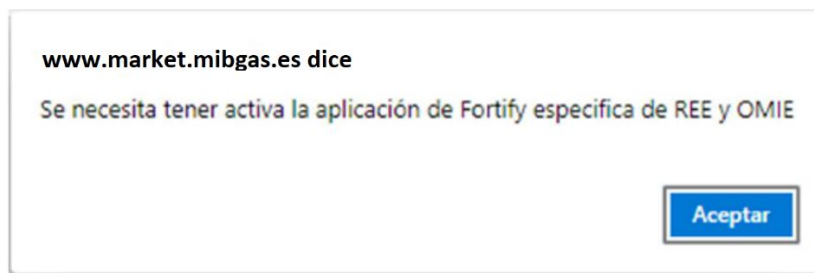


Then, run the application again from its path or from the Windows search engine: Fortify.exe:



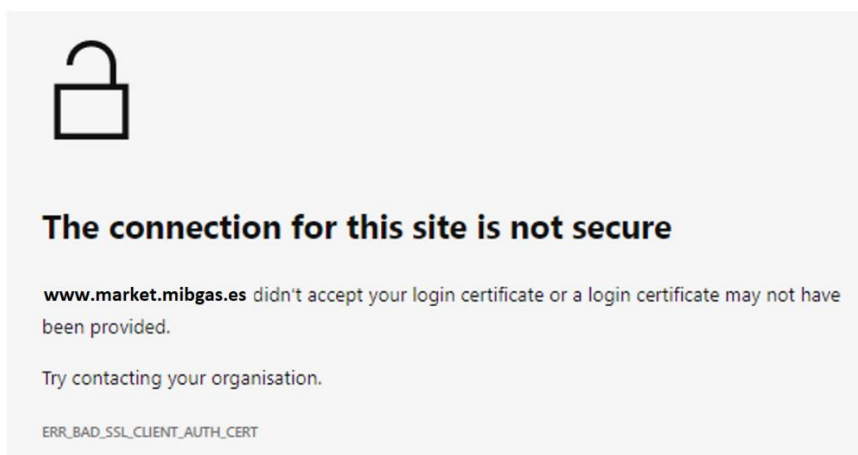
3.6 Known error or warning messages

3.6.1 The browser displays, "The Fortify application must be active"



If you access the System without any version of Fortify installed or running, a screen will pop up warning that you need to have the Fortify application installed and running.

3.6.2 The browser displays, "The connection to this site is not secure"

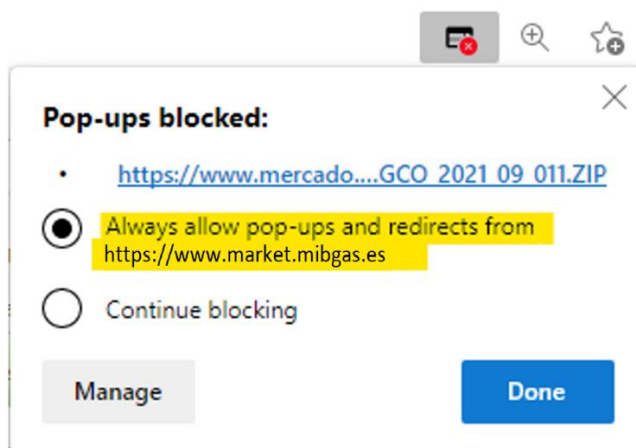


The message says that there is no valid access certificate (error code *ERR_BAD_SSL_CLIENT_AUTH_CERT*), which may be due to improper setup of the workstation or an expired certificate.

This message is specific to version 94 of the Edge browser. It may be different in new versions and in other browsers, but it also refers to SSL authentication failure.

3.6.3 Pop-up window blocking

Problems may occur when opening pop-up windows from some browsers.

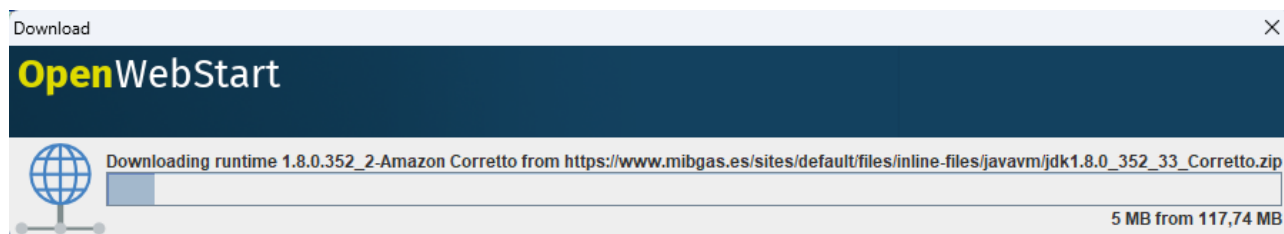


In this case, pop-up windows must be allowed for all MIBGAS websites (“*.mibgas.es”), following the setup procedures for each browser.

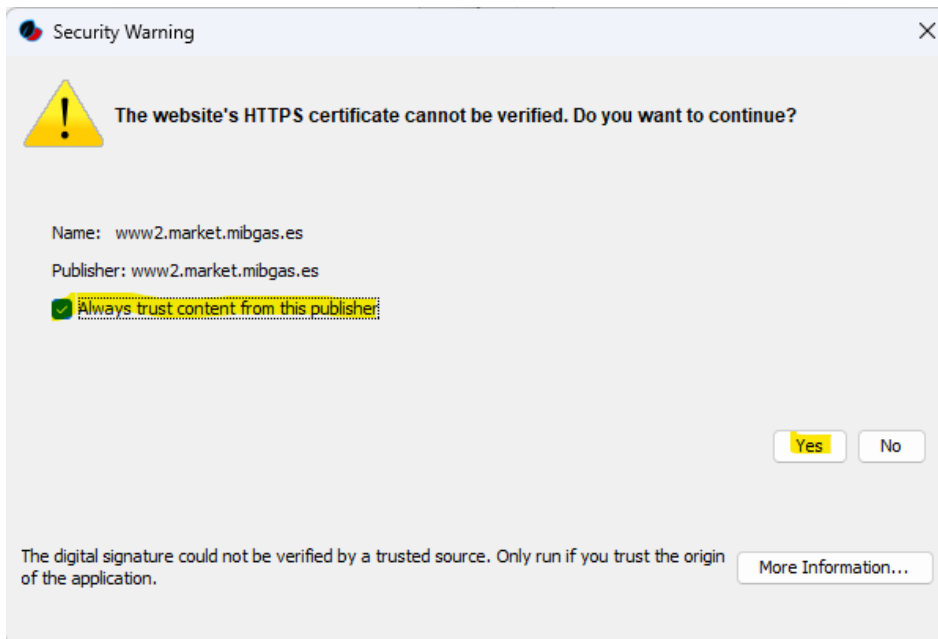
3.6.4 Messages after the execution of the Download Centre or Trading Module

After running the Download Center or Trading Module jnlpx file, a series of warning messages may appear, and must be accepted for the correct execution of this application.

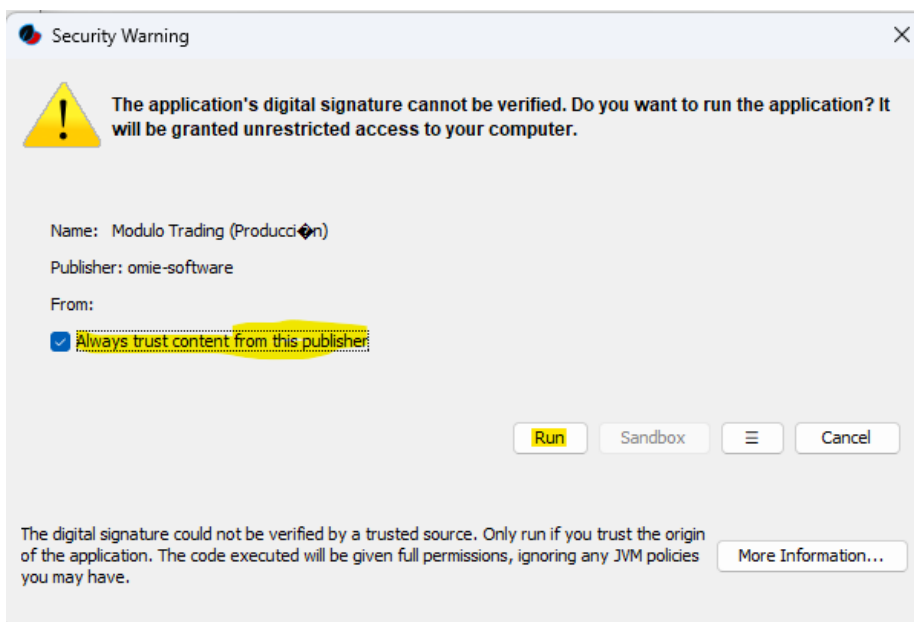
Initial virtual machine download:



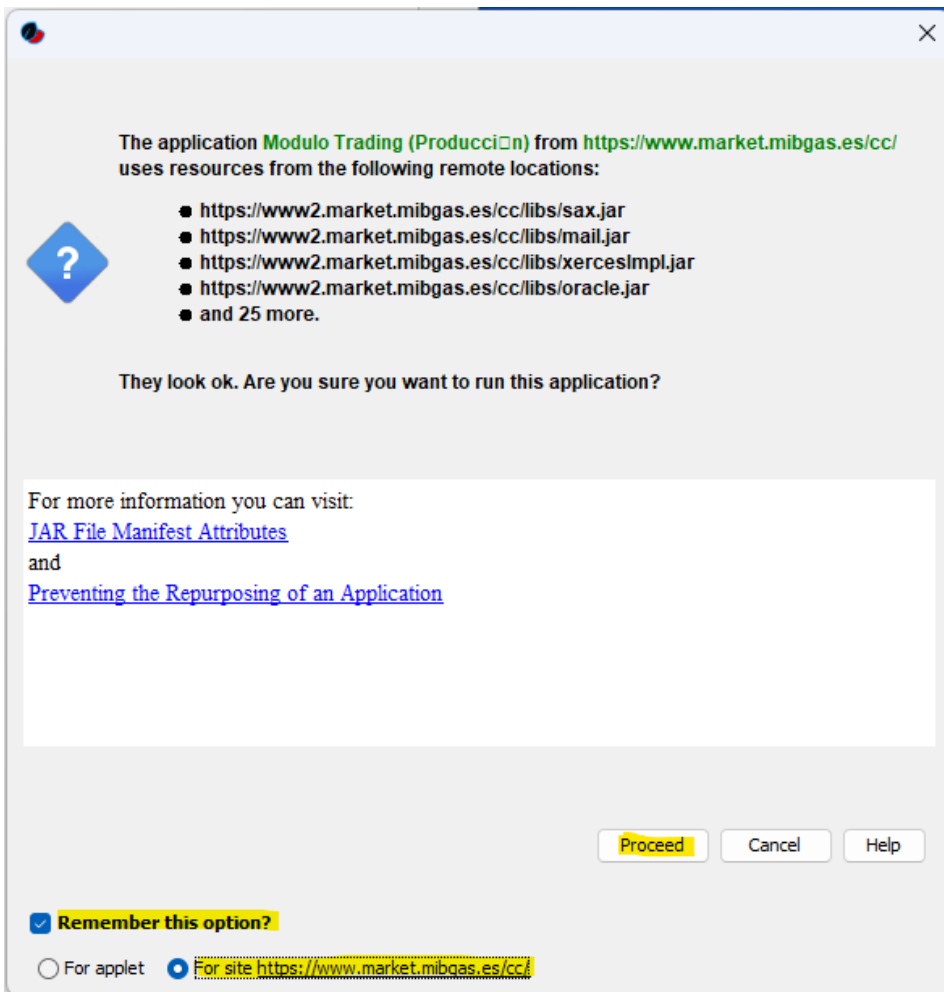
Security warning, check on “Always trust...” so it is not shown again and click on “Yes”:



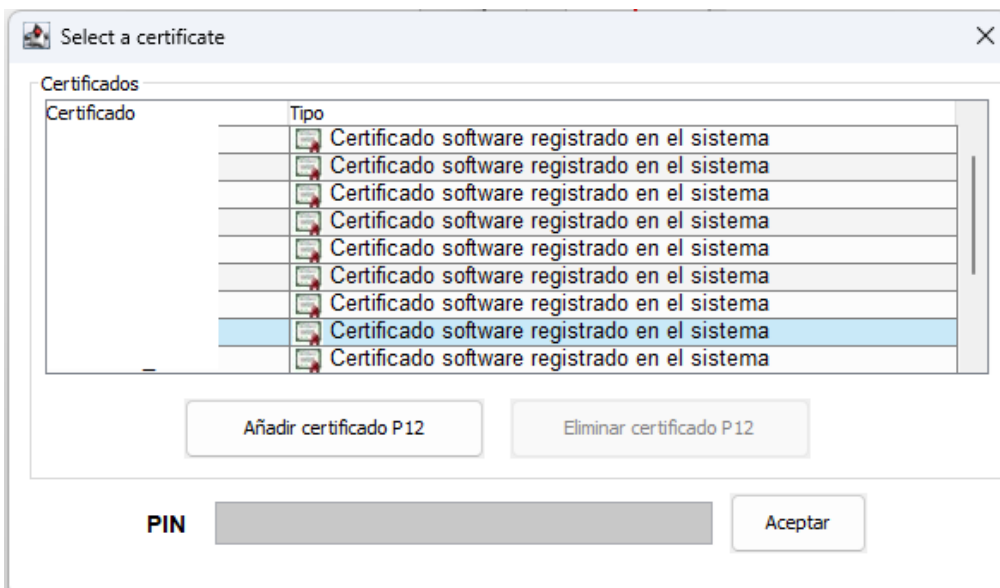
Security warning, check on “Always trust...” so it is not shown again and click on “Run”:



Security warning, check to remember the option and “Always trust...” and click on “Proceed”:



Once all the warnings have been accepted, the application should start, displaying the certificate selection screen:



3.6.5 AMQP Port blocked

In order to be able to use the MIBGAS Trading Client, the agent's network and security infrastructure must allow the use of AMQP protocol. Specifically, clients must be able to connect to server port 5671, as described in the setup guide.

In case AMQP port is not allowed in the agent infrastructure, in the agent workstation or in any existing network or security elements, access errors may occur, preventing a correct use of MIBGAS platforms.

Following, some images are depicted with possible errors related to AMQP port blocking.

» When opening the Trading Client, some messages could show up, similar to these ones:

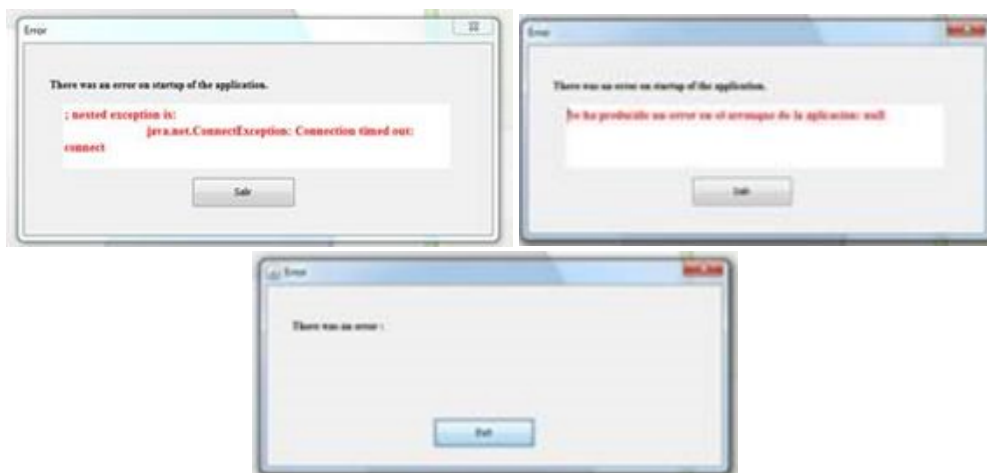
There was an error on startup of the application.

nested exception is: java.net.ConnectException: Connection timeout: connect

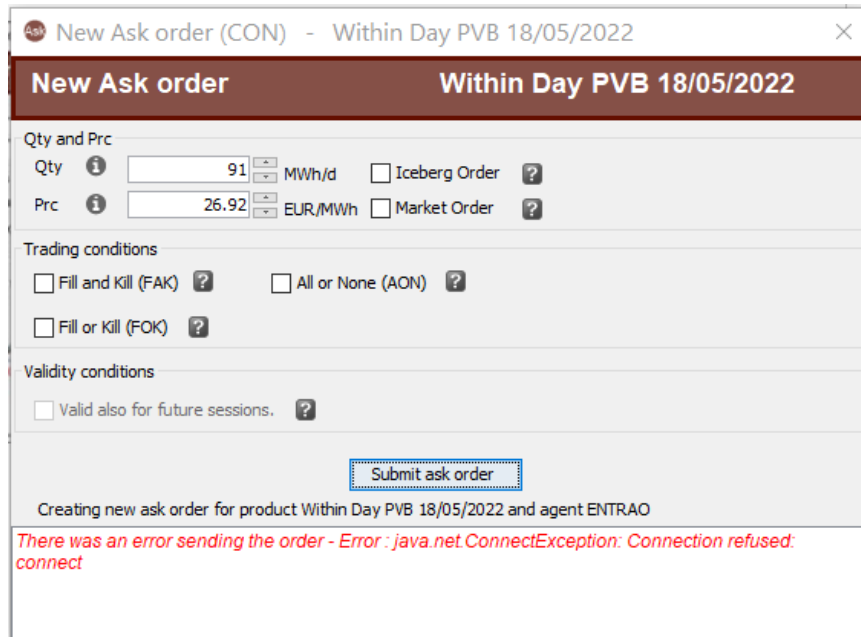
There was an error on startup of the application.

Se ha producido un error en el arranque de la aplicación: null

There was an error

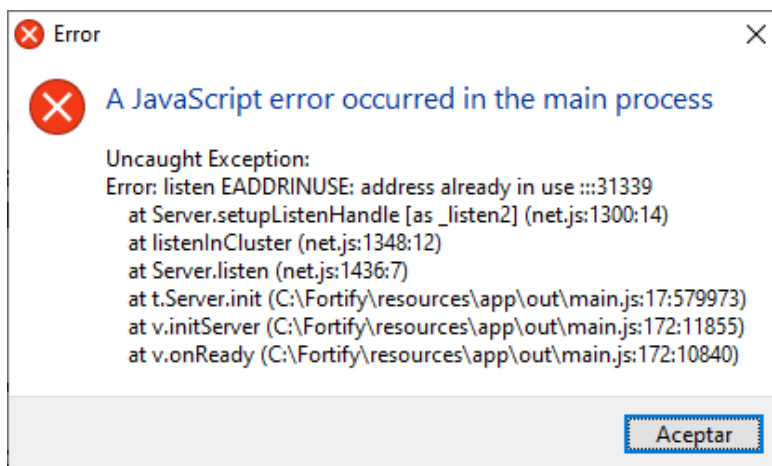


When trying to submit an order to the Trading Platform, a message similar to this one will show up:



More information on ports and IPs used to access the MIBGAS platforms can be found in the presentation [Emergency System \(SIOME\) - Implemented improvements](#), also available through the “Other documentation” section of MIBGAS Registry and Queries Platform help page (<https://www.market.mibgas.es>).

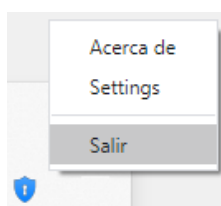
3.6.6 JavaScript: “EADDRINUSE: address already in use”



This warning is shown when you open the Fortify application when it **is already running**. This may be because another user has already started Fortify (accept the error), or because another user left their session open on the computer with Fortify running and another user started a session on the same computer. In the latter case, the first user must log out or at least close Fortify in their session.

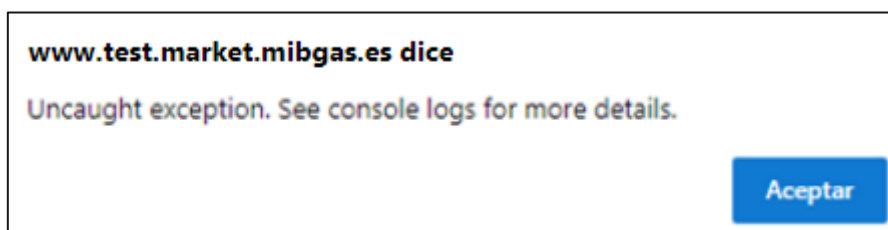
It may be due to the following causes:

- The user has administrator privileges and was the one to run the installer, then following the manual configuration to start Fortify from the user's Start menu. In this case, the manual step indicated in section 3.4 of this document must be reversed, deleting the shortcut created.
- The user already had Fortify started, in which case it is enough to accept the warning error.
- Other user leaves their session open on the computer with Fortify started, and another user logs in to the same computer, in which case it is necessary that one of the users logs out or, at least, close Fortify in his windows session. Alternatively, the computer can be restarted to start a single session.
- Fortify application is malfunctioning or hanged. In this case the user with this error should close Fortify, thus ending the process, and run Fortify again. Fortify can be closed:
 - o Through the icon located in the notification area (next to the Windows clock)



- o Forcing fortify.exe processes to close with Windows Task Manager.

3.6.7 “Uncaught Exception” message after inactivity / signing a transaction



If the alert is shown after a period of inactivity, it is usually because the session has been opened for a prolonged period. Exit and restart it to proceed as usual.

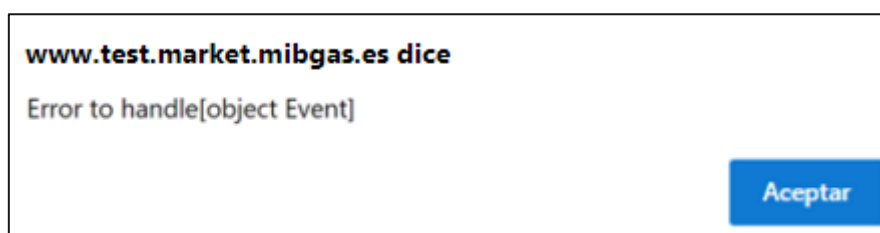
If the warning is triggered after signing a transaction (for example, with a Signature Test), this message may be due to unexpected reading errors by Fortify, regarding the installed certificates. To fix this, remove any possible expired certificate, reinstall the valid certificate and log back in.

If it is due to an excessive delay in signing transactions (see section 3.6.12) run the [installer](#) again.

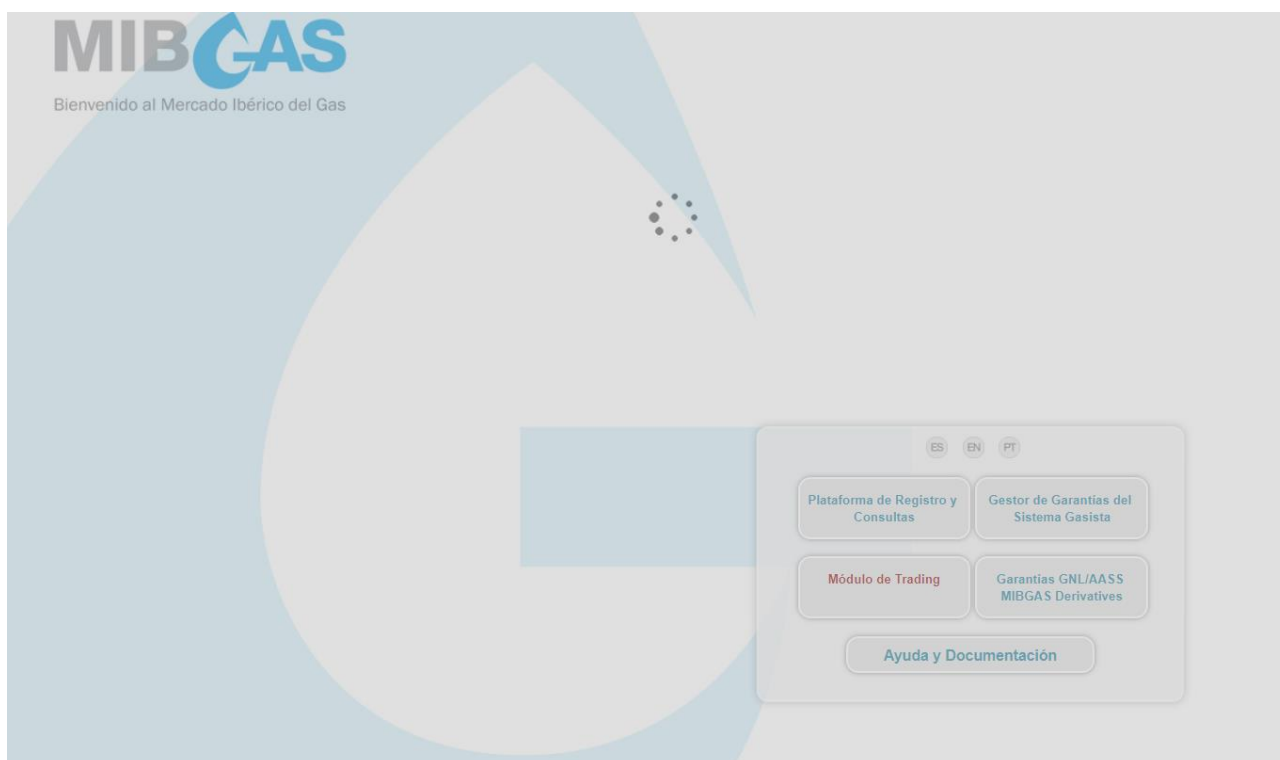
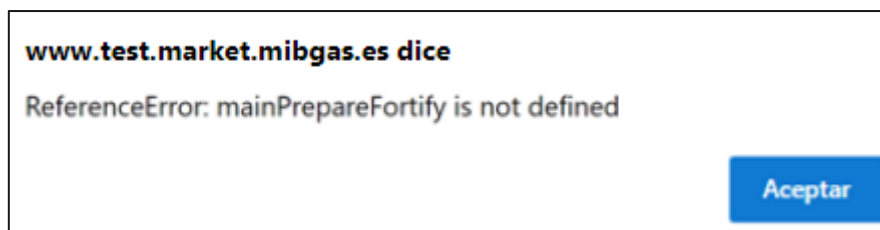
3.6.8 “Error to handle” or “ReferenceError” messages

The following messages cause a permanent page loading state after clicking OK:

» *Error to handle[object Event]*



» *ReferenceError: mainPrepareFortify is not defined.*



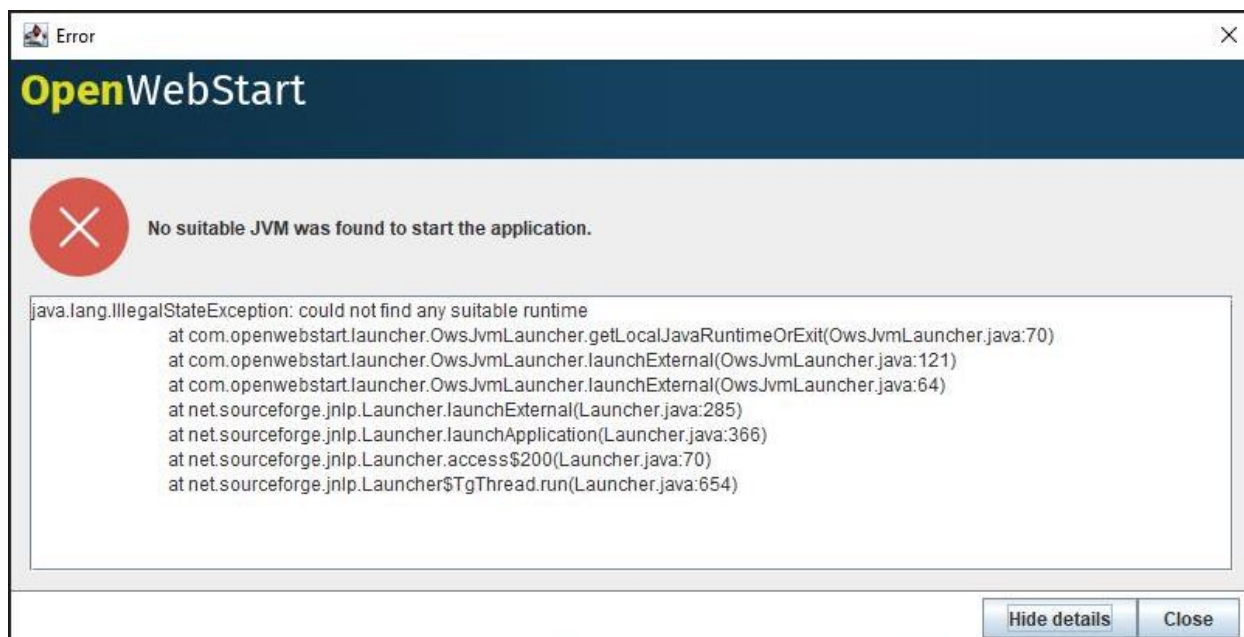
Access can be solved restarting the Fortify application as described in section 3.5.

3.6.9 The Download Center/Trading Client won't open

If you are trying to run the Download Center/Trading Client but the Certificate Selection Window does not pop up, check if the version of Java Virtual Machine shown in the “OpenWebStart > JVM Manager” menu is compatible (currently 1.8.0.352 Amazon Corretto).

Otherwise, click on the drop down menu of the wrong version, on the right (“...”) to select “Delete JVM,” and follow the steps outlined in the setup guide for the station in the section **Additional OpenWebStart Configuration** before re-running the Download Center/Trading Client.

3.6.10 OpenWebStart displays the error, “No suitable JVM was found...”



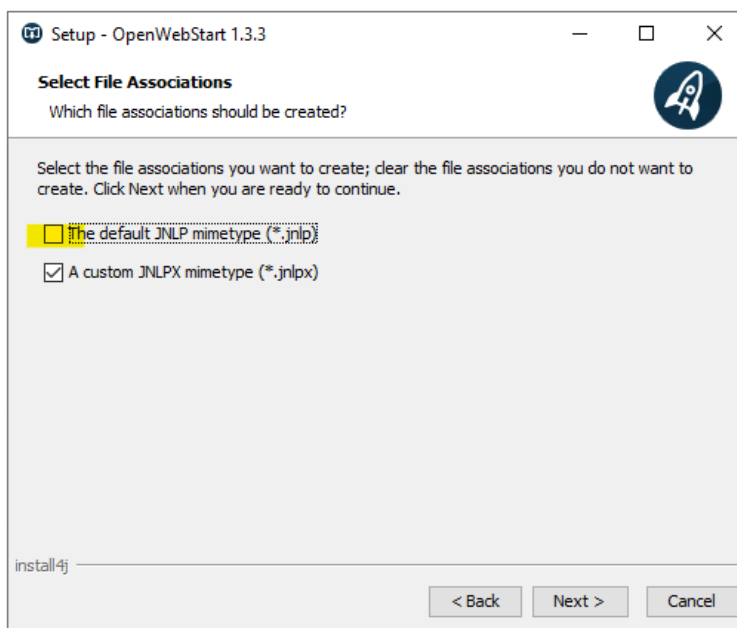
The OpenWebStart application is trying to run a jnlp application unsuccessfully.

If it is a genuine attempt, such as running the Download Centre or Trading Module, download a newest version of the jnlp file from the Registry and Queries platform (<https://www.market.mibgas.es>) and run it again.

If the error is shown again, check in *OpenWebStart > JVM Manager > Settings > Update Strategy* if downloads are blocked with the option, “Do not download any version;” in that case, at least temporarily select, “Ask if newer version should be downloaded.” Additionally, on the same screen select “Allow server from JNLP file”. Once completed, run the Download Center again.

Note: If you previously completed this setup and have **OpenWebStart version 1.5.2** installed, and **the error persists**, uninstall this version following the steps of section 3.7 to completely remove the application as well as its configuration and cache folders, and reinstall it again downloading the installer latest version that can be found in [Information system | MIBGAS - Iberian Gas Market](#).

During the installation you need to uncheck the association of files with extension *.jnlp.



If both options were marked you will need to associate the *.jnlp extension back to 'Java(TM) Web Start Launcher':

.jnlp
JNLP File



Java(TM) Web Start Launcher

.jnlp
A custom JNLPX mimetype



Launcher for .jnlp applications according to JSR-56

3.6.11 Problem related to "website's security certificate" while accessing the system

This window is shown when the OMIE CA Signing Entity certificate has not been registered in the browser (it may differ depending on the browser used).



There's a problem with this website's security certificate

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

Go to my homepage instead

Continue to this webpage (not recommended)

This may happen even if that certificate was already registered before, if an Operating System user hasn't previously logged in the MIBGAS WebSite, or due to a rootCA update in MIBGAS.

To solve this issue, the steps described in the Workstation setup guide document must be followed, starting from section 4.1.

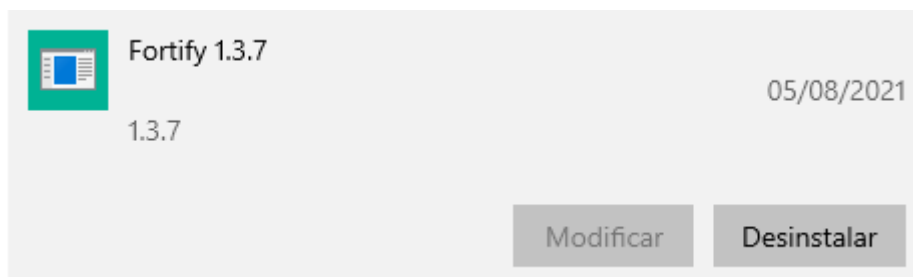
3.6.12 Delay during signed transaction

If the user experiences that a signed transaction takes up to 1 minute to complete, it is recommended to download and run the new version of the [installer](#) (v1.1 onwards), available since 03/11/2022, with new developments to optimize the browser settings in this regard.

3.7 Additional errors not found in this document

If you encounter additional errors not described in the previous sections of this document, please proceed by uninstalling the programs listed below:

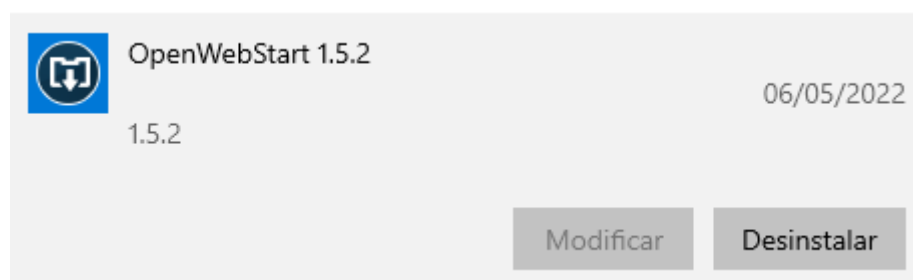
Fortify



Once done, delete the following folders:

- C:\Fortify
- C:\Users*User_name*\.fortify
- C:\Users*Nombre_de_usuario*\AppData\Roaming\Fortify

OpenWebStart



Once done, delete the following folders:

- C:\Program Files (x86)\OpenWebStart
- C:\Users*User_name*\.config\icedtea-web
- C:\Users*User_name*\.cache\icedtea-web

Delete all shortcuts to the Download Centre and/or Trading Module, as well as the downloaded jnlpx files to force the download of a new version from the Edge browser via the URL <https://www.market.mibgas.es>.

Once uninstalled, proceed with the steps described in section 2 of the Workstation Setup Guide again.