MERCADO IBÉRICO DEL GAS

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

Fecha: 03/02/2025

Versión 1.3.2

CONTENTS

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:

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

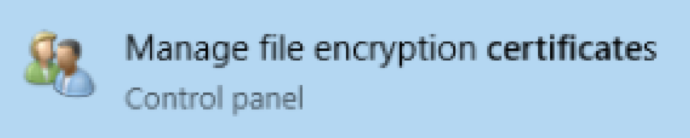
3. Answers to common questions

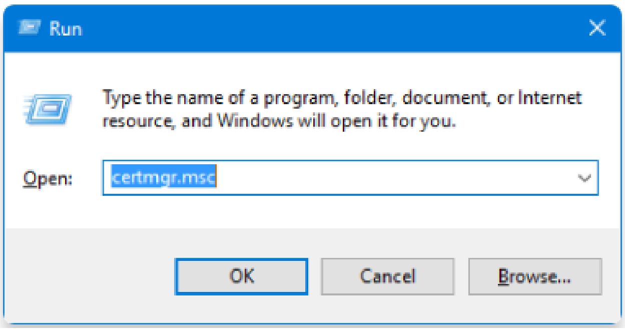
3.1 Can I continue logging on with Internet Explorer?

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?

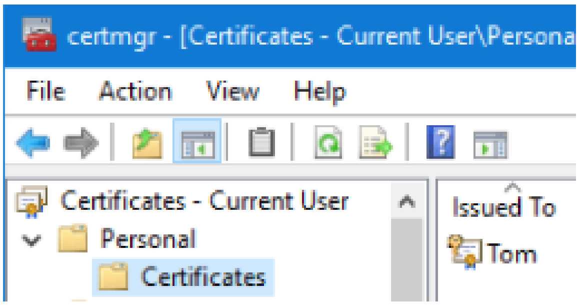
You can check, import, or delete the digital certificates installed in the Windows certificate store on the computer from Control Panel > Manage user certificates [certmgr]> Certificates - Current user > Personal > Certificates, or from the browser's Security options.





Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

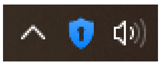
Open: certmgr.msc


certmgr - [Certificates - Current User\Persona
File
Action
View
Help
Certificates - Current User
Personal
Certificates
Issued To
Tom

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*.

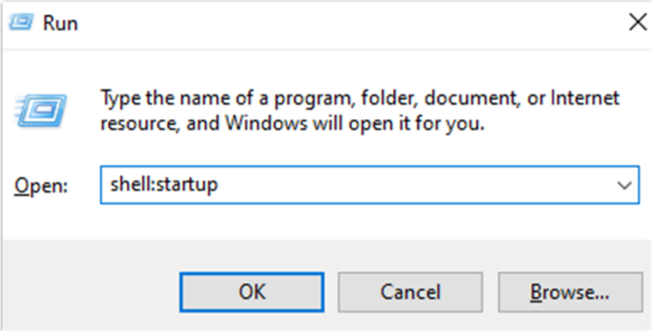
Once it is enabled, log back in for the log to begin registering.

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.



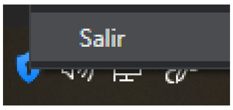
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: shell:startup

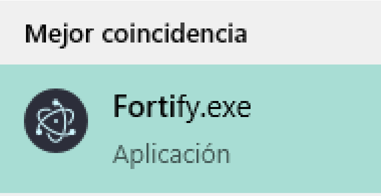
Note: performing this step in a session with administration privileges, contrary to the indications offered, would provoke the error indicated in point 3.6.5 of this guide.

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:

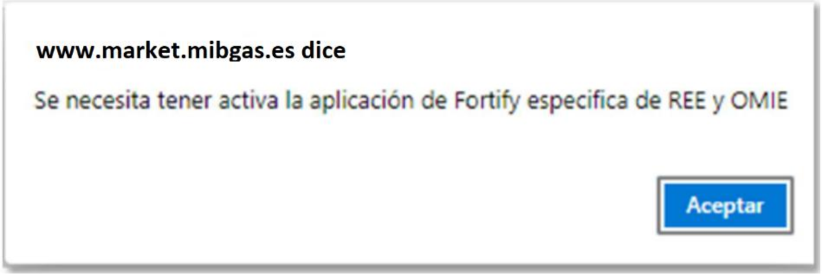


Then, run the application again from its path or from the Windows search engine: Fortify.exe:



3.6 Known error or warning messages

3.6.1 The browser displays, “The Fortify application must be active”

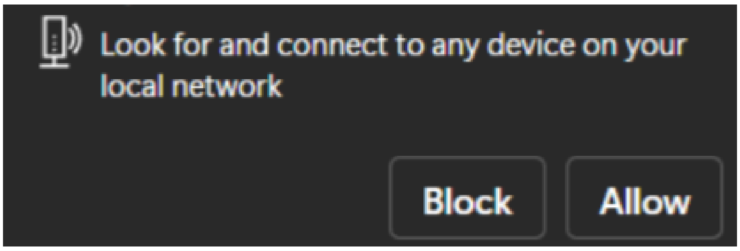


www.market.mibgas.es dice

Se necesita tener activa la aplicación de Fortify especifica de REE y OMIE

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.

On the other hand, in versions prior to 1.2 of the installer, and after updating Microsoft Edge to version 143, the browser may request permission to access devices on the local network when connecting to MIBGAS servers.

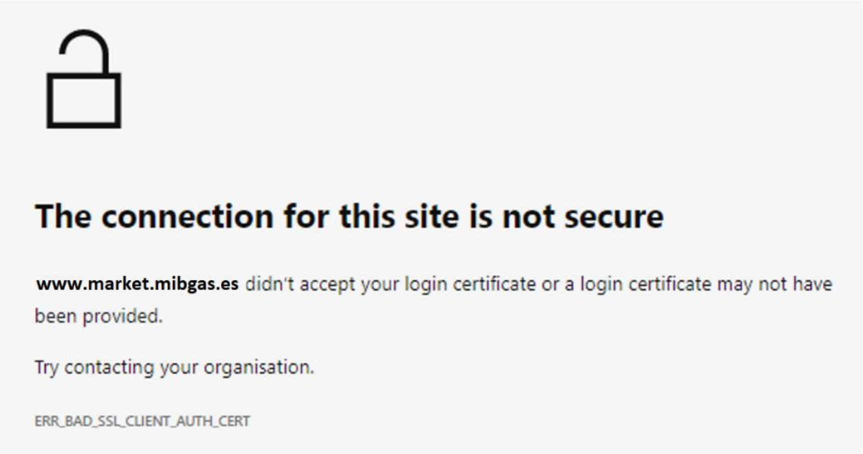


Look for and connect to any device on your local network

This permission is necessary for the Fortify application to be located and used during the access process. If permission to access the local network is not enabled, the message ‘The Fortify application must be active’ may appear.

It is recommended to download and install the latest version of the installer, which automatically configures the necessary permissions. If you are unable to run the installer, you can **configure the settings manually** by following these steps: *Site information (symbol to the left of the URL) > Permissions for this site > Local network access > select Allow.*

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



The connection for this site is not secure

www.market.mibgas.es didn't accept your login certificate or a login certificate may not have been provided.

Try contacting your organisation.

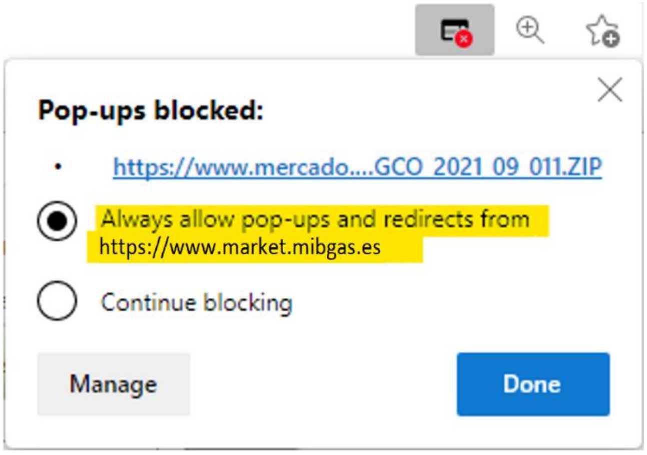
ERR_BAD_SSL_CLIENT_AUTH_CERT

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 windows blocked

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



Pop-ups blocked:

- https://www.mercado....GCO 2021 09 011.ZIP

● Always allow pop-ups and redirects from https://www.market.mibgas.es

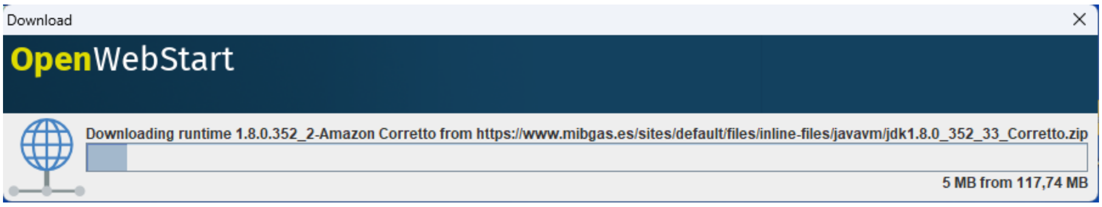
○ Continue blocking

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.

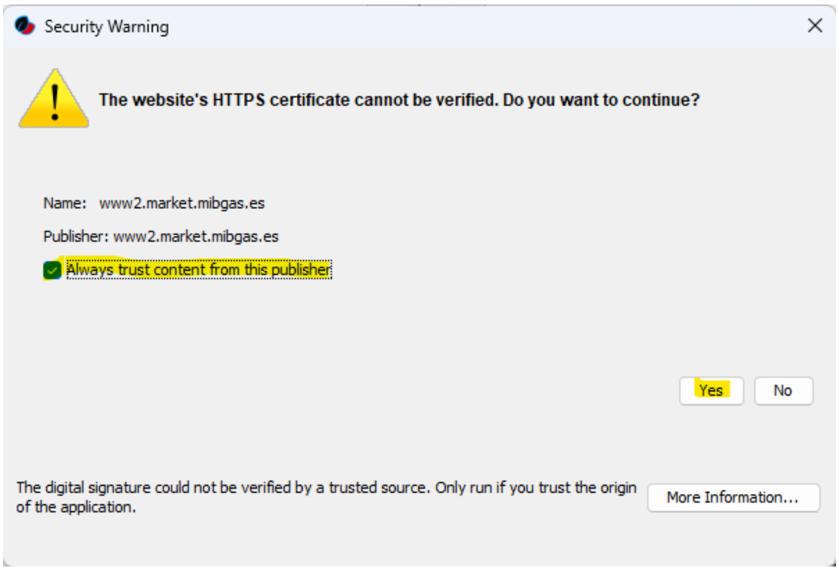
Initial virtual machine download:



Downloading runtime 1.8.0.352_2-Amazon Corretto from https://www.mibgas.es/sites/default/files/inline-files/javavm/jdk1.8.0_352_33_Corretto.zip

5 MB from 117,74 MB

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



Security Warning

The website's HTTPS certificate cannot be verified. Do you want to continue?

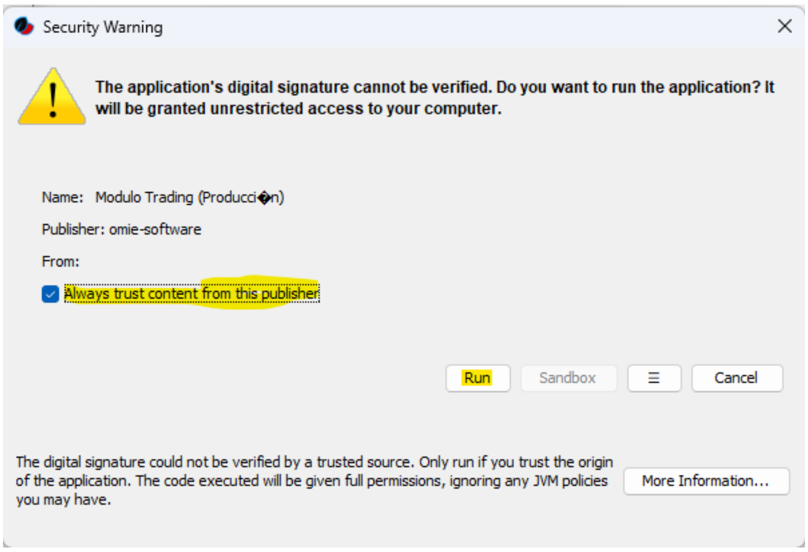
Name: www2.market.mibgas.es

Publisher: www2.market.mibgas.es

☑ Always trust content from this publisher

The digital signature could not be verified by a trusted source. Only run if you trust the origin of the application.

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



Security Warning

The application's digital signature cannot be verified. Do you want to run the application? It will be granted unrestricted access to your computer.

Name: Modulo Trading (Producci�n)

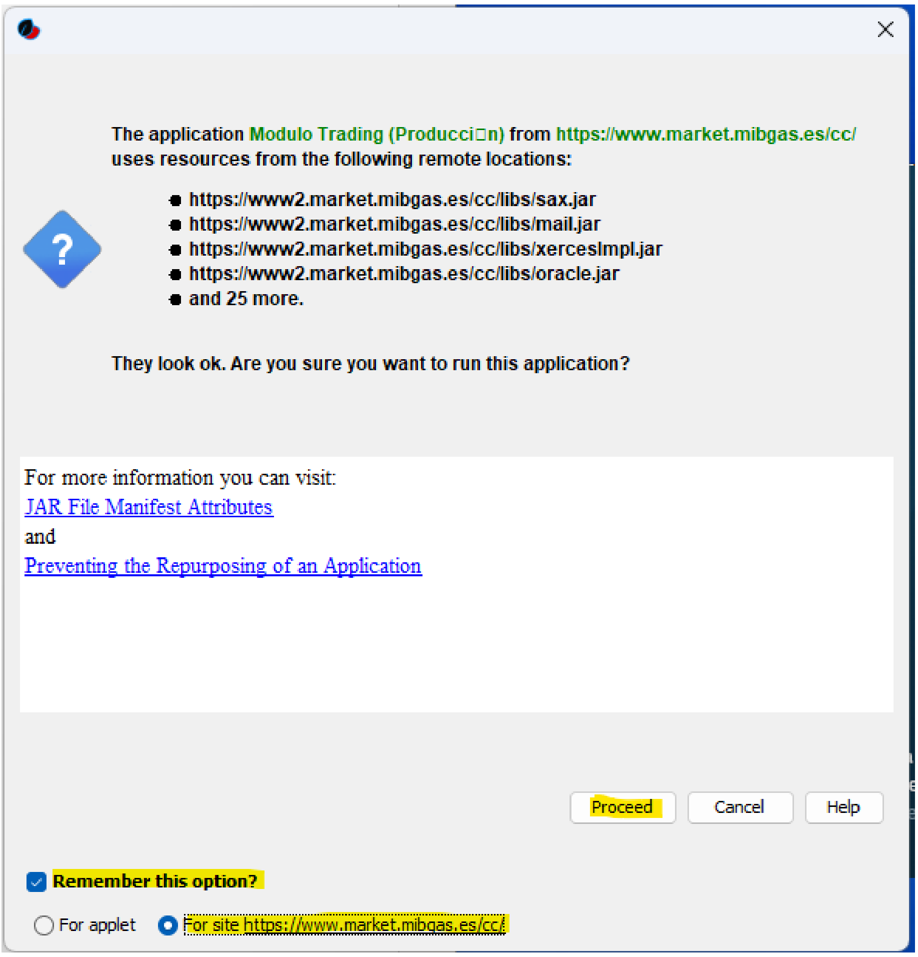
Publisher: omie-software

From:

☑ Always trust content from this publisher

The digital signature could not be verified by a trusted source. Only run if you trust the origin of the application. The code executed will be given full permissions, ignoring any JVM policies you may have.

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



The application Modulo Trading (Producci□n) from https://www.market.mibgas.es/cc/ uses resources from the following remote locations:

- https://www2.market.mibgas.es/cc/libs/sax.jar
- https://www2.market.mibgas.es/cc/libs/mail.jar
- https://www2.market.mibgas.es/cc/libs/xercesImpl.jar
- https://www2.market.mibgas.es/cc/libs/oracle.jar
- and 25 more.

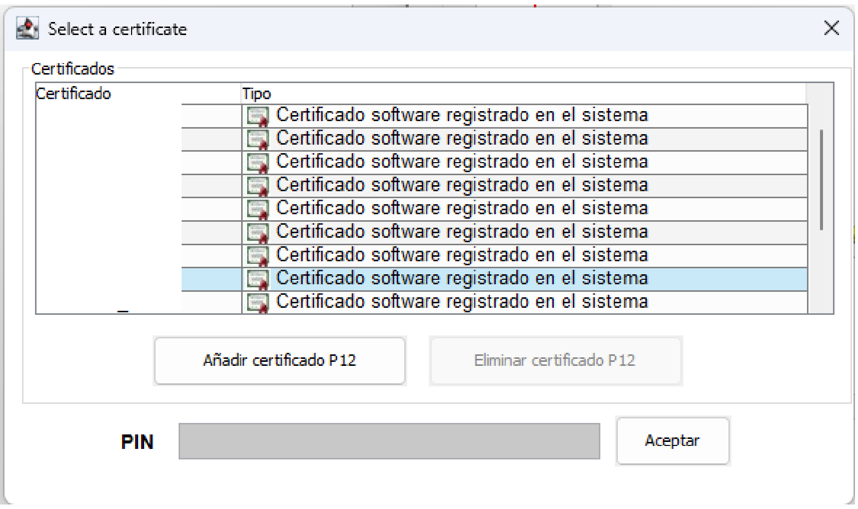
They look ok. Are you sure you want to run this application?

For more information you can visit:
JAR File Manifest Attributes
and
Preventing the Repurposing of an Application

☑ Remember this option?

○ For applet ● For site https://www.market.mibgas.es/cc/

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



Select a certificate

Certificados

Certificado	Tipo
	Certificado software registrado en el sistema
	Certificado software registrado en el sistema
	Certificado software registrado en el sistema
	Certificado software registrado en el sistema
	Certificado software registrado en el sistema
	Certificado software registrado en el sistema
	Certificado software registrado en el sistema
	Certificado software registrado en el sistema
	Certificado software registrado en el sistema

PIN

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.

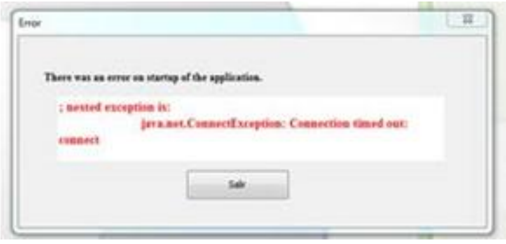
Following, some images are depicted with possible errors related to AMQP port blocking.

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

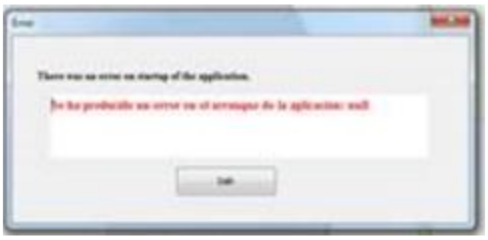
There was an error on startup of the application.
Se ha producido un error en el arranque de la aplicación: null

There was an error



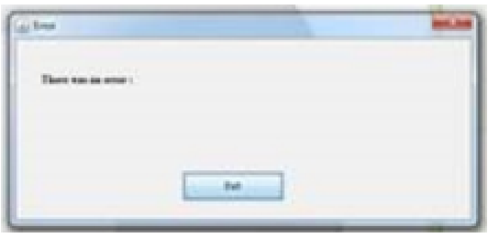
There was an error on startup of the application.

; nested exception is:
java.net.ConnectException: Connection timed out:
connect



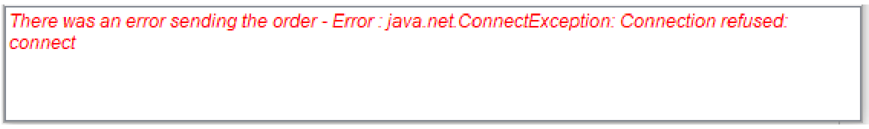
There was an error on startup of the application.

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



There was an error :

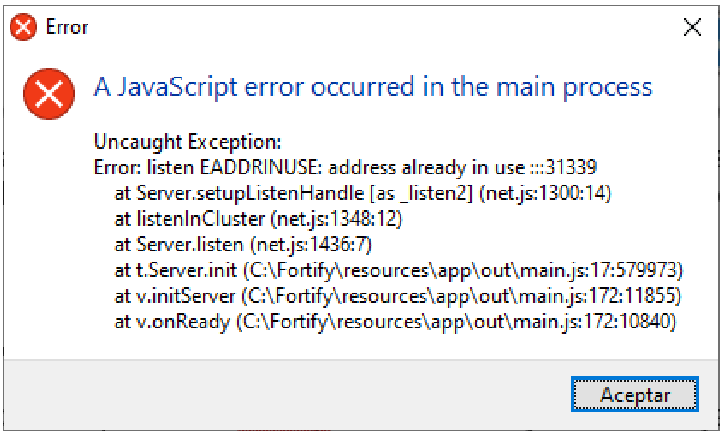
When trying to submit an order to the Trading Platform, a message similar to this one will show up:



There was an error sending the order - Error : java.net.ConnectException: Connection refused: connect

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”



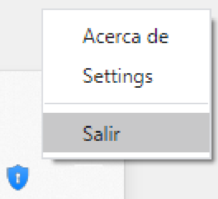
A JavaScript error occurred in the main process

```
Uncaught Exception:
Error: listen EADDRINUSE: address already in use :::31339
    at Server.setupListenHandle [as _listen2] (net.js:1300:14)
    at listenInCluster (net.js:1348:12)
    at Server.listen (net.js:1436:7)
    at t.Server.init (C:\Fortify\resources\app\out\main.js:17:579973)
    at v.initServer (C:\Fortify\resources\app\out\main.js:172:11855)
    at v.onReady (C:\Fortify\resources\app\out\main.js:172:10840)
```

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.

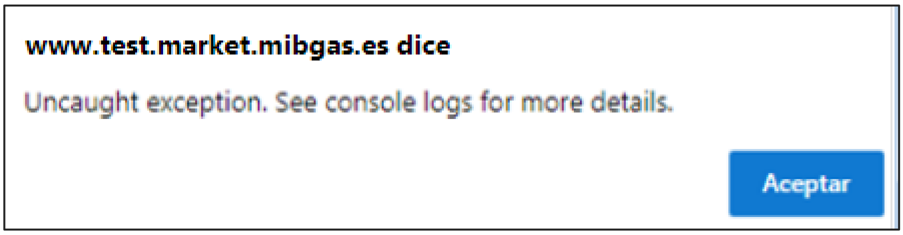
It may be due to the following causes:

- 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:
    - Through the icon located in the notification area (next to the Windows clock)



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

3.6.7 "Uncaught Exception" message after inactivity / signing a transaction


www.test.market.mibgas.es dice

Uncaught exception. See console logs for more details.

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.

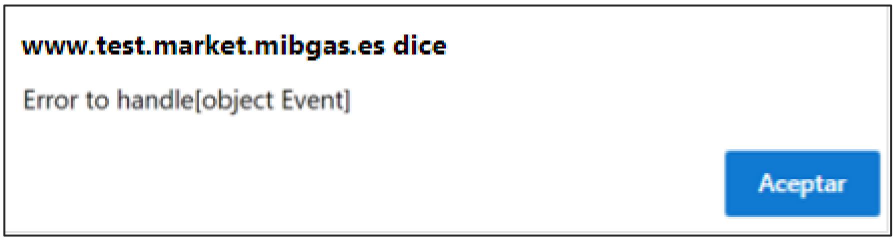
If the warning is triggered after signing a transaction (for example, with a Signature Test), this message may be due to unexpected reading errors by Fortify, regarding the installed certificates. To fix this, remove any possible expired certificate, reinstall the valid certificate and log back in.

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:

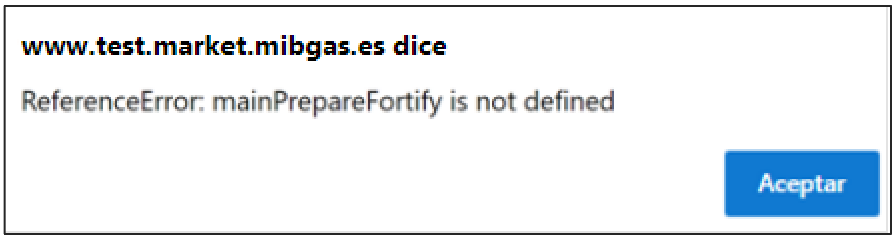
Error to handle[object Event]



www.test.market.mibgas.es dice

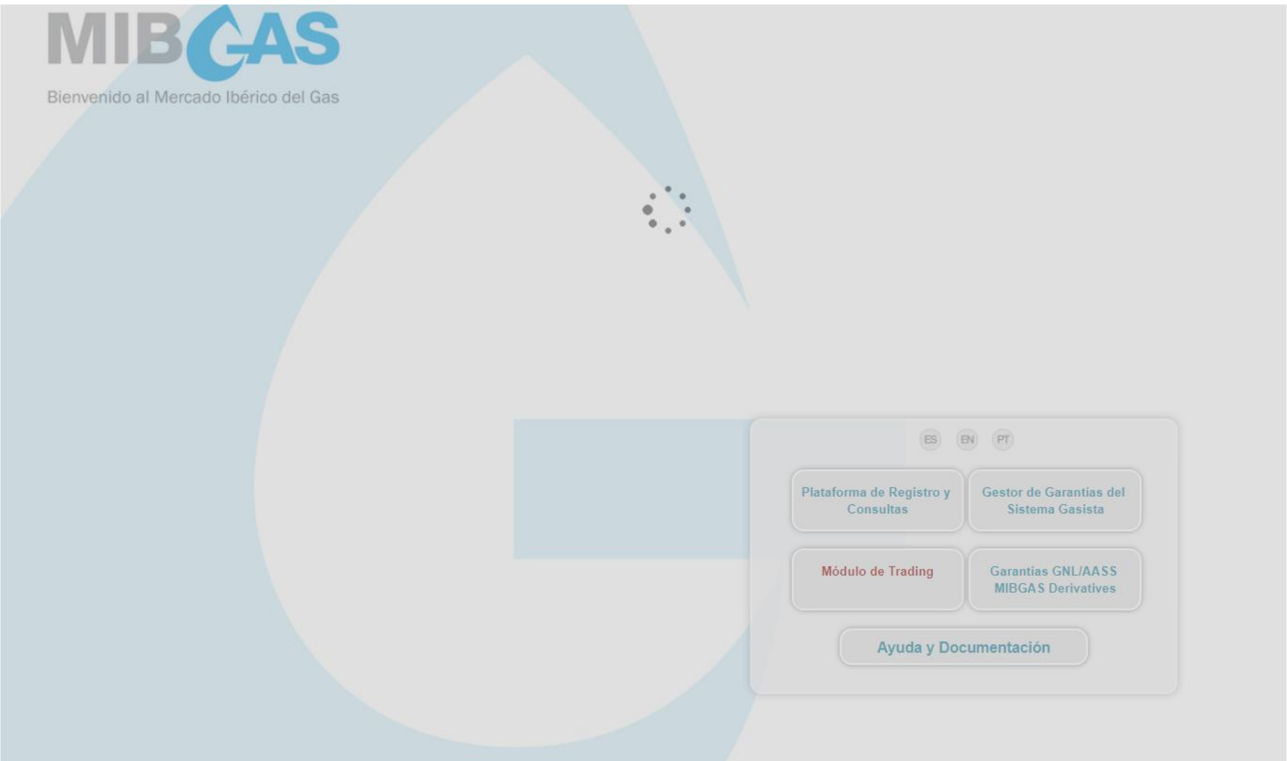
Error to handle[object Event]

ReferenceError: mainPrepareFortify is not defined.



www.test.market.mibgas.es dice

ReferenceError: mainPrepareFortify is not defined



MIBGAS
Bienvenido al Mercado Ibérico del Gas
ES
EN
PT
Plataforma de Registro y Consultas
Gestor de Garantías del Sistema Gasista
Módulo de Trading
Garantías GNL/AASS MIBGAS Derivatives
Ayuda y Documentación

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

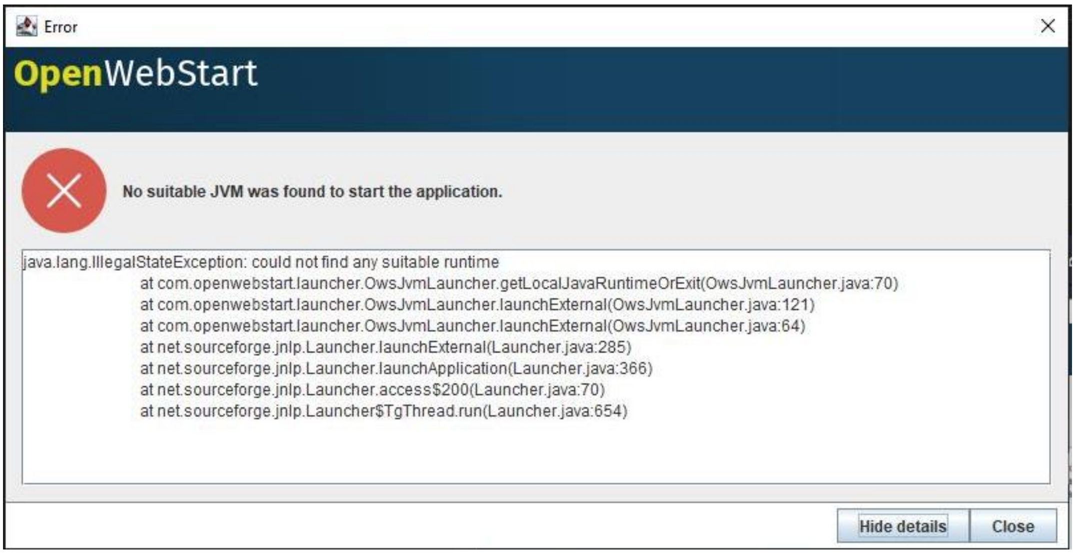
3.6.9 The Download Center/Trading Client won't open

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*," afterwards click on *'Refresh'* to confirm the removal. If the wrong version still shows on the screen it is recommended to reboot the computer and repeat the previous step.

Once the wrong version is removed, launch the Download Center or Trading Client from its executable file.

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



No suitable JVM was found to start the application.

```
java.lang.IllegalStateException: could not find any suitable runtime
        at com.openwebstart.launcher.OwsJvmLauncher.getLocalJavaRuntimeOrExit(OwsJvmLauncher.java:70)
        at com.openwebstart.launcher.OwsJvmLauncher.launchExternal(OwsJvmLauncher.java:121)
        at com.openwebstart.launcher.OwsJvmLauncher.launchExternal(OwsJvmLauncher.java:64)
        at net.sourceforge.jnlp.Launcher.launchExternal(Launcher.java:285)
        at net.sourceforge.jnlp.Launcher.launchApplication(Launcher.java:366)
        at net.sourceforge.jnlp.Launcher.access$200(Launcher.java:70)
        at net.sourceforge.jnlp.Launcher$TgThread.run(Launcher.java:654)
```

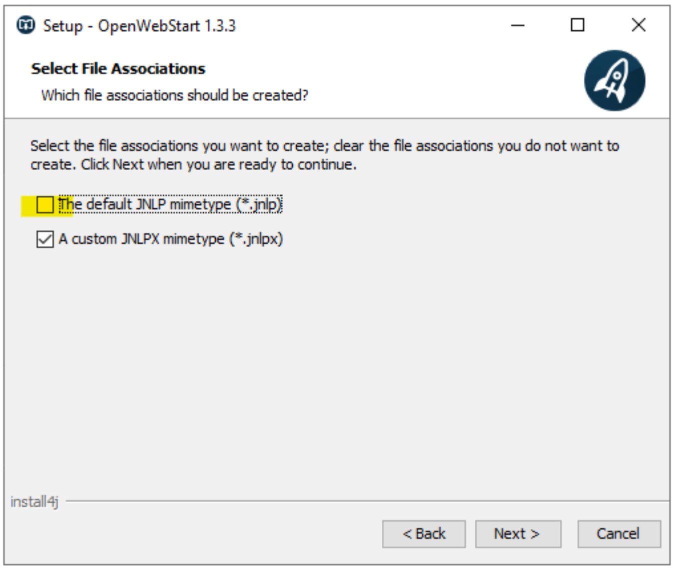
The OpenWebStart application is trying to run a jnlpx application unsuccessfully.

If it is a genuine attempt, such as running the Download Centre or Trading Module, download a newest version of the jnlpx 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 or Trading client 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.



Setup - OpenWebStart 1.3.3

Select File Associations

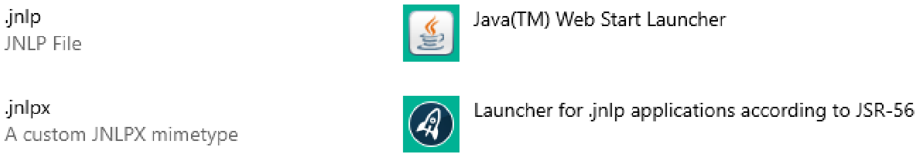
Which file associations should be created?

Select the file associations you want to create; clear the file associations you do not want to create. Click Next when you are ready to continue.

□ The default JNLP mimetype (*.jnlp)

☑ A custom JNLPX mimetype (*.jnlpx)

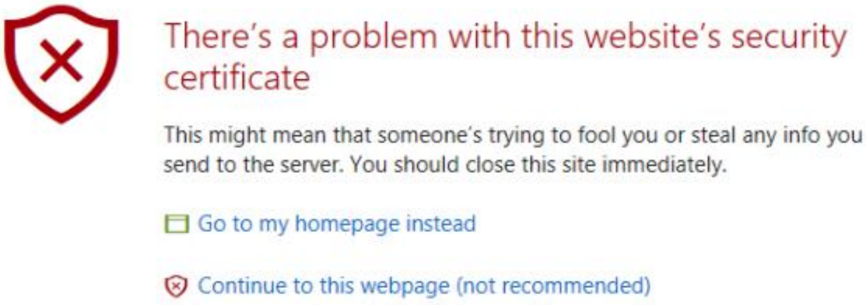
If both options were marked you will need to associate the *jnlp extension back to 'Java(TM) Web Start Launcher':



.jnlp JNLP File	Java(TM) Web Start Launcher
.jnlpx 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.

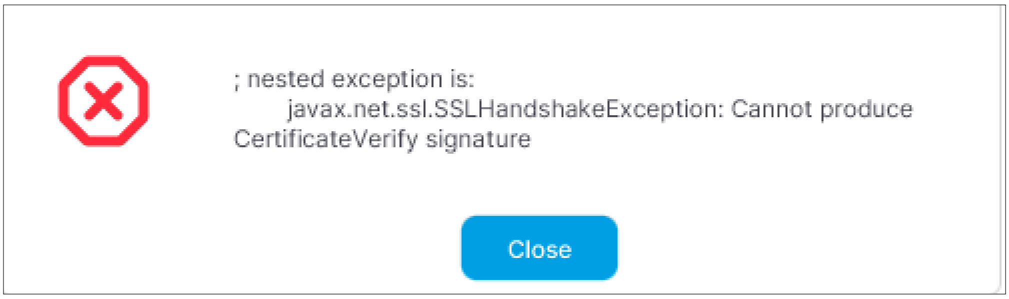
To solve this issue, the steps described in the Workstation setup guide document must be followed, starting from section 4.3.

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.

3.6.13 OpenWebStart shows "Cannot produce CertificateVerify signature"

Occasionally, the exception "Cannot produce CertificateVerify signature" has been observed when attempting to launch the MIBGAS Trading Module or Download Centre:



```
; nested exception is:
        javax.net.ssl.SSLHandshakeException: Cannot produce
CertificateVerify signature
```

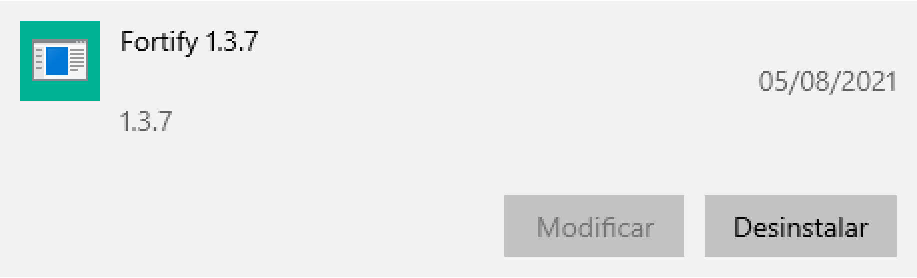
To resolve this issue, the user must uninstall the certificate provided by MIBGAS. To do so, follow the steps in section 3.2 of this document, select your certificate within the "Personal" folder, and right-click to choose "Delete."

After this, register the certificate again as described in section 5 of the agent Workstation Setup Guide.

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



Fortify 1.3.7

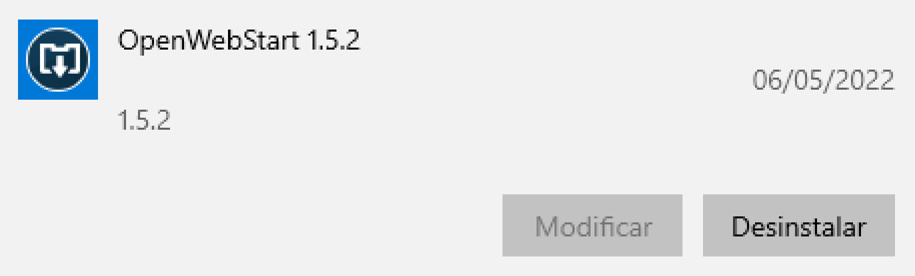
05/08/2021

1.3.7

Once done, delete the following folders:

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

OpenWebStart



OpenWebStart 1.5.2

06/05/2022

1.5.2

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.