Advanced Settings

Advanced Settings

Pandora RC (formerly called eHorus) saves its parameters in a file called `ehorus_agent.conf` whose location varies depending on the operating system used.

Configuration file location

GNU/Linux

```
/etc/ehorus/ehorus_agent.conf
```

To be able to modify this file you need administrator privileges (root).

Mac OS

```
/usr/local/ehorus_agent/ehorus_agent.conf
```

To be able to modify this file you need administrator privileges (root).

MS Windows

```
%ProgramFiles%\ehorus_agent\ehorus_agent.conf
```

To modify this file you need to run Notepad as administrator (right mouse button → run as administrator).

Agent Management

To make any configuration changes to the agent, it is required to be restarted with root or administrator rights.

- On GNU/Linux® (root):

```
/etc/init.d/ehorus_agent_daemon
```

- On MS Windows® (administrator):

Control Panel → Herramientas administrativas → Services → eHorus Agent → Restart.

- On Mac OS (root):

```
launchctl start com.ehorus.ehorus_agent
```

General Agent Parameters

Agent Password

Optionally, a different agent connection password can be specified for each machine. This password is specified *-clearly*, without encryption- in the agent configuration file, in the following configuration token:

```
password xxxx
```

Once the agent is restarted, the password will be hashed like this:

```
password [[db6f086273f8c93e57808dafef45eae6ae67ae639eb34b6a6|]]
```

This behavior is normal and is similar for other configuration tokens that may contain sensitive information (proxy access username and password, etc.).

Session expiration time

The Pandora RC WEB client remains connected to the agent while the browser session is open and while there is a connection. If you leave the session open and unused, the session on that computer will be locked until you close it.

To prevent this, the agent has an inactivity timeout mode that is set to 300 seconds by default. You can override that behavior by modifying the following configuration token:

```
session_timeout 300
```

Agent Connectivity Settings

The design goal of Pandora RC is for the agent to be accessible wherever it is, even in complex topologies with poor connectivity. For this there are some configuration tokens that regulate how the agent connects with the server.

The agent periodically checks that the connection is still alive (even though it appears to be connected), this is known as “keepalive”. You can regulate how many seconds it is done if you think this can improve the behavior of your agent in the event of power outages, etc.

```
ping_interval 300
```

In addition, you can modify the general network timeout, to lower or raise it depending on your specific needs. By default it is 5 seconds.

```
timeout 5
```

There are two advanced parameters that should be handled with care, they are those that regulate the maximum payload size and the maximum block size, and both are specified in bytes:

```
max_payload_size 131072
block_size 16384
```

Proxy usage

The Pandora RC agent connects to a Pandora RC server on the internet with port `18080`, if it cannot connect, the agent can be (optionally) told to try a connection through a proxy.

To do this, it is necessary to edit the agent's configuration file (in administrator mode) and use the following configuration tokens, specifying the IP address and the port of the HTTP proxy that the agent will use.

The proxy must support the CONNECT method.

```
proxy_address 127.0.0.1
proxy_port 3186
```

Sending information from the remote system

By default, the Pandora RC agent sends a small summary of the computer where it is installed (Disk, RAM, CPU, OS version, etc.). If for privacy you do not want to send this information, you can deactivate it with the following configuration token:

```
disable_info 1
```

Local connection against agent

There is an (optional) mode that allows the agent to listen on a local IP address and port and allow incoming connections directly from the Pandora RC client. Despite the fact that the connection is local, the Pandora RC agent will always contact the Pandora RC server on the Internet to validate the client's connection (username and password) and give them access, in addition to the agent's local authentication, if any.

```
eh_local_port 41118
```

The agent will try to find out which is the most appropriate IP address to listen to, and it will be the one that “publishes” in the portal for which the client connects. Generally this will be the IP address by which you connect to the server. If it does not detect it well or you prefer to enter it by hand, you can use the following configuration token:

```
eh_local_address 192.168.50.2
```

It must be taken into account that when using this connection mode, we will notice a substantial improvement in speed, especially in remote desktop and in file transfer. On the other hand, furthermore, it will require communication between client and remote client is clear of obstacles such as corporate or local firewalls. In the case of MS Windows® or GNU/Linux®, it will be necessary to deactivate the firewalls that are installed by default in said systems.

When an agent is in local connection mode, the machine can be accessed directly, using an interface modification that allows you to choose between remote connection or direct connection. Due to security restrictions of the Web Socket protocol, in order to make the local connection, you will have to do it exclusively from Google Chrome®, Mozilla Firefox® or Microsoft Edge® browsers. This connection mode is not supported with Safari® or MS Internet Explorer®.

Connection with SSL certificates

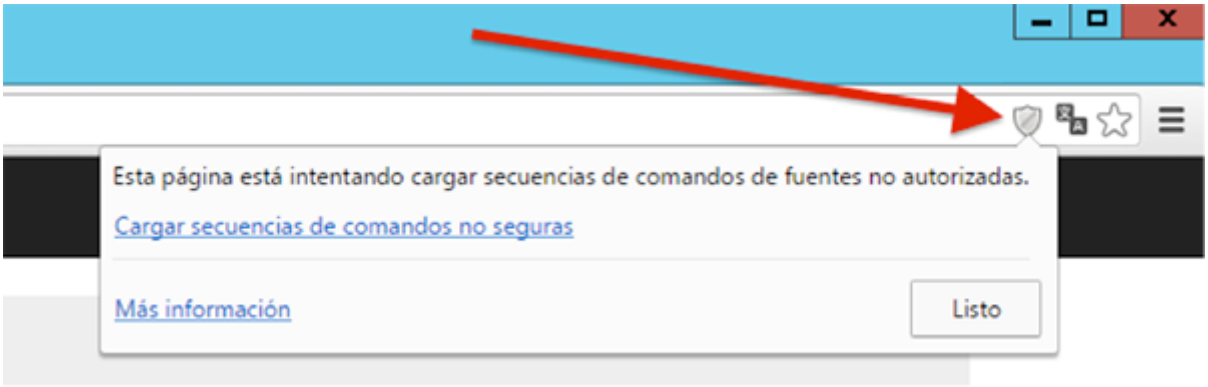
For the local connection to be secure and reliable, it is possible to indicate to the agent a valid SSL certificate file (by a CA recognized by the browser to be used). This must be manually configured using the following configuration tokens:

```
eh_local_cert /full_path/to_public_ssl_cert
eh_local_key /full_path/to_private_ssl_key
```

The files must be in PEM (OpenSSL) format.

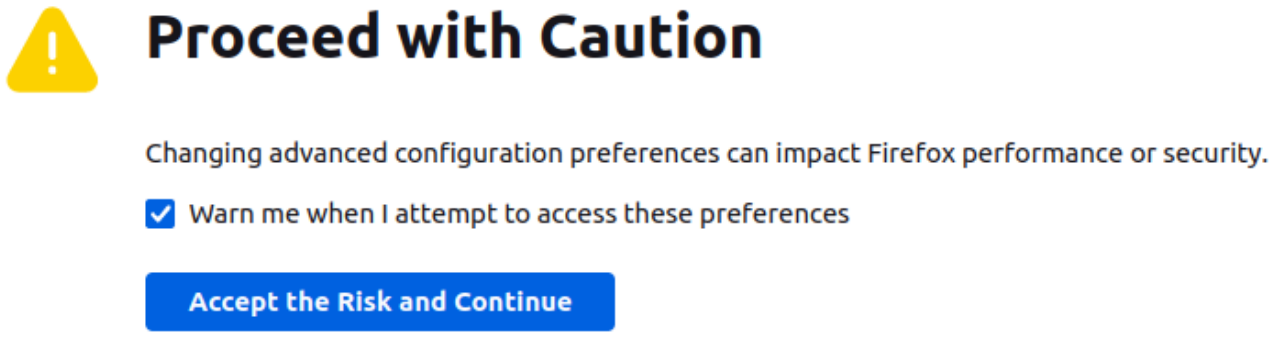
Connection without SSL certificates: Chrome

Right-clicking will bring up a dialog informing you that we are trying to load unauthorized sequences. Click on “Load unsafe scripts”.

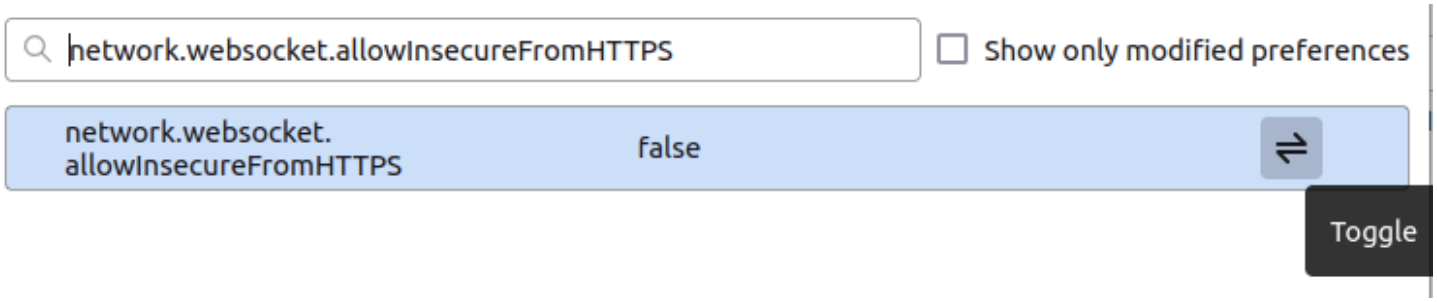


Connection without SSL certificates: Firefox

In the case of Mozilla Firefox® you must modify the general settings of the browser. In a new tab, type: `about:config`. There is a warning that the configuration is for advanced users, click `Accept the Risk and Continue`.



Search for the *token* `network.websocket.allowInsecureFromHTTPS` and click the button to change it to the opposite value, `true`.



This change is permanent. You will not need to change the configuration again in subsequent browser sessions.

Set Up File Transfer

The agent allows to specify a directory from which files can be uploaded/downloaded, this base directory is specified in the configuration file using the following configuration token:

```
storage_dir /home/ehorus
```

On MS Windows if you want to access all system drives, you can set this parameter to the value `/`.

Log files

The agent can store in a text record (log file) the information on its status, incoming connections, problems, and so on. To do this, you must activate the configuration token specified in the log file:

```
log_file 'C:\ProgramData\ehorus_agent\ehorus_agent.log'
```

And you can also modify how much information to dump to that file with the following configuration token.

```
verbose x
```

Where X can be a numeric value from 0 to 9. A value of 0 is minimal information, and a value of 9 is maximum debugging information. The agent does not control the size of the log, so if it is configured to return the maximum information, it can generate a very large log.

```
verbose 4
```

Agent Revision

If for whatever reason, you need to reprovision the agent, follow these steps:

- Stop the agent.
- Delete from the configuration file the configuration tokens: `eh_hash` and `eh_key` and start the agent again. It should be provisioned again with a different EKID.

Enable/Disable file deletion

You can disable (default is enabled) the functionality of deleting files from the remote file manager. To do this use the following configuration token:

```
enable_file_delete 0
```

Hide App Icon

It is possible to deactivate (by default it is activated) the Pandora RC agent service launching the desktop notification application. This application displays its icon in the notification area (tray area). To do this use the following configuration token:

```
hide_tray 1
```

The value 1 means that the application is not launched and therefore the icon is not seen. The default value is 0.

Pop-up notices for access

There is an optional functionality that allows the user who is using the computer to receive a notification to inform or require confirmation of external access. This is especially critical to comply with certain legal regulations for remote access to computers. By default it is deactivated, but to activate it, it is enough to activate certain configuration tokens.

This functionality can be configured individually to regulate how each service is accessed (file transfer, process management, service management, remote shell, remote desktop, access sharing) and also serves to disable the use of one of those services in case you don't want it to be available.

The possible values for these configuration items are:

- `Request`: The user will be asked to accept the incoming connection, through a pop-up window. This window is timed out, and if the connection to the service is not explicitly accepted, access will be denied.
- `Inform`: It will only inform the user. If the user does not see it or presses the button that has seen it, the remote user will still enter.
- `Always`: The remote user enters without the local user having to authorize or see any pop-up messages. It is the default value
- `Disable`: The service will not be available in any case.

```
access_terminal always|request|inform|disable
access_display always|request|inform|disable
access_processes always|request|inform|disable
access_services always|request|inform|disable
access_files always|request|inform|disable
access_share always|request|inform|disable
```

On the other hand, the configuration element that defines the confirmation window timeout is:

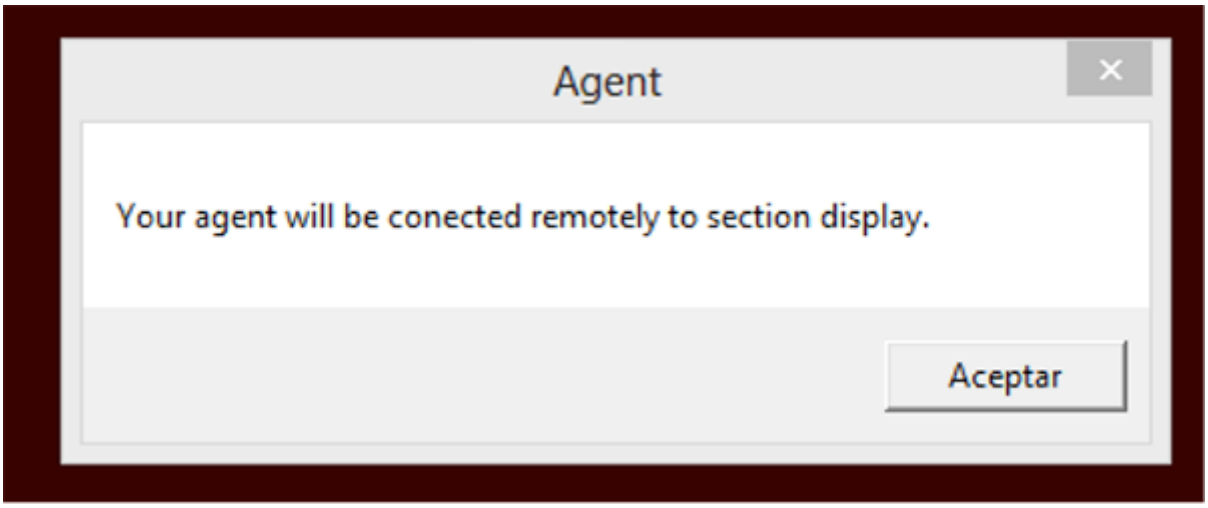
```
access_dialog_timeout 30
```

The default value is 30 seconds. This timeout cannot be greater than the client keepalive refresh time, which is 60 seconds.

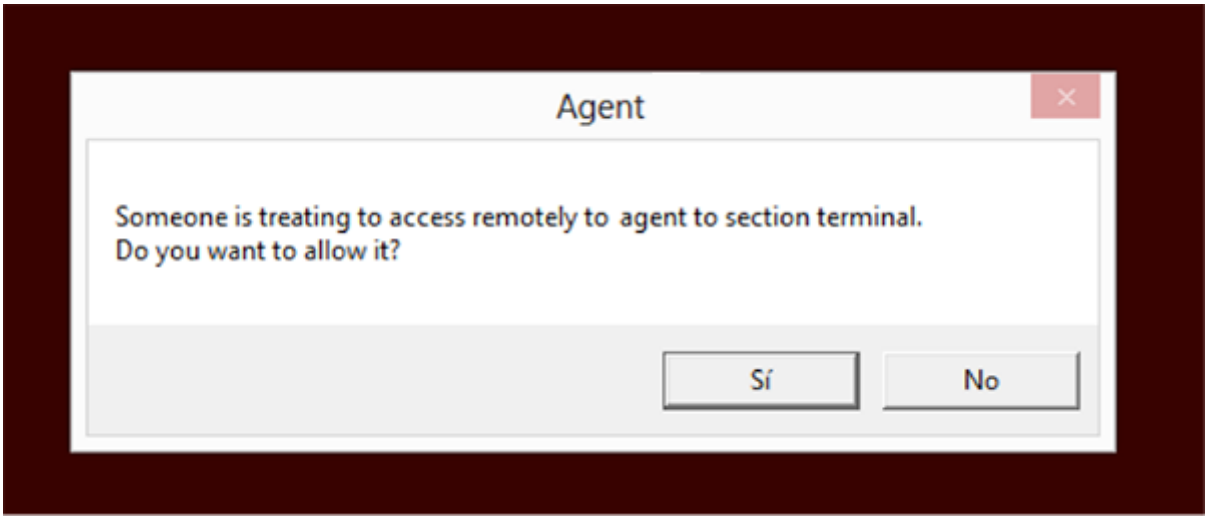
To use a customizable popup system, you must load an external DLL:

```
access_method 'C:\path\to\dll'
```

What the “Information” screen looks like is this:



And when the configuration “forces” the local user to confirm the connection, the information displayed is the following:



In GNU/Linux this functionality is not implemented.

Double screen

On Windows systems that have more than one display, the agent will automatically attempt to discover the primary display. If you want to use another screen or both screens at the same time, you will have to modify the agent configuration file:

```
display_selected -1 | 0 | 1 | 2
```

- The value -1 shows all screens.
- The value 0 (default) will show the main screen.
- Value 1 shows screen No. 1 (the second, in most cases)
- Value 2 (to infinity) will display screen 2..3.. etc (if any).

Server Balancing

As of version 1.1.0, the Pandora RC agent can automatically request a new server from the directory before each connection attempt. To enable this feature, add the following line to the agent configuration file:

```
huh_balancing 1
```

Back to Pandora FMS Documentation Index