Configuraciones avanzadas

Configuraciones avanzadas

Pandora RC (antes llamado eHorus) guarda sus parámetros en un fichero llamado `ehorus_agent.conf` cuya ubicación varía según el sistema operativo utilizado.

Ubicación del fichero de configuración

GNU/Linux

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

Para poder modificar este fichero se necesitan privilegios de administrador (root).

Mac OS

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

Para poder modificar este fichero se necesitan privilegios de administrador (root).

MS Windows

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

Para modificar este fichero se necesita ejecutar Notepad como administrador (botón secundario del ratón → ejecutar como administrador).

Gestión del agente

Para efectuar cualquier cambio de configuración en el agente, se requiere de su reinicio con derechos de root o administrador.

- En GNU/Linux® (root):

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

- En MS Windows® (administrator):

Panel de control → Herramientas administrativas → Servicios → eHorus Agent → Restart.

- En Mac OS® (root):

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

Parámetros generales del Agente

Contraseña de agente

Opcionalmente se puede especificar un contraseña de conexión al agente diferente para cada máquina. Esta contraseña se especifica -*en claro*, sin cifrar- en el fichero de configuración del agente, en el siguiente *token* de configuración:

```
password xxxx
```

Una vez se reinicia el agente, la contraseña será cifrada mediante *hash* de este tipo:

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

Ese comportamiento es normal y es similar para otros *tokens* de configuración que puedan contener información sensible (usuario y contraseña de acceso al *proxy*, etcétera).

Tiempo de expiración de sesión

El cliente WEB de Pandora RC se queda conectado al agente mientras mantenga la sesión del navegador abierta y mientras haya conexión. Si deja la sesión abierta y sin usar, la sesión en ese equipo quedará bloqueada hasta que la cierre.

Para evitar esto, el agente tiene un modo de desconexión automático (*timeout*) por inactividad que está configurado por defecto a 300 segundos. Se puede modificar ese comportamiento modificando el siguiente *token* de configuración:

```
session_timeout 300
```

Ajustes de conectividad del agente

El objetivo de diseño de Pandora RC es que el agente sea accesible esté donde esté, incluso en topologías complejas con mala conectividad. Para ello hay algunos *tokens* de configuración que regulan como se conecta el agente con el servidor.

El agente realiza periódicamente una comprobación de que la conexión siga viva (aunque parezca que está conectada), a esto se le conoce como *keepalive*. Se puede regular cada cuántos segundos se realiza si cree que esto puede mejorar el comportamiento de su agente ante cortes de servicio eléctrico, etcétera.

```
ping_interval 300
```

Además, puede modificar el *timeout* general de red, para bajarlo o subirlo en función de sus necesidades específicas. Por defecto son 5 segundos.

```
timeout 5
```

Existen dos parámetros avanzados que se deben manejar con cautela, son los que regulan el tamaño máximo de *payload* y el tamaño máximo de *bloque* y ambos se especifican en bytes:

```
max_payload_size 131072
block_size 16384
```

Uso de proxy

El agente de Pandora RC se conecta a un servidor de Pandora RC en internet por medio del puerto `18080`, si no puede conectarse, se le puede indicar (opcionalmente) al agente que intente una conexión a través de un *proxy*.

Para ello es preciso editar el fichero de configuración del agente (en modo administrador) y utilizar los siguientes *tokens* de configuración, especificando la dirección IP y el puerto del *proxy* HTTP que utilizará el agente.

El *proxy* debe soportar el método CONNECT.

```
proxy_address 127.0.0.1
proxy_port 3186
```

Envío de información del sistema remoto

Por defecto, el agente Pandora RC envía un pequeño resumen del equipo donde está instalado (Disco, RAM, CPU, versión del SO, etcétera). Si por privacidad no se desea enviar esta información, puede desactivarla con el siguiente *token* de configuración:

```
disable_info 1
```

Conexión local contra el agente

Existe un modo (opcional) que permite que el agente escuche en una dirección IP y puerto local y permita conexiones entrantes directamente del cliente de Pandora RC. A pesar de que la conexión sea local, el agente de Pandora RC siempre contactará con el servidor de Pandora RC en internet para validar la conexión del cliente (usuario y contraseña) y darle acceso, además de la autentificación local del agente si la hubiera.

```
eh_local_port 41118
```

El agente intentará averiguar cual es la dirección IP más apropiada para escuchar, y será la que "publique" en el portal para el que cliente se conecte. Generalmente esta será la dirección IP por la que se conecta al servidor. Si no la detectara bien o se prefiere meter a mano, se puede usar el siguiente *token* de configuración:

```
eh_local_address 192.168.50.2
```

Hay que tener en cuenta que al usar este modo de conexión, se notará una mejora sustancial en la velocidad, especialmente en el escritorio remoto y en la transferencia de archivos. Por el contrario necesitará, además, que la comunicación entre el cliente y el cliente remoto esté despejada de obstáculos tales como *firewalls* corporativos o locales. En el caso de MS Windows® o GNU/Linux® habrá que desactivar los *firewalls* que traen instalados por defecto dichos sistemas operativos.

Cuando un agente tiene el modo de conexión local, se puede acceder a la máquina directamente, utilizando una modificación de la interface que permite elegir entre conexión remota o conexión directa. Debido a restricciones de seguridad del protocolo Web Socket para poder realizar la conexión local, tendrá que hacerlo exclusivamente desde los navegadores web Google Chrome®, Mozilla Firefox® ó Microsoft Edge®. Este modo de conexión no está soportado con Safari® ni MS Internet Explorer®.

Conexión con certificados SSL

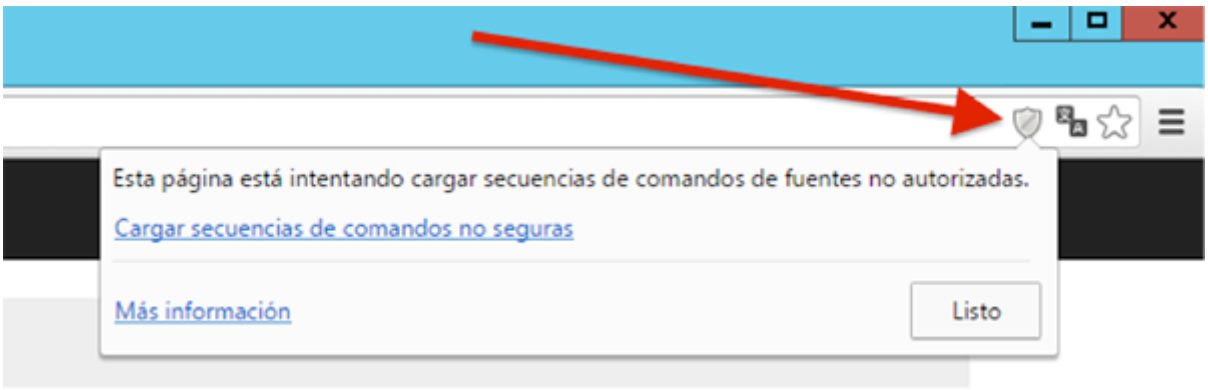
Para que la conexión local sea segura y confiable, es posible indicar al agente un fichero de certificado SSL válido (por una CA reconocida por el navegador que se vaya a usar). Esto se debe configurar manualmente usando los siguientes *tokens* de configuración:

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

Los ficheros deben estar en formato PEM (OpenSSL).

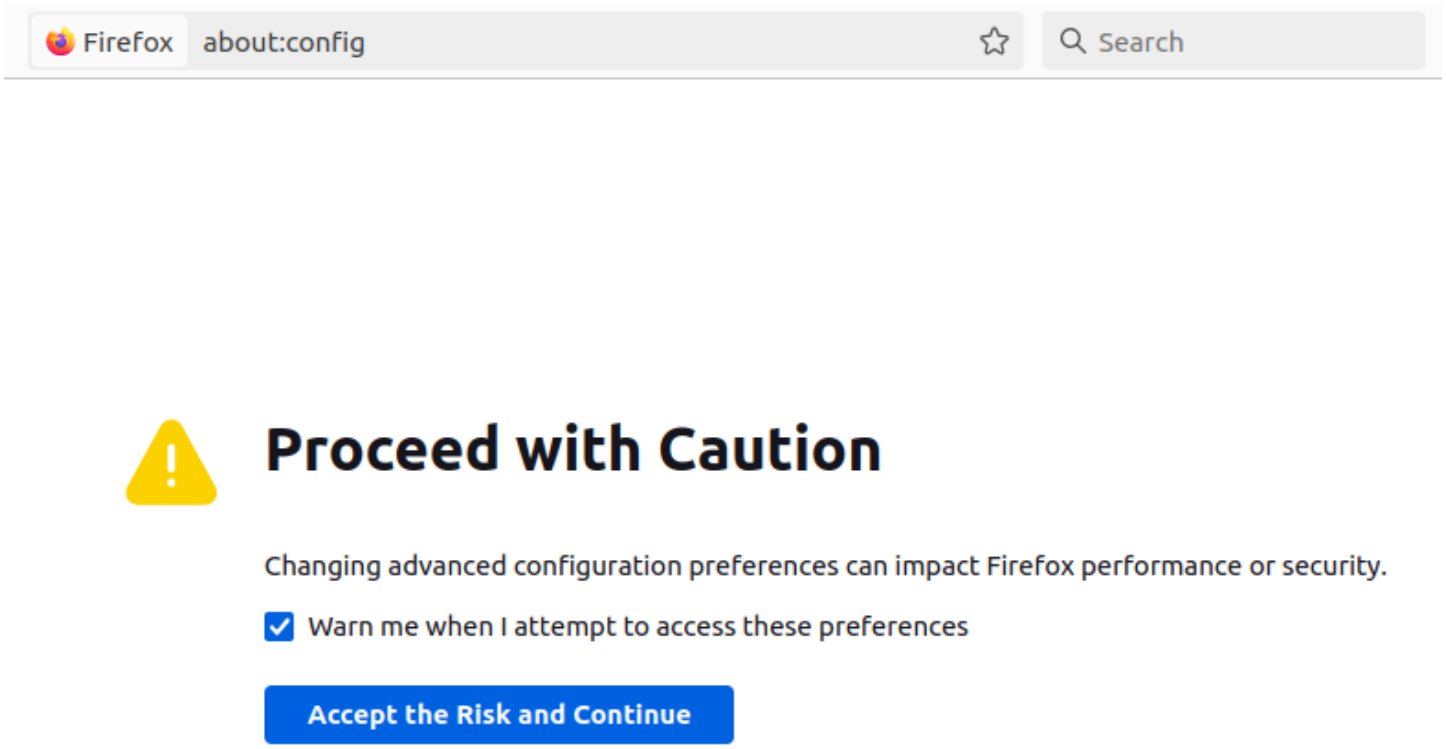
Conexión sin certificados SSL: Chrome

Al hacer clic con el botón secundario aparecerá un diálogo donde informa de que estamos intentando cargar secuencias no autorizadas. Se debe hacer clic en “Cargar secuencias de comandos no seguras”.

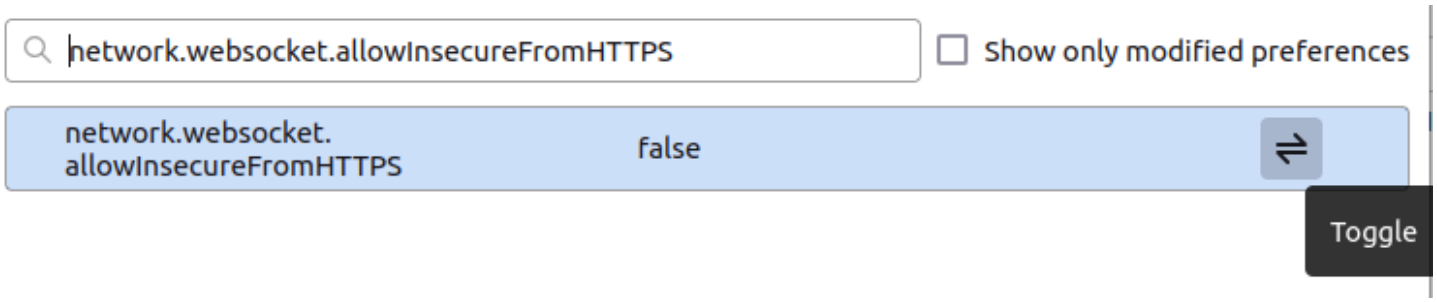


Conexión sin certificados SSL: Firefox

En el caso de Mozilla Firefox® se debe modificar la configuración general del navegador. En una nueva pestaña, escribir: `about:config`. Hay una advertencia de que la configuración es para usuarios avanzados, se hace clic en `Accept the Risk and Continue`.



Buscar el *token* `network.websocket.allowInsecureFromHTTPS` y se hacer clic en el botón para cambiar al valor contrario, `true`.



Este cambio es permanente. No hará falta volver a cambiar la configuración en sucesivas sesiones del navegador.

Configurar transferencia de archivos

El agente permite especificar un directorio desde el cual se pueden cargar/descargar archivos, este directorio base se especifica en el fichero de configuración mediante el siguiente token de configuración:

```
storage_dir /home/ehorus
```

En MS Windows si desea acceder a todas las unidades del sistema, puede establecer este parámetro con el valor `/` .

Ficheros de registro

El agente puede almacenar en un registro de texto (fichero *log*) la información de su estado, conexiones entrantes, problemas, etcétera. Para ello debe activar el *token* de configuración que especifica el fichero *log*:

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

Y también puede modificar cuanta información volcar a dicho fichero con el siguiente *token* de configuración.

```
verbose x
```

Donde X puede ser un valor numérico de 0 a 9. Un valor de 0 es información mínima, y un valor de 9 es información de depuración máxima. El agente no controla el tamaño del *log*, por lo que este, si está configurado para devolver la máxima información, puede generar un *log* muy grande.

```
verbose 4
```

Reprovisión del agente

Si por lo que fuera, necesitara reaprovisionar el agente, seguir los siguientes pasos:

- Detener el agente.
- Borrar del fichero de configuración los tokens de configuración: `eh_hash` y `eh_key` e iniciar de nuevo el agente. Debería provisionarse de nuevo con un EKID diferente.

Activar/Desactivar borrado de archivos

Se puede desactivar (por defecto está activado) la funcionalidad de borrar archivos desde el gestor de ficheros remoto. Para ello utilice el siguiente *token* de configuración:

```
enable_file_delete 0
```

Ocultar icono de la aplicación

Se puede desactivar (por defecto está activado) el que el servicio del agente de Pandora RC lance la aplicación de notificación de escritorio. Esta aplicación muestra su icono en el área de notificación (*tray area*). Para ello utilice el siguiente token de configuración:

```
hide_tray 1
```

El valor 1 hace que no se lance la aplicación y por tanto no se vea el icono. El valor por defecto es

0.

Avisos emergentes para acceso

Existe una funcionalidad opcional que permite que el usuario que está usando el ordenador reciba una notificación para informar o requerir confirmación del acceso externo. Esto es especialmente crítico para cumplir ciertas regulaciones legales de acceso remoto a equipos. Por defecto viene desactivado, pero para activarlo basta con activar ciertos *tokens* de configuración.

Esta funcionalidad se puede configurar de forma individual para regular como se accede a cada servicio (transferencia de ficheros, gestión de procesos, gestión de servicios, *shell* remota, escritorio remoto, compartir acceso) y también sirve para desactivar el uso de uno de esos servicios por si no se desea que esté disponible.

Los valores posibles para estos elementos de configuración son:

- `Request`: Se pedirá al usuario que acepte la conexión entrante, a través de una ventana emergente. Esta ventana tiene un timeout, y si no se acepta explícitamente la conexión al servicio, el acceso se denegará.
- `Inform`: Solamente informará al usuario. Si el usuario no la ve o pulsa el botón de que la ha visto, el usuario remoto entrará igualmente.
- `Always`: El usuario remoto entra sin que el usuario local tenga que autorizar ni ver ningún mensaje emergente. Es el valor por defecto
- `Disable`: El servicio no estará disponible en ningún caso.

```
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
```

Por otro lado, el elemento de configuración que define el timeout de la ventana de confirmación es:

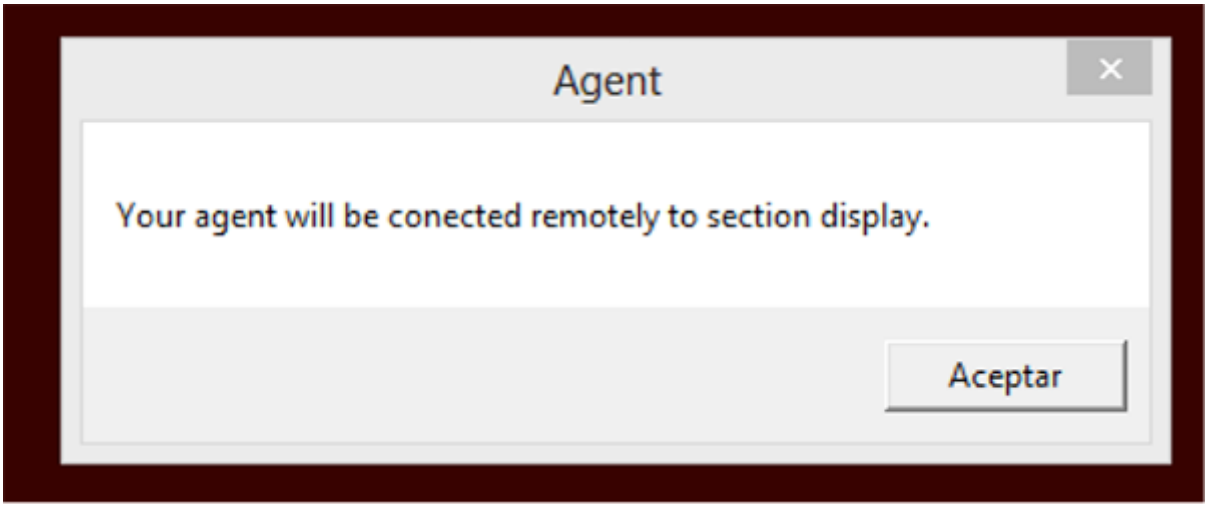
```
access_dialog_timeout 30
```

El valor por defecto es de 30 segundos. Este *timeout* no puede ser mayor del tiempo de refresco del *keepalive* del cliente, que son 60 segundos.

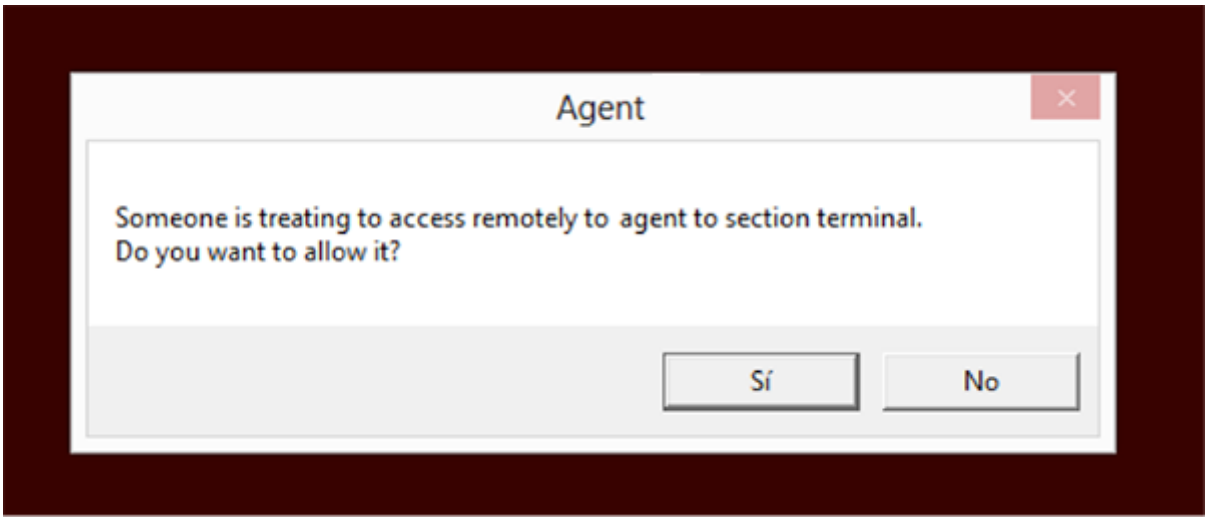
Para utilizar un sistema de *popups* personalizable, debe cargar una DLL externa:

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

El aspecto que tiene la pantalla de “Información” es este:



Y cuando la configuración “fuerza” al usuario local a confirmar la conexión, la información mostrada es la siguiente:



En GNU/Linux no está implementada esta funcionalidad.

Doble pantalla

En sistemas Windows que tengan más de una pantalla, el agente automáticamente intentará detectar la pantalla principal. En caso de querer usar otra pantalla o ambas pantallas a la vez, habrá que modificar el fichero de configuración del agente:

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

- El valor -1 muestra todas las pantallas.
- El valor 0 (por defecto) mostrará la pantalla principal.
- El valor 1 muestra la pantalla Nº 1 (la segunda, en la mayoría de los casos)
- El valor 2 (hasta infinito) mostrará la pantalla 2..3.. etc (si la hubiera).

Balanceo de servidores

A partir de la versión 1.1.0, el agente de Pandora RC puede pedir un nuevo servidor de forma automática al directorio antes de cada intento de conexión. Para habilitar esta característica, añada la siguiente línea al fichero de configuración del agente:

```
eh_balancing 1
```

Volver al Índice de Documentación Pandora FMS