User Manual

CYBERHAWK

USER MANUAL

TABLE OF CONTENTS

1. Introduction

1.1 Definitions

ANTIVIRUS	Antivirus is software designed to identify, neutralize and eliminate malicious software (including computer viruses).
ENCRYPTION	Encryption is a cryptographic process by which it is desired to make the comprehension of a document impossible for anyone who does not have the (de)encryption key.
CYBERHAWK	NÉOSOFT decontamination solution
LOG	The “log” term represents an event history and, by extension, the file containing this history.
SAS	A SAS is a mean that allows passing from one place to another, from one environment to another.

1.2 Abbreviations

AV	Antivirus
CSV	Comma-Separated Values
DNS	Domain Name System
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
IS	Information System
MySQL	My Structured Query Language
N / A	Non Applicable
Syslog	System Log
TXT	Text
USB	Universal Serial Bus
WEB	World Wide Web

2. Preamble

2.1 CyberHawk

In order to transfer files (firmware, documents etc.) from removable media (USB drives) to trusted / sensitive networks, physical interventions on network equipment(s) are required.

Inherent problematic with this practice is spreading (automatically or not) potentially malicious elements inside the trusted / sensitive network. These elements, according to their threat level, could affect the availability, integrity or confidentiality of the network.

The NÉOSOFT "CyberHawk" solution eliminates the need of removable media usage inside trusted / sensitive network, through the use of modules decontamination on an isolated server, accessible via a web interface for file transfers.

Access to the file management web interface can be provided on a separated information system (IS), or on a secure dedicated station (self-service / kiosk station).

Within CyberHawk, each user is free to create his personal space and transfer files of their choice. These files are then analyzed by several modules (antivirus engines, scripts, blacklists, etc.) before being stored (or deleted if a threat is detected by at least one antivirus).

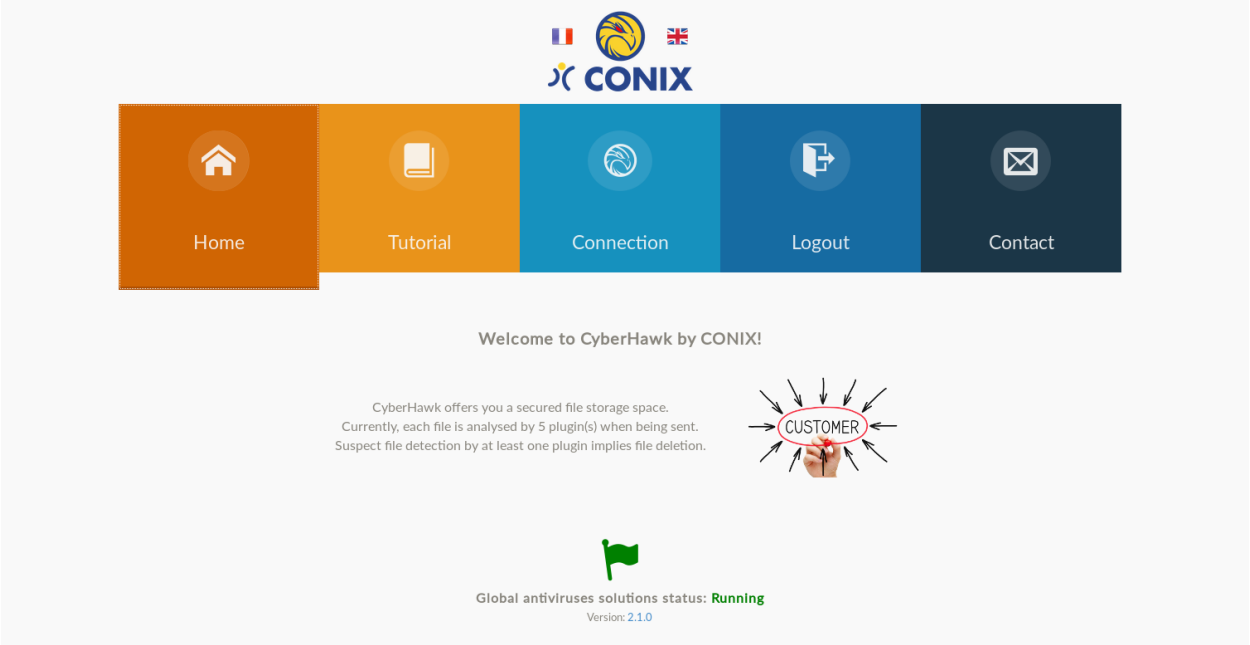
Unlike competitive solutions allowing USB keys decontamination on physical terminal, CyberHawk allows decontamination via the network, regardless of the medium used. It can also be used for secure files' exchange on the same network.

Note: Decontamination is performed on the sent file(s) but is not performed on the removable media.

2.2 WEB Access

Access to the application is possible via web browser in HTTP / HTTPS (according to the choice of the client). The choice of the browser used is free. However, access to the application via an obsolete or non-up-to-date browser can lead to the loss of certain functionalities (drag and drop, simultaneous transmission, transfer speed, etc.).

Basic use is possible whatever browser you choose. Please refer to the "Compatibility" section for more information on features related to recent browsers.



CyberHawk access URL is client-dependent (IP, DNS usage, SSL usage, etc.) and is therefore not cited in this manual.

Please note that in some cases and if requested by the customer, a workstation can be provided in "Web interactive Kiosk / Self-Service Station" mode to provide exclusive access to CyberHawk.

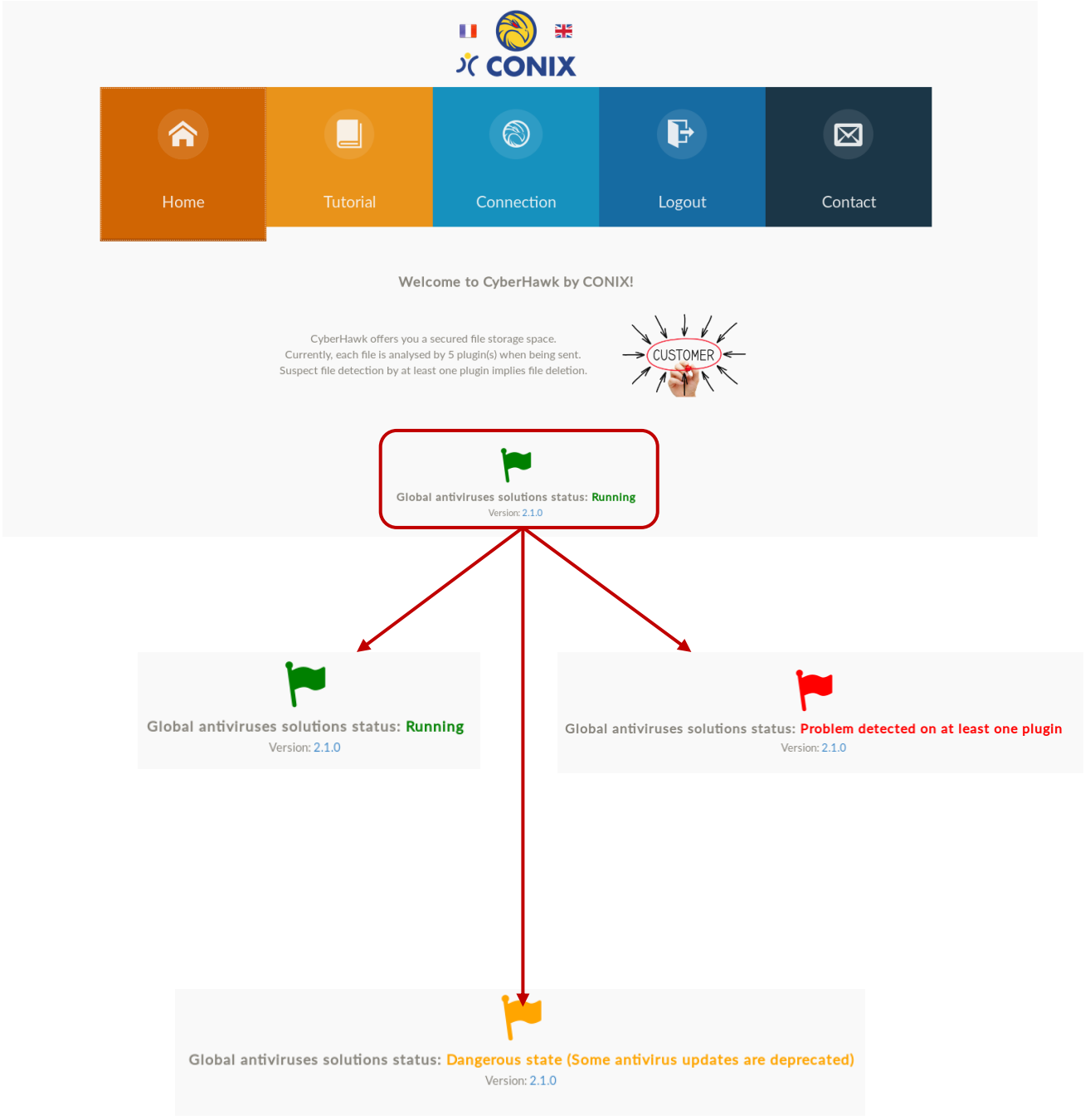
2.3 CyberHawk platform running state

Various plugins (antivirus engines, scripts, blacklists, etc.) are used by the CyberHawk platform to decontaminate the sent files. These modules are enabled during installation and may vary depending on the installation. Post-install activation / deactivation remains possible.

Three antiviruses are currently available in the solution, allowing complementarity and a wider field of detection:

NAME	LOGO
ClamAV	
Sophos	
Comodo	

Before any operation on the platform, each user can know the status of the various antivirus engines when accessing the home page of the CyberHawk WEB application. Three types of different antiviral statuses are available on the application, each with its consequences on the use of the application.



Details about platform and modules status can be viewed by clicking on the flag.

It is important to be aware of the consequences of each status before using the platform. In case of a state differing from a normal state (green), it is important to contact the CyberHawk administrator to investigate the source of the problem.

STATUS	COMMENTARIES	CONSEQUENCES	REMEDIATION
Running	Normal and correct operation of	None.	N / A

	all plugins. Antiviral databases are up to date.	Uploading and Downloading files are possible.	
Dangerous state	Normal and correct operation of all plugins. Antivirus databases are not up to date on one antivirus (at least).	None. Uploading and Downloading files are possible but dangerous.	Updates are normally performed automatically. **This type of message should not occur, please contact your administrator for investigation.**
Problem detected	Abnormal operation detected on one plugin (at least).	Uploading files is impossible because dangerous (impossible analysis). Only download of existing files on CyberHawk remains possible.	**This type of message should not occur, please contact your administrator for investigation.**

2.4 Access Modes

Depending on the choices made by your administrator during the installation, access to CyberHawk can be done in several ways:

1. With simple identification (Login only)
2. With authentication (Login / Password)
3. Using both manners (choice is made by the user according to the confidentiality of his documents)

Although registrations are free by default, some choices during installation may prevent this functionality:

1. Free registrations (default value)
2. Validated registrations (administrator's validation is required)
3. Registrations deactivated (users' database manually populated)

Finally, on administrator's request during the installation, personal data may be required during your registration (Name, First name).

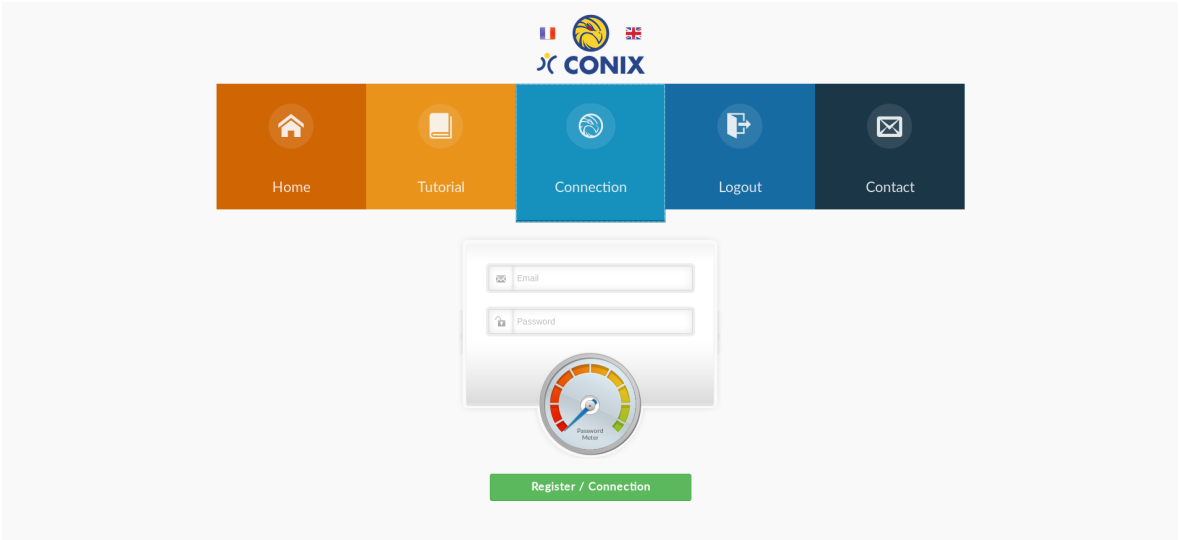
3. User Manual

3.1 Language selection

Although a default language choice is made during installation, it is possible for the user to switch to another language by clicking on the flag provided in the top frame of the screen.

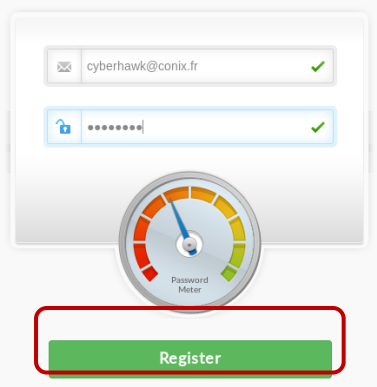
3.2 Registration

Access to personal space is available in the "Connection" central tab, whether you are already a user of the application or a new user. Registrations are free by default unless they have been explicitly disabled during installation.



Your registration process will be made according to the choices made during the CyberHawk installation. You will be guided step by step in the configuration of your personal space if you are new user.

To illustrate your registration, we will take the example of a registration with a complex password (authentication) and requesting personal information. Finally, we will take the configuration case requesting a validation by the administrator of your account. All other cases of registration are simpler.

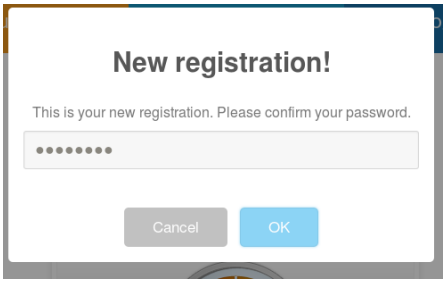


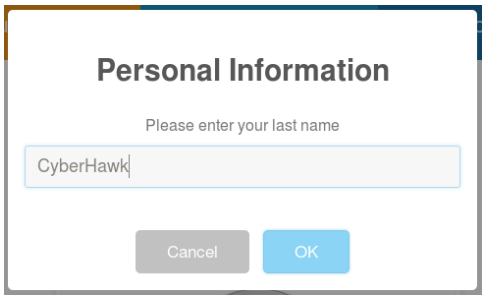
The first step of your registration is to choose an identifier (email address) and a password.

Length and complexity of this password depends on the choice of your administrator. Be sure to follow this policy and choose a valid password: a gauge will tell you in real time the robustness of your password.

Access to the next step is only possible if both fields are validated (valid email and password respecting the policy).

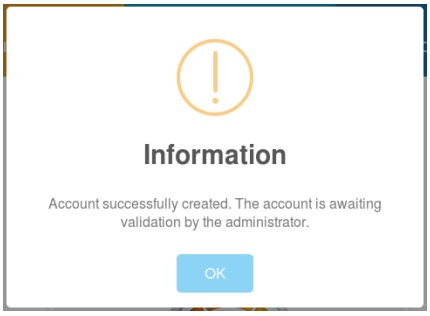
In case of a new registration and to avoid any oversight, please repeat your password before proceeding to the next step.



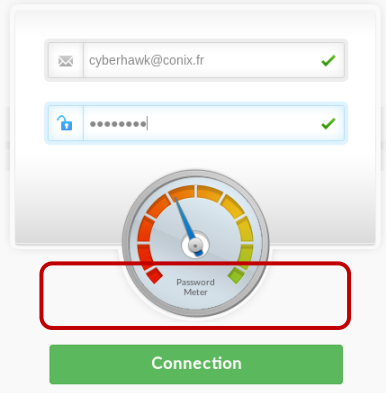


Then enter your personal information when it is requested to complete your registration process and access your personal sharing space.

In this case, a validation of the account by the administrator will be necessary before you can access your personal space. When no validation is required, you will be directly redirected to your personal CyberHawk space.



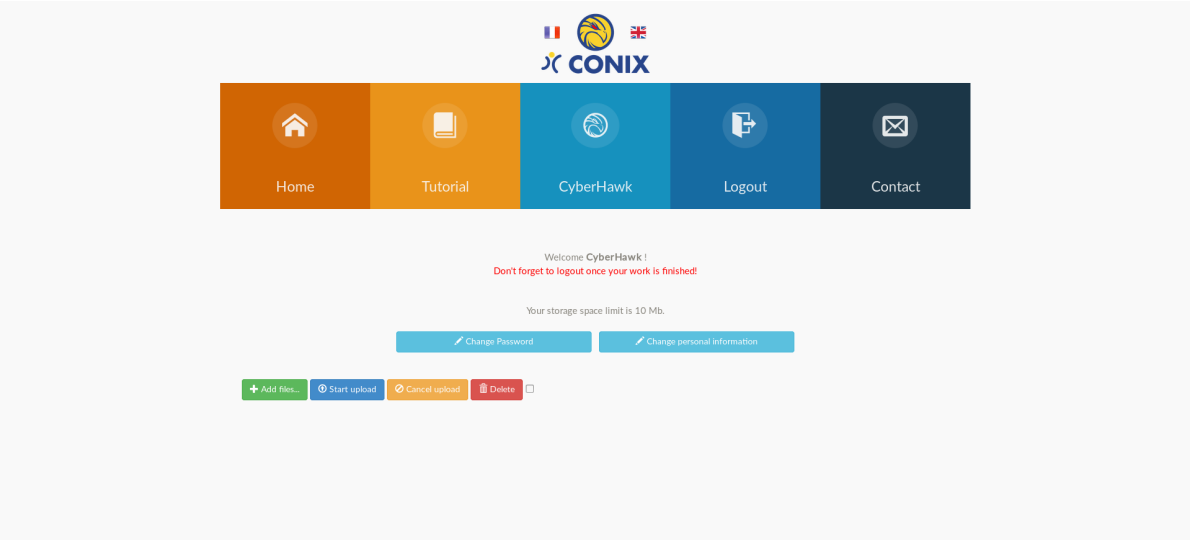
3.3 Identification / Authentication



When your account already exists on the application and has been validated by your administrator, you can connect directly to your personal space from the "Connection" central tab by entering your login and password.

In case your account does not have a password (identification), please leave the second field blank.

You will then be redirected directly to your personal space



Your personal space is unique and belongs to you. No other user is able to view your files (except when sharing). A storage space limit is assigned to you by your administrator (choice made during installation).

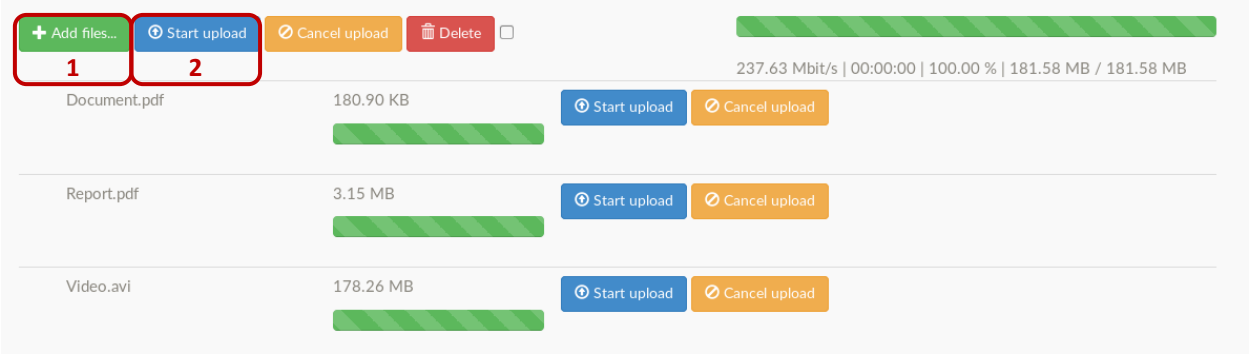
Once you have finished your work, do not forget to log out of the application using the “Logout” button.

Note: All personal spaces are emptied of their documents periodically, depending on the configuration chosen during installation. Thus, your old documents may disappear if they are on your space for too long (a week by default).

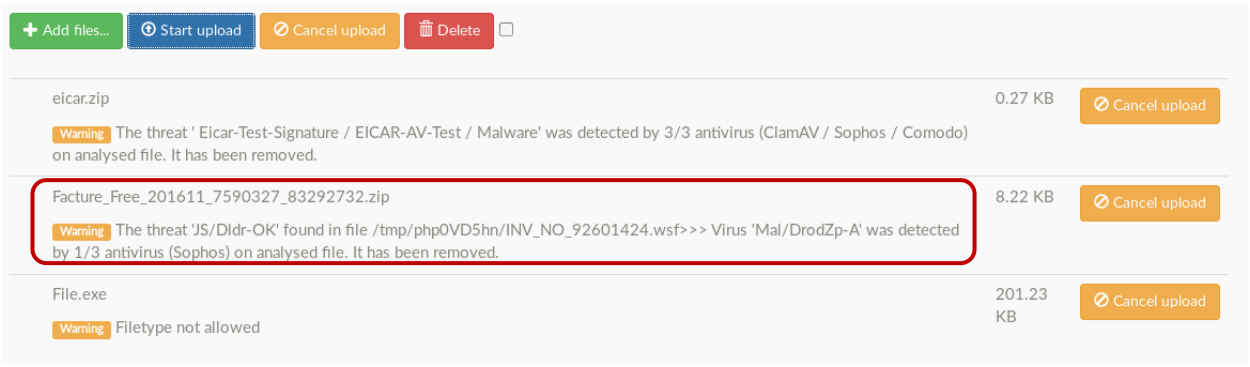
3.4 Files upload

After connecting to the application, you can upload your files using the provided interface.

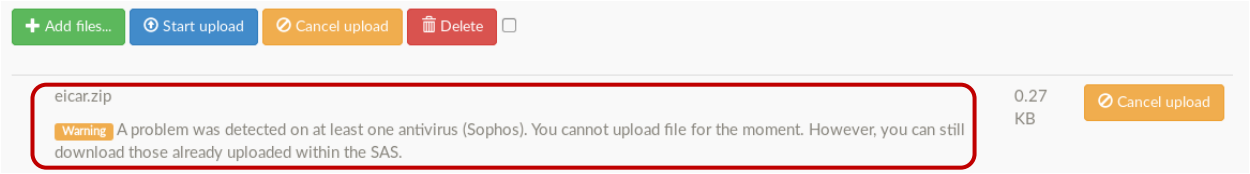
The CyberHawk interface allows simple file management (push, deletion). Each file is sent to the server and then scanned in order of receipt on CyberHawk by the three antivirus engines. This analysis can take some time, depending on the number of files to be analyzed as well as the number of simultaneous users.



When uploading an invalid file (size too large, prohibited extension, etc.) or when potentially infected file is detected (by at least one of the three antiviruses), the user is warned via the web interface, and the file is removed from the CyberHawk server. It will not be possible to access it again. However, it will remain on your media.

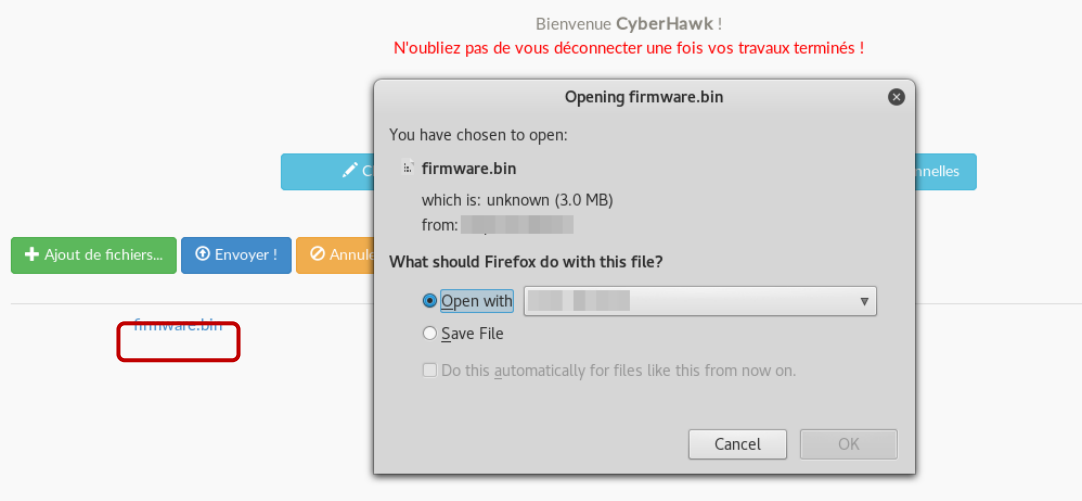


Finally, in case one of the antivirus is unable to analyze the files (as stated in §1.3), only already present files' download remains possible. All new uploads are blocked.



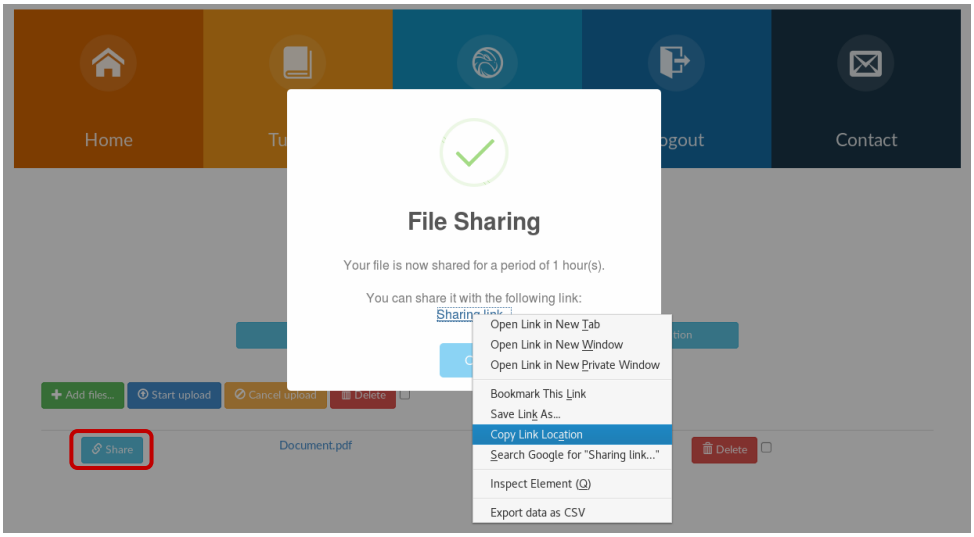
3.5 Files download

Once connected to the application, you can recover your safe files at any time, simply by clicking on it. A download window will open, allowing you to select the destination of your download.



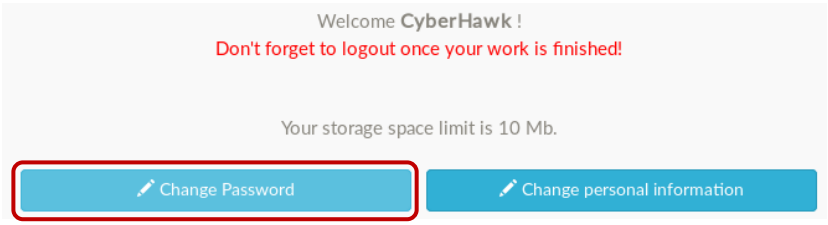
3.6 Files Sharing

When the option is activated by your administrator, you can, if you wish, share one of your documents with a third-party user, using CyberHawk or not. All you have to do is click on the sharing link, in order to generate a direct access link to the file, valid for a fixed time.



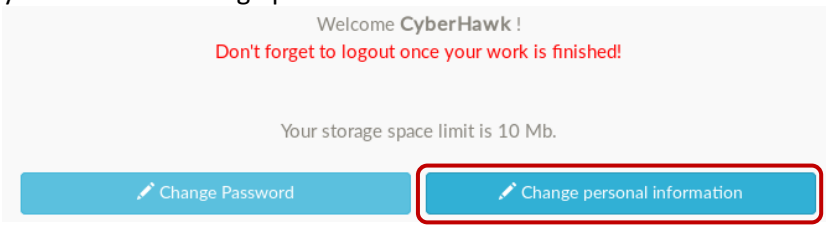
3.7 Password modification

You can, if you wish, change your password at any time within the application. Simply click on the "Change Password" button and follow the instructions!



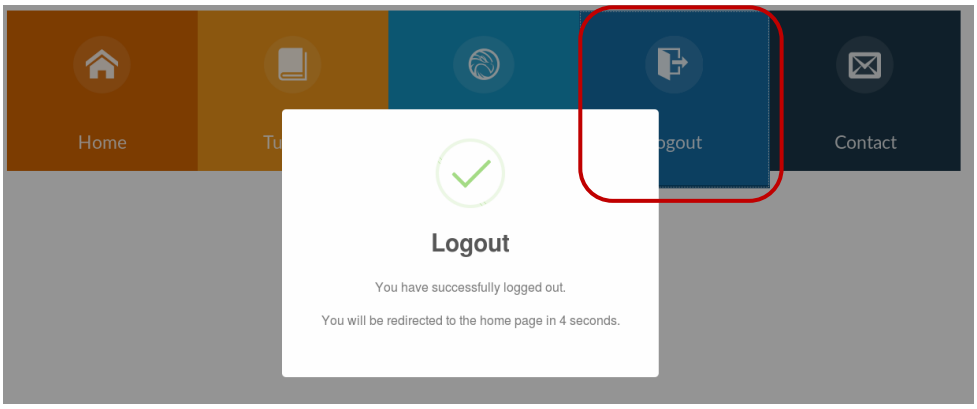
3.8 Personal data modification

You can, if you wish, change your personal data (Name, First name) at any time within the application. Simply click on the "Change personal information" button and follow the instructions!



3.9 Logout

When you have completed your work, do not forget to log out of the application using the button provided. Your logout will prevent the next user from accessing your data.

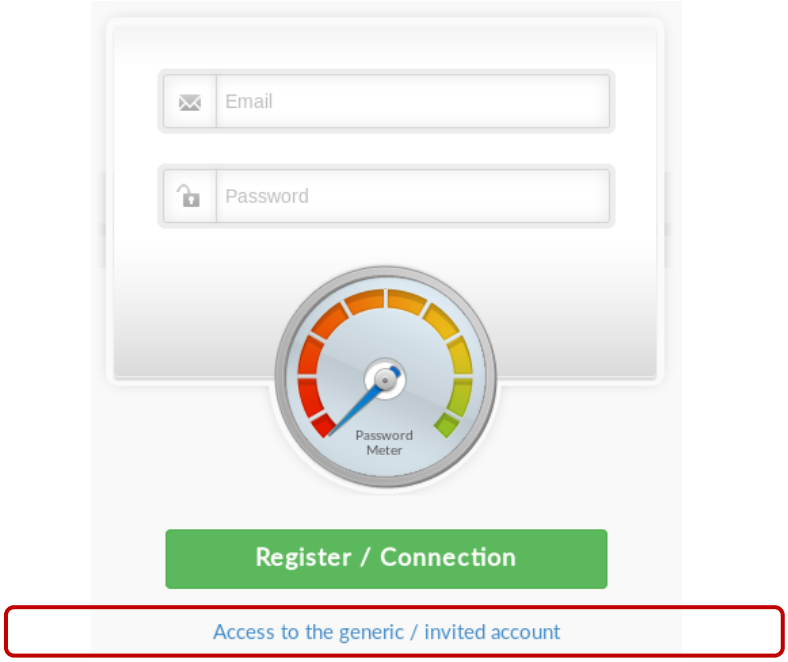


4. « Generic / Invited » Account

A « Generic / Invited » Account can be activated by the administrator during installation, or within his parameters.

When activated by administrator, a new button will appear during connection, allowing accessing CyberHawk without any account.

Important: « Generic / Invited » account is a shared account between all users using it. Data confidentiality is not guaranteed.



Once connected, this account can be used as a normal user account.

5. Kiosk / Self-Service Station

5.1 Startup

The platform startup is made as any computer (portable or not). A minimalist distribution is installed (from "Porteus Kiosk") and allows a partitioned startup on a read-only encrypted system.

During startup, no access to the system is possible and only the CyberHawk WEB interface is displayed in full screen. The system is configured to reject incoming connections and allow only outbound connections to the IP / URL of the CyberHawk server.

Since the system is read-only and encrypted, no post-installation configuration is possible. Any configuration changes (IP, URL, system settings) must be made when reinstalling the system.

5.2 General Use

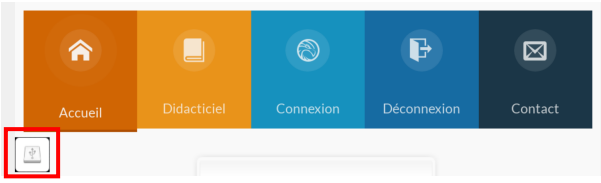
The use of CyberHawk in kiosk / self-service mode remains the same as the normal use described above (§3).

Only few points differ when uploading and downloading a file. Since the system is read-only, only uploads / downloads to / from removable media are possible. Before any action, it is necessary to insert a removable media in the kiosk / self-service station.

File upload is done in the same way as described above (§3) by selecting the file(s) to be sent from the removable media.

File download is done automatically, directly to the removable media if it is inserted.

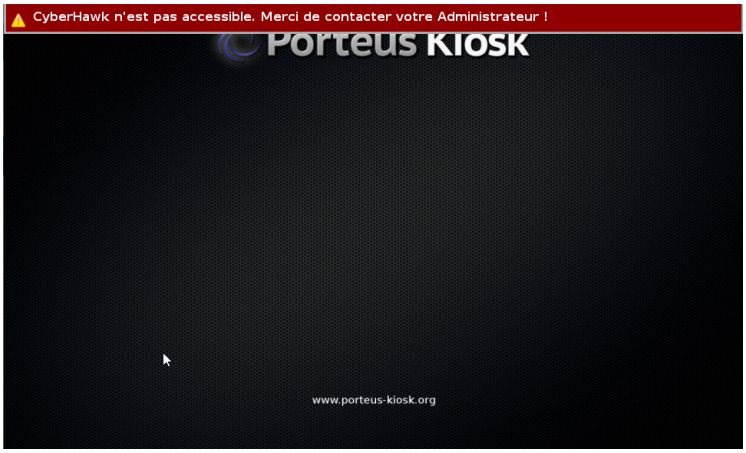
The removable media can then be removed from the system after disconnecting it using the provided button.



It may happen that the disconnection is not taken into account when using the button if the key is still being read / written. If so, just wait a few seconds before trying again.

5.3 Issues & Remediation

In the case that the IP / URL of CyberHawk server is not accessible, the following capture message is displayed to the user and the Kiosk will not start. Please check the network connection and status of CyberHawk platform before restarting the self-service station.

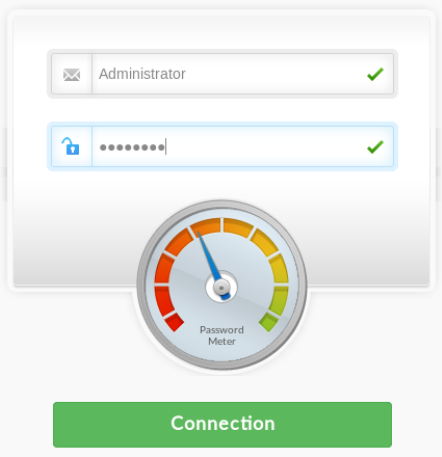


If there is an issue with the kiosk / self-service station (blocking, slowdowns, etc.), it is only necessary to restart it.

6. Administrator Manual

6.1 Authentication

Access to the administration interface is made with authentication only (with password). The process is the same as for user authentication. An 'Administrator' account is created during installation with a complex password set.

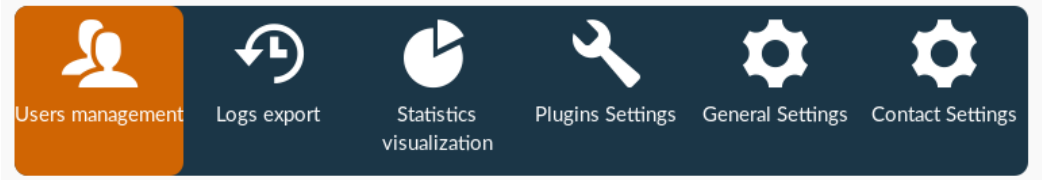


In addition to administrative features, the administrator has a sharing space similar to users' one. However, its space is unlimited and can allow to manually upload updates to antiviral engines (if needed).

6.2 General Settings

Access to CyberHawk general settings is available only from Administrator interface, clicking on the « Settings » button.

These settings, rebuilt in new 2.1.0 version, allow performing users' management, but also general platform settings (post-install).

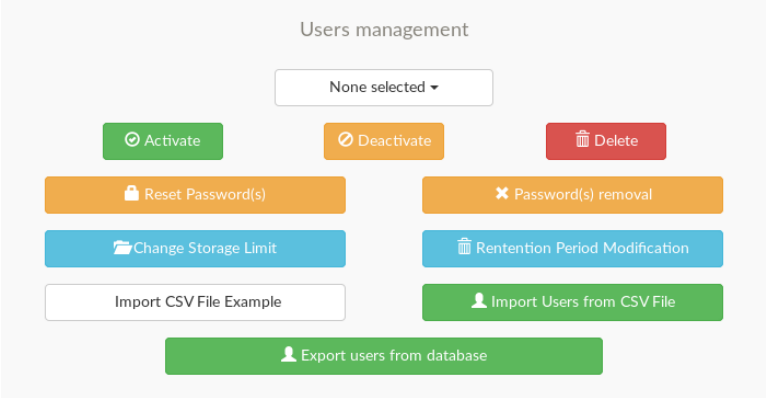


6.3 Users management

User management remains relatively simple in CyberHawk and allows the following actions:

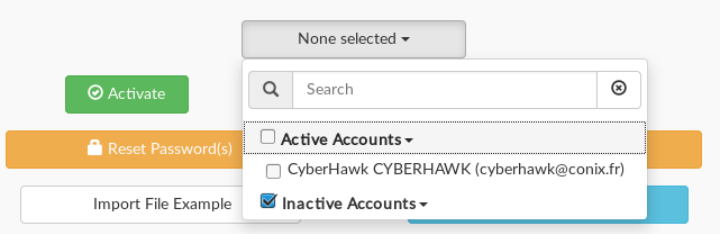
- Activation / Deactivation / Removal of users' accounts
- Users' passwords resetting

- Removing users' account passwords (changing authentication to identification)
- Change storage limit for some users
- Change retention period for some users
- Importing users from an Excel file (CSV) with sample file available
- Export users from database



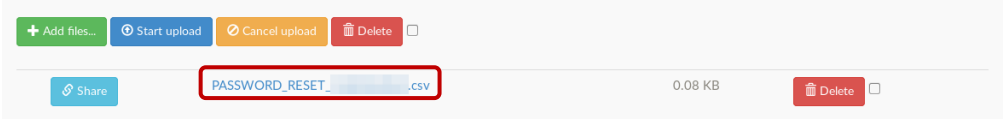
Users are displayed in a drop-down menu and divided into two groups:

- Active accounts
- Inactive accounts



Whatever the action (except import detailed below), the first step is to select the users concerned and then to apply the action. The effect is immediate for some, with confirmation for others.

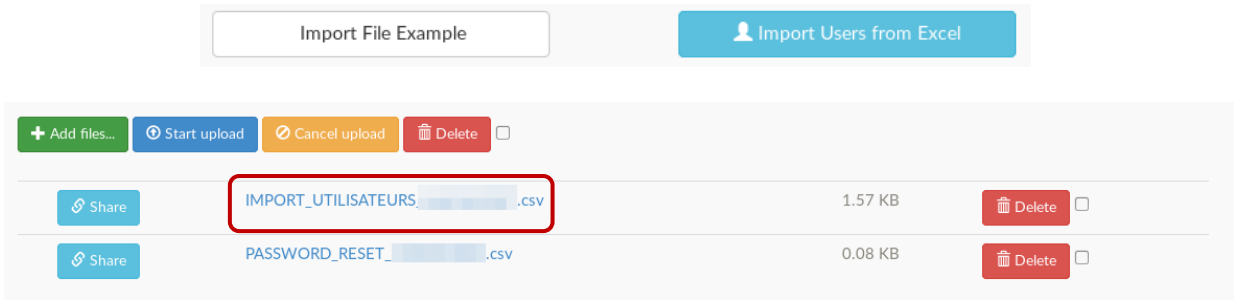
When resetting user passwords, a CSV file is created in the administrator's personal space. This file contains a list of all affected users and their new password.



	A	B	C	D	E
1	Nom	Prénom	Email	Password	
2	CyberHawk	CyberHawk	cyberhawk@conix.fr	b(lBphuOP5	
3	Dupont	Jacques	jacques.dupont@cyberhawk.fr	756RDrQ(1j	
4					

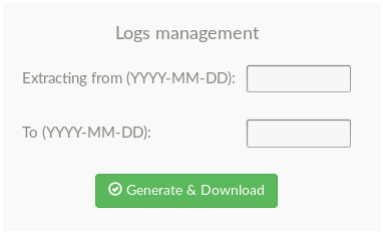
Finally, importing user(s) is possible from a CSV file. The format of this CSV file must be strictly respected (Name, First name, Email) to allow a correct insertion. A sample file can be downloaded directly from the application ("Import File Example" button). Once completed, this file has to be

uploaded in the administrator interface (with its other files), before clicking on the button "Import Users from Excel". When the import completes, the CSV file is replaced with a new one, containing all imported users and their generated passwords.



6.4 Logs export

Application logs are available in Syslog and MySQL format. They can also be consulted in XML format by the administrator via the CyberHawk WEB interface. He only needs to use the extraction form provided.



When generating the log file, a XML file is created in the administrator's personal space. This file contains all the application logs (connection failures, file submissions, virus detections, etc.).

6.5 Statistics visualization

Currently, two types of statistics are available within CyberHawk:

- Modules' detections since CyberHawk install
- Modules' detections since 1 year

These statistics will be improved within future versions.

6.6 Plugins Settings

This new tab allows changing modules settings after installation. It allows the following actions:

- Module Activation / Deactivation
- Adding / Removing extensions within Whitelist / Blacklist
- Modifying alerts delays (for antivirus only)
- Adding new modules (Antivirus, scripts, etc.)

6.7 General Settings

This new tab allows changing CyberHawk settings after installation. It allows the following actions:

- Change default language
- Activation / Deactivation of plugins analysis for Administrator
- Activate / Deactivate « Generic / Invited » account
- Etc.

6.8 Contact Settings

This new tab allows changing CyberHawk “Contact” page settings after installation.

6.9 Manual antiviral signatures updates

Although advised to be made automatically using a CyberHawk Update Server (internally), manual updating of antiviral engines is still possible.

It can only be done from the administrator account by following the following steps:

1. Manually download the update package from the mirror server. The mirror server makes this package available for each of our CyberHawk customers.
    a. http://www.IP or DNS/download.php?clientid=XXXXX-[...]-XXXXX
    b. Client ID (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX): Unique client identifier, provided during CyberHawk installation.
    c. The downloaded file is encrypted with a unique dedicated key for each client. It can only be decrypted by the CyberHawk server, which verifies its integrity and the validity of its contents.

2. Upload the downloaded file to the 'Administrator' account personal space.

3. The file will be taken into account automatically by CyberHawk at its next update, by default at midnight.

7. Compatibilities

The application is compatible with the following browsers:

- Google Chrome - 7.0+
- Apple Safari - 4.0+
- Mozilla Firefox - 3.0+
- Opera - 10.0+
- Microsoft Internet Explorer 6.0+

However, some features are only available on some recent browsers:

- Select and upload multiple files
  - *Firefox 3.6+*
  - *Safari 5+*
  - *Google Chrome*
  - *Opera 11+*
- Drag & Drop
  - *Firefox 4+*
  - *Safari 5+*
  - *Google Chrome*
- Download progress bar
  - *Firefox 4+*
  - *Safari 5+*
  - *Google Chrome*
- Images preview
  - *Firefox 4+*
  - *Google Chrome*
  - *Opera 11+*