Manuel Utilisateur

CYBERHAWK

MANUEL UTILISATEUR

SOMMAIRE

1. Introduction

1.1 Définitions

ANTIVIRUS Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (dont les virus informatique).

CHIFFREMENT Le chiffrement (ou cryptage) est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.

CYBERHAWK Solution NÉOSOFT de SAS de décontamination.

LOG Le terme log désigne un historique d'événements et par extension le fichier contenant cet historique.

SAS Le SAS est un dispositif qui permet de passer d'un lieu à un autre, d'un environnement à un autre.

1.2 Abréviations

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

2. Préambule

2.1 CyberHawk

Afin de transférer des fichiers (firmwares, documents, etc.) contenus sur des média amovibles (supports USB) vers des réseaux de confiance (ou à sécurité renforcée), des interventions physiques sur les équipements du réseau sont nécessaires.

La problématique inhérente à cette pratique reste la propagation (automatique ou non) d'éléments potentiellement malveillants à l'intérieur du réseau de confiance. Ces éléments, en fonction de leur niveau de menace, pourraient porter atteinte à la disponibilité, l'intégrité ou encore à la confidentialité de celui-ci.

La solution de SAS NÉOSOFT « CyberHawk » permet de s'affranchir du besoin d'utilisation de médias amovibles à l'intérieur du réseau de confiance, grâce à l'utilisation d'un serveur de décontamination cloisonné, accessible via une interface web d'échange de fichiers.

L'accès à l'interface web de gestion de fichiers peut être mis à disposition sur un système d'information (SI) séparé de moindre importance, ou sur une station dédiée sécurisée (borne libre-service).

Sur CyberHawk, chaque utilisateur est libre de créer son espace personnel et de transférer les fichiers de son choix. Ces fichiers sont ensuite analysés par plusieurs modules (solutions antivirales, routines, Blacklists, etc.) avant d'être stockés (ou supprimés si une menace est détectée par au moins un module).

Contrairement aux solutions physiques concurrentes permettant la décontamination de clés USB sur borne, CyberHawk permet une décontamination via le réseau quel que soit le support utilisé. Elle peut aussi être utilisée pour l'échange sécurisé de fichiers sur un même réseau.

Note : La décontamination est effectuée sur le / les fichier(s) envoyé(s) mais n'est pas réalisée sur le média amovible.

2.2 Accès WEB

L'accès à l'application est possible sur navigateur web en HTTP / HTTPS (selon le choix du client). Le choix du navigateur utilisé est libre. Néanmoins, l'accès à l'application via un navigateur obsolète ou non à jour peut mener à la perte de certaines fonctionnalités (glisser-déposer, envois simultanés, vitesse de transfert, etc.).

Une utilisation basique est possible quel que soit le navigateur choisi. Merci de vous référer à la section « Compatibilité » pour plus de précisions sur les fonctionnalités liées aux navigateurs récents.

L'URL d'accès de CyberHawk est dépendante du client (IP, Utilisation DNS, Utilisation SSL, etc.) et n'est donc pas citée dans ce manuel.

Veuillez enfin noter que, dans certains cas et si le client en fait la demande, une station de travail peut être fournie en mode « kiosque web / borne interactive » afin de fournir un accès exclusif à CyberHawk.

2.3 Etat de la plateforme CyberHawk

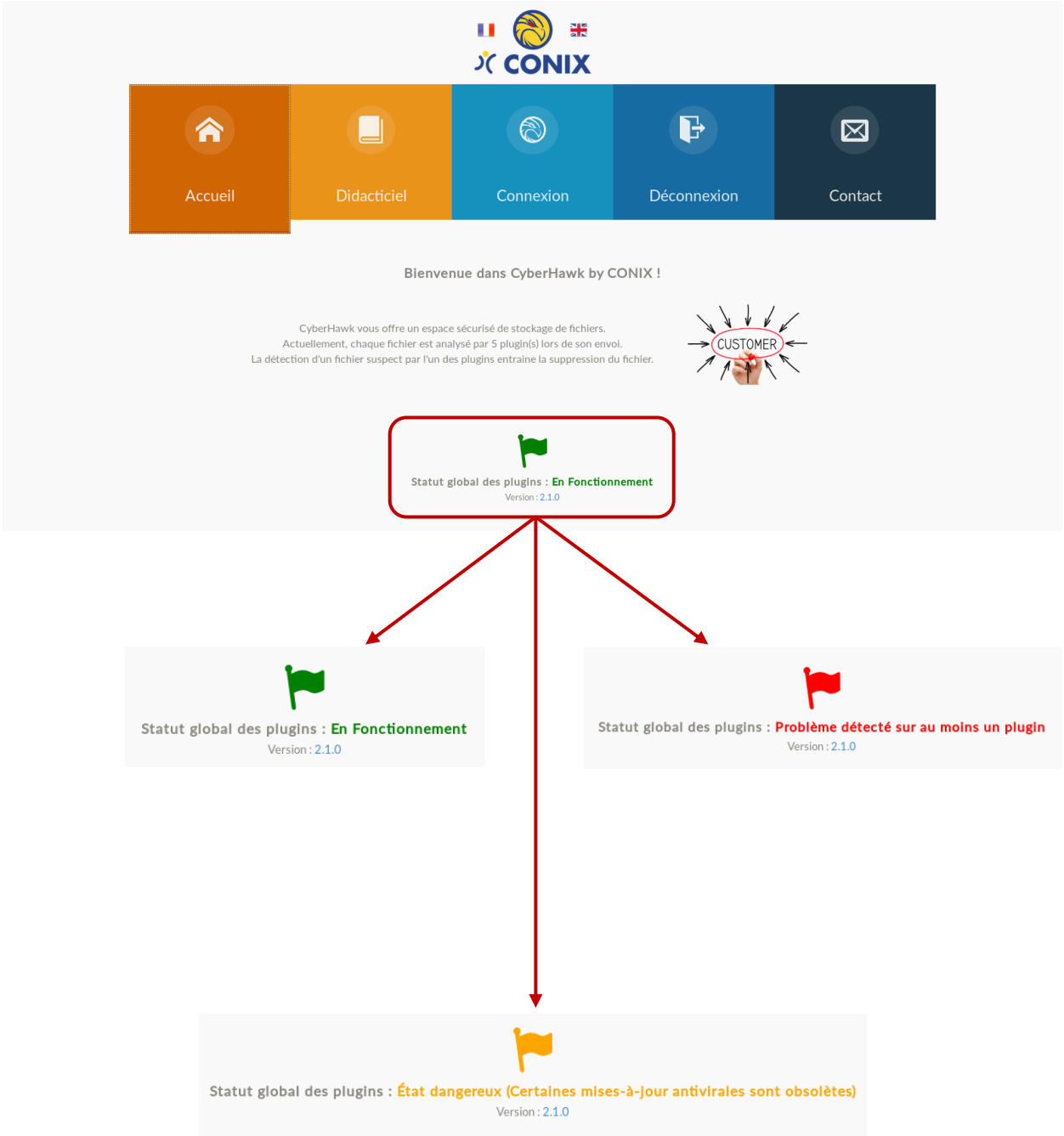
Différents modules (antivirus, routines, scripts, etc.) sont utilisés par la plateforme CyberHawk afin de décontaminer les fichiers envoyés. Ces modules sont activés lors de l'installation et peuvent varier en fonction des installations. L'activation / désactivation post-install des modules reste possible.

Trois antivirus sont pour le moment disponibles dans la solution, permettant une complémentarité ainsi qu'un champ de détection plus vaste :

NOM	LOGO
ClamAV	
Sophos	
Comodo	

Avant toute opération sur la plateforme, il est possible pour chaque utilisateur de connaître l'état des différents moteurs antiviraux lors de l'accès à la page d'accueil de

l'application WEB CyberHawk. Trois types de statuts antiviraux différents sont disponibles sur l'application, avec chacun ses conséquences sur l'utilisation de l'application.



Les détails sur l'état de la plateforme et des modules peuvent être visionnés en cliquant sur le drapeau.

Il convient de prendre conscience des conséquences de chaque statut avant toute utilisation de la plateforme. Dans le cas d'un état différent du fonctionnement normal (vert), il est impératif de contacter l'administrateur CyberHawk pour investigation sur la source du problème.

STATUT	COMMENTAIRES	CONSEQUENCES	REMEDIATIONS
En fonctionnement	Fonctionnement normal et correct de tous les modules. Les bases antivirales sont à jour.	Aucune. Dépôt et récupération de fichiers possible.	N / A
Etat dangereux	Fonctionnement normal et correct de tous les modules. Les bases antivirales ne sont pas à jour sur un antivirus (au moins).	Aucune. Dépôt et récupération de fichiers possible mais dangereuse.	Les mises-à-jour sont normalement effectuées automatiquement. **Ce type de message ne devant pas survenir, merci de contacter votre administrateur pour investigation.**
Problème détecté	Fonctionnement anormal détecté sur un module (au moins).	Dépôt de fichiers impossible car dangereuse (analyse impossible). Seule la récupération de fichiers déjà existants sur CyberHawk reste possible.	**Ce type de message ne devant pas survenir, merci de contacter votre administrateur pour investigation.**

2.4 Modes d'accès

En fonction des choix faits par votre administrateur lors de l'installation, l'accès à CyberHawk peut se faire de plusieurs façons :

1. Par simple identification (Login uniquement)
2. Par authentification (Login / Password)
3. Par les deux manières (au choix de l'utilisateur en fonction de la confidentialité de ses documents)

Egalement, bien que les inscriptions soient libres par défaut, certains choix lors de l'installation peuvent empêcher cette fonctionnalité :

1. Inscriptions libres (par défaut)
2. Inscriptions à validations (une validation du compte par l'administrateur est nécessaire)
3. Inscriptions désactivées (base d'utilisateurs peuplée manuellement)

Enfin, sur demande de l'administrateur à l'installation, des données personnelles peuvent être requises lors de votre inscription (Nom, Prénom).

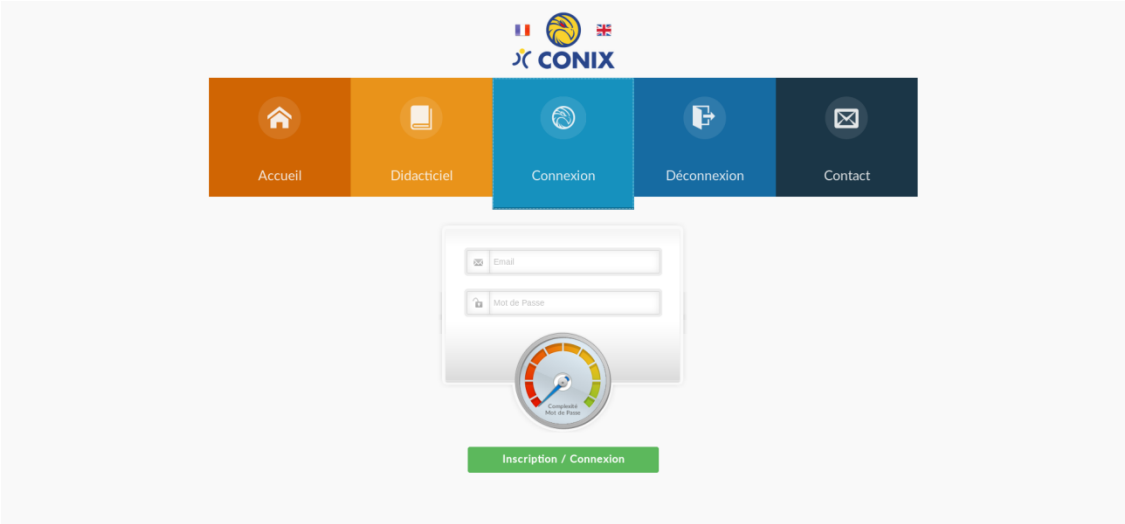
3. Manuel Utilisateur

3.1 Choix de langue

Bien qu'un choix de langue par défaut soit fait à l'installation, il est possible pour l'utilisateur de basculer vers une autre langue en cliquant sur le drapeau prévu à cet effet dans le cadre haut de l'écran.

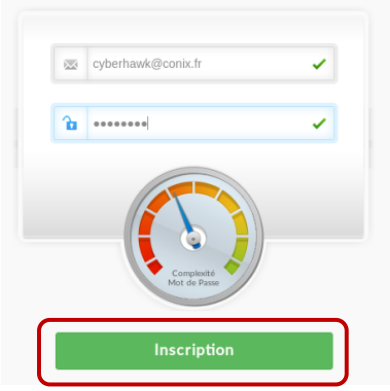
3.2 Inscription

L'accès à l'espace personnel est disponible dans l'onglet central « Connexion », que vous soyez déjà utilisateur de l'application ou nouvel utilisateur. Les inscriptions sont libres par défaut, sauf si elles ont été explicitement désactivées à l'installation.



Votre parcours d'inscription sera dicté par les choix réalisés lors de l'installation CyberHawk tout en vous guidant pas à pas dans la configuration de votre espace personnel si vous êtes nouvel utilisateur.

Pour illustrer au mieux votre inscription, nous prendrons l'exemple d'une inscription avec mot de passe complexe (authentification) et demande d'informations personnelles. Enfin, nous prendrons le cas de configuration demandant une validation par l'administrateur de votre compte. Tous les autres cas d'inscription étant plus simples.

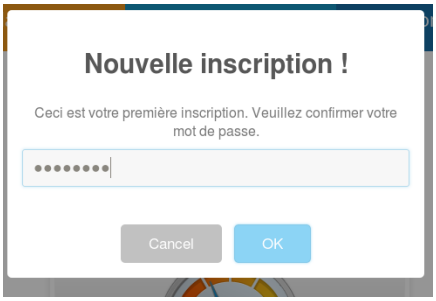


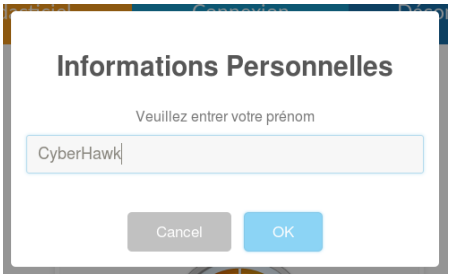
La première étape de votre inscription consiste à choisir un identifiant (adresse email) ainsi qu'un mot de passe.

La longueur et la complexité de celui-ci dépendent du choix de votre administrateur. Veillez donc à respecter cette politique et à choisir un mot de passe valide : une jauge vous indiquera en temps réel la robustesse de votre mot de passe.

L'accès à l'étape suivante n'est possible que si les deux champs sont validés (courriel valide et mot de passe respectant la politique).

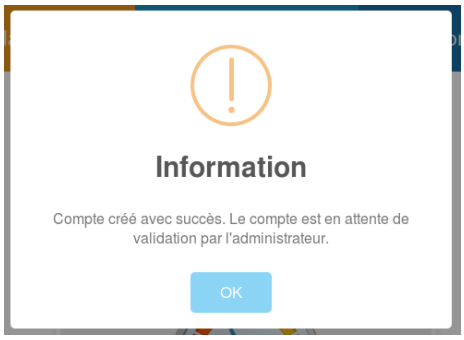
Lors d'une nouvelle inscription et afin d'éviter tout oubli, veuillez répéter votre mot de passe avant de passer à l'étape suivante.



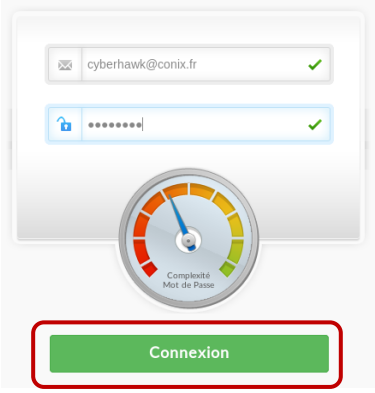


Saisissez ensuite vos informations personnelles à mesure qu'elles vous sont demandées afin de terminer votre processus d'inscription et de pouvoir accéder à votre espace personnel de partage.

Dans le cas présent, une validation du compte par l'administrateur sera nécessaire avant de pouvoir accéder à votre espace personnel. Lorsqu'aucune validation n'est nécessaire, vous serez alors directement redirigé vers votre espace CyberHawk.



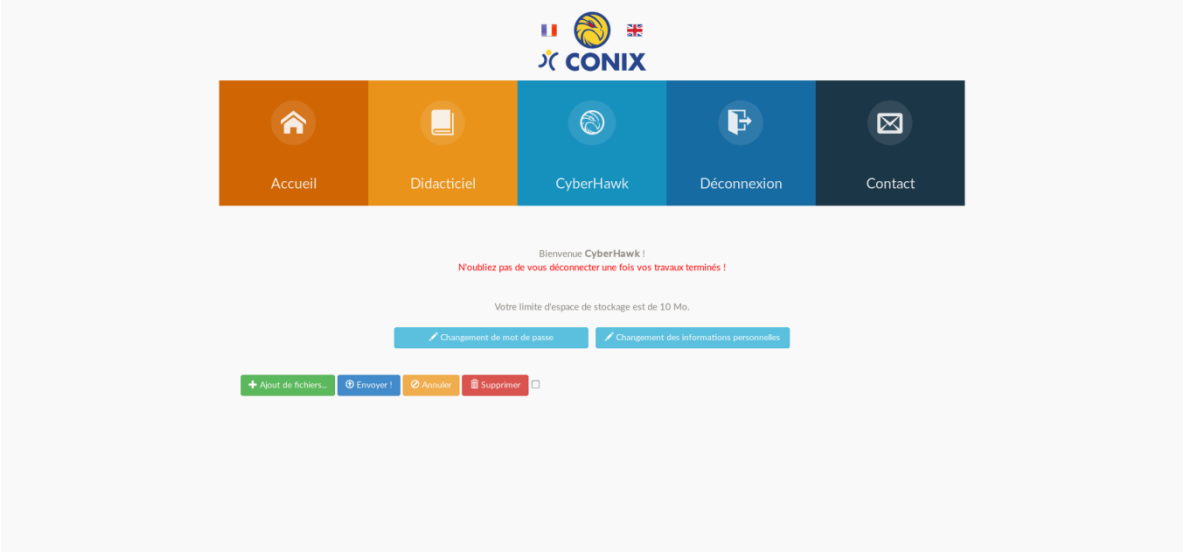
3.3 Identification / Authentification



Lorsque votre compte existe déjà sur l'application et a été validé par votre administrateur, vous pouvez vous connecter directement à votre espace personnel depuis l'onglet central « Connexion » en renseignant votre identifiant (email) ainsi que votre mot de passe de connexion.

Dans le cas ou votre compte ne comporte pas de mot de passe (identification), veuillez laisser le second champ vide.

Vous serez ensuite redirigé directement vers votre espace personnel



Votre espace personnel est unique est vous appartient. Aucun autre utilisateur n'est en mesure de récupérer vos fichiers (sauf en cas de partage). Une limite d'espace de stockage vous est attribuée par votre administrateur (choix lors de l'installation).

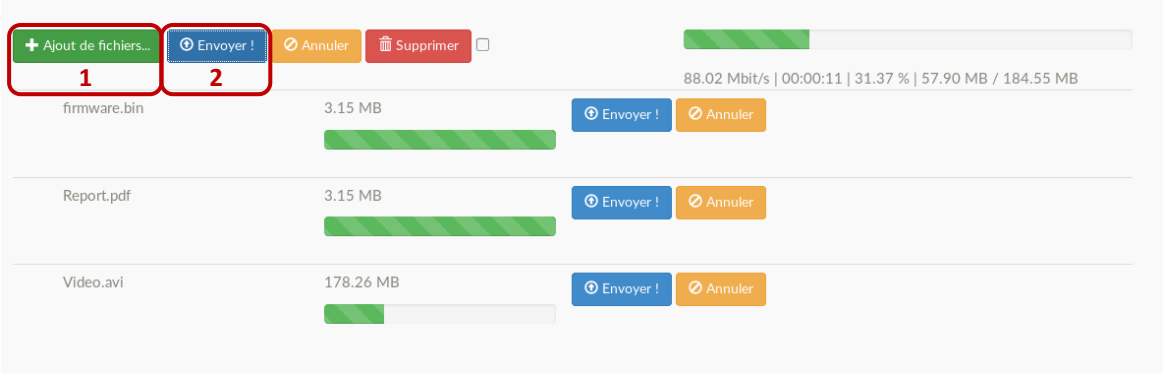
Une fois vos travaux terminés, n'oubliez pas de vous déconnecter de l'application en utilisant le bouton prévu à cet effet.

Note : Tous les espaces personnels sont vidés de leurs documents périodiquement, selon la configuration choisie lors de l'installation. Ainsi, il se peut que vos anciens documents disparaissent s'ils sont sur votre espace depuis trop longtemps (une semaine par défaut).

3.4 Envoi de fichiers

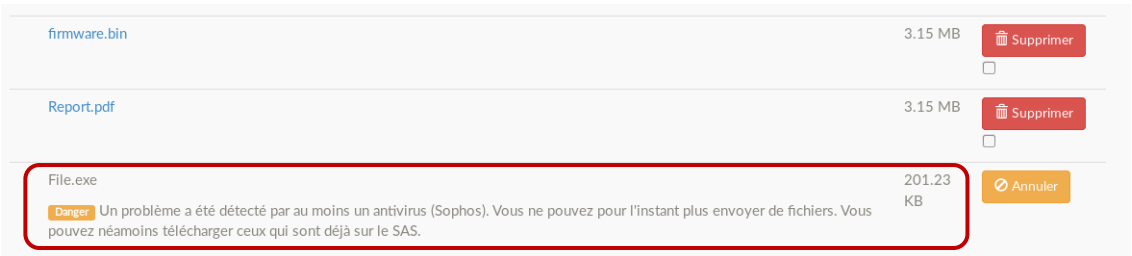
Après votre connexion à l'application, il vous est possible d'envoyer vos fichiers grâce à l'interface prévue à cet effet.

L'interface CyberHawk permet une gestion simple des fichiers (ajout, suppression). Chaque fichier est envoyé vers le serveur, puis analysé dans l'ordre de réception par CyberHawk par les trois moteurs antiviraux. Cette analyse peut prendre un certain temps, en fonction du nombre de fichiers à analyser ainsi que du nombre d'utilisateurs simultanés.



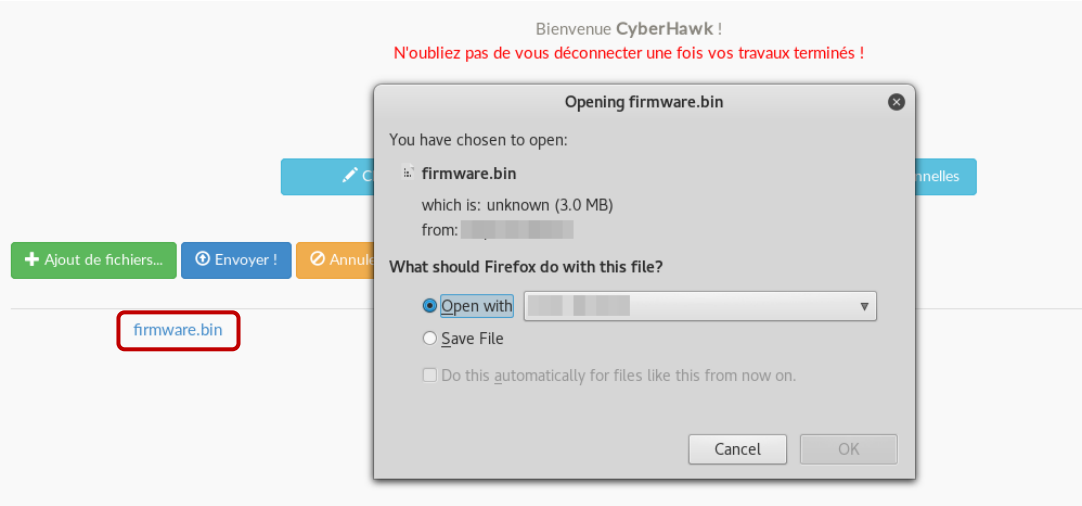
Lors de l'envoi d'un fichier invalide (taille trop importante, extension interdite, etc.) ou de la détection d'un fichier potentiellement infecté (par au moins l'un des trois antivirus), l'utilisateur est averti via l'interface, et le fichier est supprimé du serveur CyberHawk. Il ne sera pas possible d'y accéder de nouveau. Il reste néanmoins sur votre média.

Enfin, dans le cas où l'un des antivirus ne serait pas en mesure d'analyser les fichiers (tel qu'énoncé en §1.3), seule la récupération de fichiers déjà présents reste possible. Tous les nouveaux envois sont bloqués.



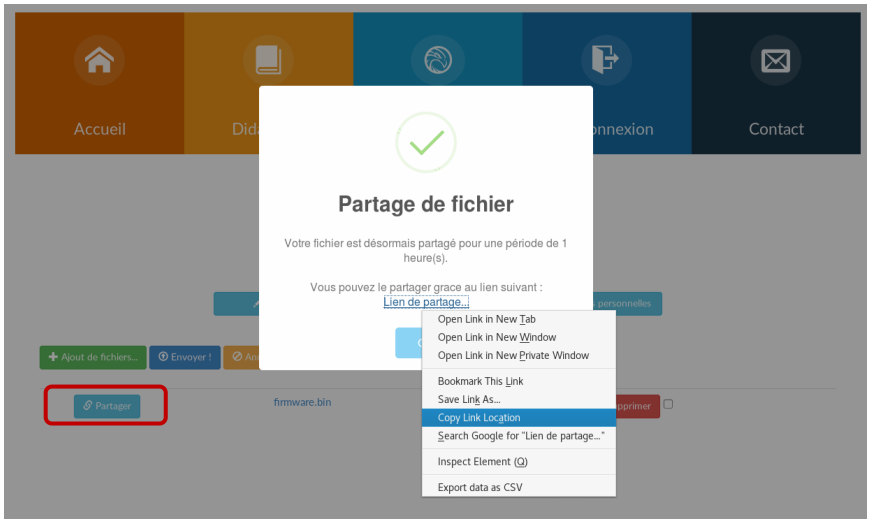
3.5 Récupération de fichiers

Une fois connecté sur l'application, vous pouvez récupérer vos fichiers sains à tout moment, simplement en cliquant dessus. Une fenêtre de téléchargement s'ouvrira alors, vous permettant de sélectionner la destination de votre téléchargement.



3.6 Partage de fichiers

Lorsque l'option est activée par votre administrateur, vous pouvez, si vous le désirez, partager l'un de vos documents avec une tierce personne, utilisatrice ou non de CyberHawk. Il vous suffit seulement de cliquer sur le lien de partage, afin de générer un lien d'accès direct au fichier, valide pour une durée déterminée.



3.7 Modification du mot de passe

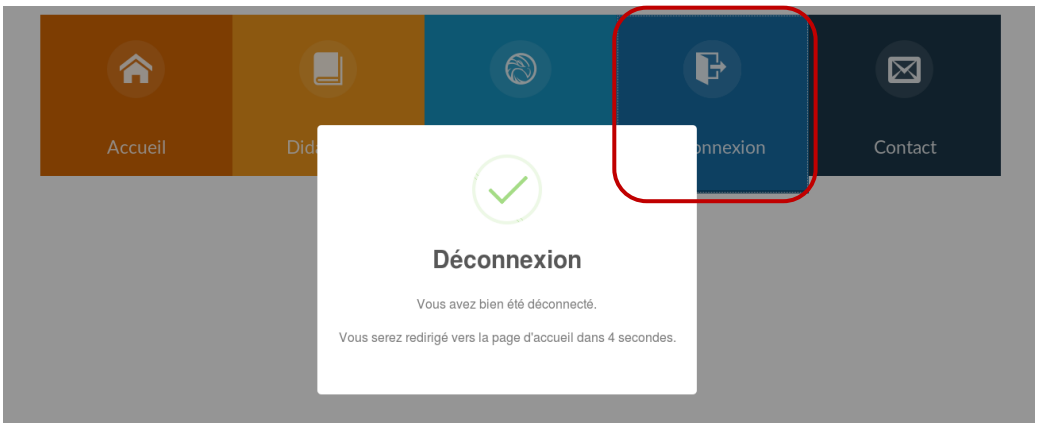
Vous pouvez, si vous le désirez, changer à tout moment votre mot de passe au sein de l'application. Il vous suffit simplement de cliquer sur le bouton « Changement de mot de passe » et de suivre les instructions !

3.8 Modification des données personnelles

Vous pouvez, si vous le désirez, changer à tout moment vos données personnelles (Nom, Prénom) au sein de l'application. Il vous suffit simplement de cliquer sur le bouton « Changement des informations personnelles » et de suivre les instructions !

3.9 Déconnexion

Une fois vos travaux terminés, n'oubliez pas de vous déconnecter de l'application en utilisant le bouton prévu à cet effet. Votre déconnexion empêchera l'utilisateur suivant d'accéder à vos données.

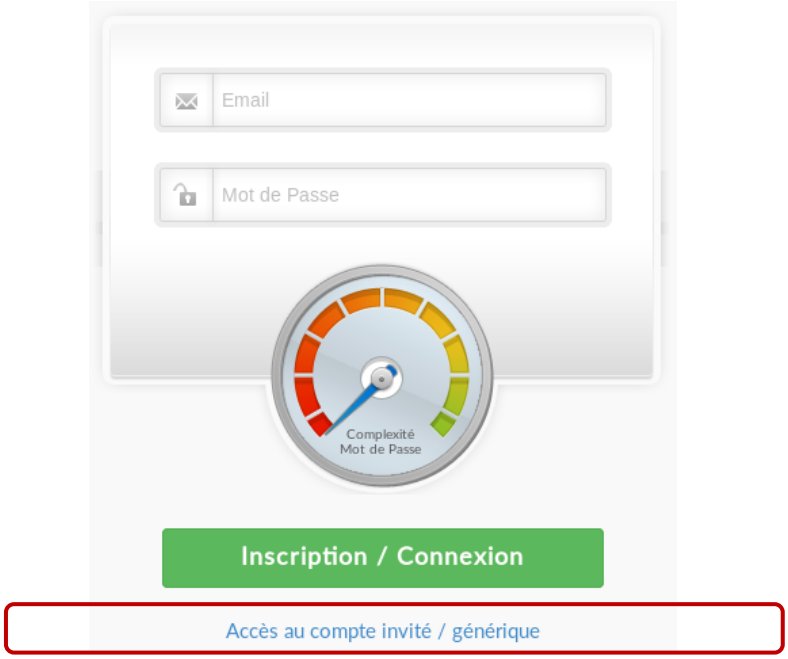


4. Compte « Générique / Invité »

Un compte « Générique / Invité » peut être activé par l'administrateur lors de l'installation, puis ensuite dans ses paramètres.

Lorsque ce module est activé par l'administrateur, un nouveau bouton est affiché lors de la connexion et permet l'accès à CyberHawk sans compte.

Attention : Le compte « Générique / Invité » est un compte partagé entre tous les utilisateurs qui l'utilisent. Aucune confidentialité des données n'est garantie sur ce compte.



Une fois connecté, ce compte s'utilise de la même manière que celle utilisée pour les comptes utilisateurs.

5. Kiosque / Poste Libre-Service

6.1 Démarrage

Le démarrage de la plateforme s'effectue de la même manière que n'importe quel ordinateur (portable ou non). Une distribution minimaliste est installée (issue de « Porteus Kiosk ») et permet un démarrage cloisonné sur un système chiffré en lecture seule.

Lors du démarrage, aucun accès au système n'est possible et seule l'interface WEB de CyberHawk s'affiche en plein écran. Le système est configuré pour n'accepter aucune connexion entrante et seulement des connexions sortantes vers l'IP / URL du serveur CyberHawk.

Le système étant en lecture seule et chiffré, aucune configuration post-installation n'est possible. Tout changement de configuration (IP, URL, paramètres système) doit se faire lors de la réinstallation du système.

6.2 Utilisation générale

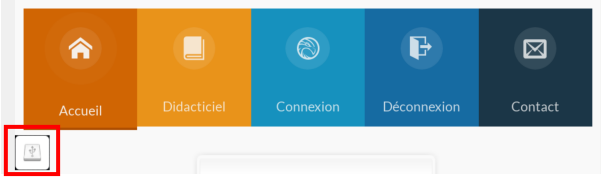
L'utilisation de CyberHawk en mode kiosque / poste libre-service reste la même que l'utilisation normale décrite précédemment (§3).

Seuls quelques points diffèrent lors de l'envoi d'un fichier et de son téléchargement. En effet, le système étant en lecture seule, seuls les envois / téléchargements depuis / vers un média amovible sont possibles. Avant toute action, il convient donc d'insérer un média amovible dans le kiosque / poste libre-service.

L'envoi d'un fichier se fait ensuite de la même manière que celle décrite précédemment (§3) en sélectionnant le(s) fichier(s) à envoyer depuis le média amovible.

La récupération de fichiers se fait de façon automatique, directement vers le média amovible s'il est inséré.

Le média amovible peut ensuite être retiré du système après avoir déconnecté celui-ci à l'aide du bouton prévu.



Il peut arriver que la déconnexion ne soit pas prise en compte lors de l'utilisation du bouton si la clé est encore en cours de lecture / écriture. Il suffit donc d'attendre quelques secondes avant de réessayer.

6.3 Problèmes & Résolutions

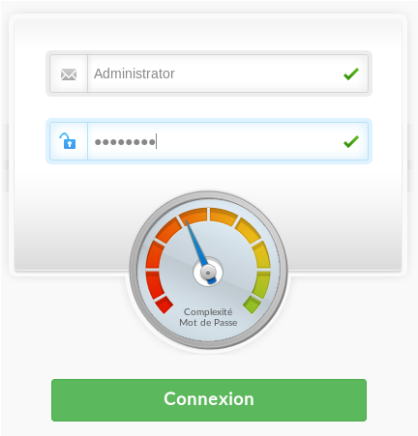
Dans le cas où L'IP / URL du serveur CyberHawk n'est pas accessible, le message de la capture suivante est affiché à l'utilisateur et le Kiosque ne démarre pas. Veuillez vérifier la connexion réseau ainsi que l'état de la plateforme CyberHawk avant de redémarrer le poste libre-service.

En cas de problème sur le kiosque / poste libre-service (blocage, ralentissements, etc.), il est uniquement nécessaire de le redémarrer.

6. Manuel Administrateur

7.1 Authentification

L'accès à l'interface d'administration ne se fait qu'à partir d'une authentification (avec mot de passe). Le processus est le même que pour une authentification utilisateur. Un compte 'Administrator' est créé lors de l'installation avec un mot de passe complexe défini.



L'administrateur dispose, en plus de fonctionnalités d'administration, d'un espace de partage similaire à celui des utilisateurs. Cependant, son espace est illimité et peut lui permettre d'envoyer manuellement les mises à jour des moteurs antiviraux.

7.2 Paramètres généraux

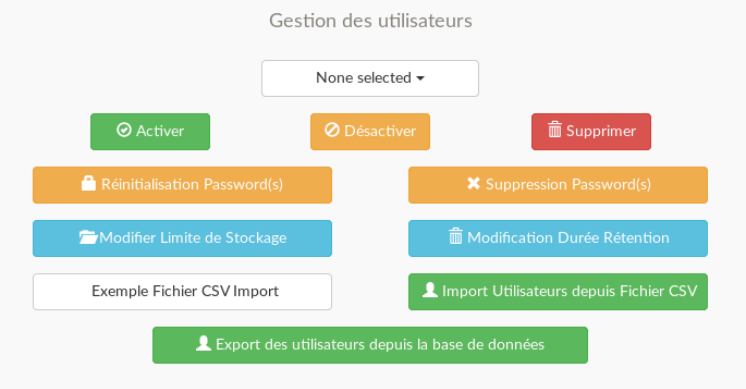
L'accès aux paramètres généraux de CyberHawk est disponible depuis l'interface administrateur uniquement, en cliquant sur le boutton « Settings ».

Ce paramétrage, revu dans la nouvelle version 2.1.0, permet de gérer les utilisateurs, mais également le paramétrage général de la plateforme (post-installation).

7.3 Gestion des utilisateurs

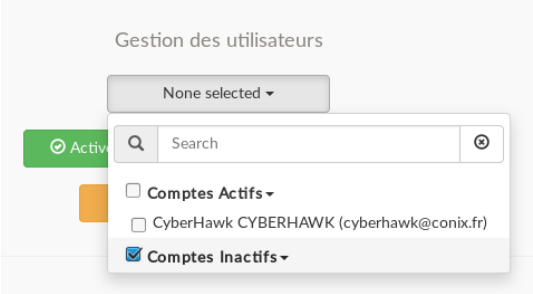
La gestion des utilisateurs reste relativement simple dans CyberHawk et permet les actions suivantes :

- Activation / Désactivation / Suppression de comptes utilisateurs
- Réinitialisation de mots de passe de comptes utilisateurs
- Suppression de mots de passe de comptes utilisateurs (passage en identification)
- Changement des limites de stockage de certains utilisateurs
- Changement de la durée de rétention de fichiers de certains utilisateurs
- Import d'utilisateurs depuis un fichier Excel (CSV) avec fichier d'exemple disponible
- Export des utilisateurs depuis la base de données



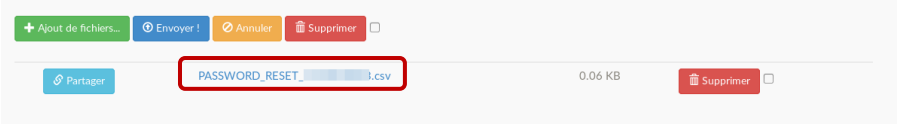
Les utilisateurs sont affichés dans un menu déroulant et divisés en deux groupes :

- Les comptes actifs
- Les comptes inactifs



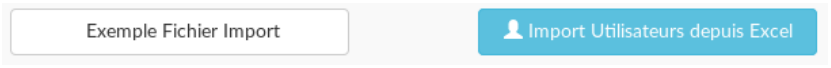
Quel que soit l'action à réaliser (sauf import), la première étape consiste à sélectionner les utilisateurs concernés puis à appliquer l'action. L'effet est immédiat pour certaines, avec confirmation pour d'autres.

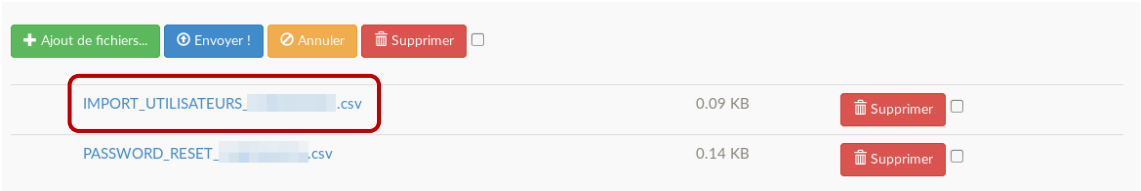
Lors de la réinitialisation des mots de passe utilisateurs, un fichier CSV est créé dans l'espace personnel de l'administrateur. Ce fichier contient la liste de tous les utilisateurs concernés ainsi que leur nouveau mot de passe de connexion.



	A	B	C	D	E
1	Nom	Prénom	Email	Password	
2	CyberHawk	CyberHawk	cyberhawk@conix.fr	b(IBphuOP5	
3	Dupont	Jacques	jacques.dupont@cyberhawk.fr	756RDrQ(1j	
4					

Enfin, l'import d'utilisateur(s) est possible depuis un fichier CSV. Le format de ce fichier CSV doit être respecté à la lettre (Nom ; Prénom ; Email) pour permettre une insertion correcte. Un exemple de fichier peut être téléchargé directement depuis l'application (Bouton « Exemple Fichier Import »). Une fois complété, ce fichier doit être uploadé dans l'interface administrateur (avec ses autres fichiers), puis il ne reste plus qu'à cliquer sur le bouton « Import Utilisateurs depuis Excel ». Lorsque l'import se termine, le fichier CSV est remplacé par un nouveau, contenant tous les utilisateurs importés et leurs mots de passe générés.





7.4 Exportation des logs

Les logs applicatifs sont disponibles au format Syslog et MySQL. Ils sont également consultables au format XML par l'administrateur via l'interface WEB CyberHawk. Il lui suffit d'utiliser le formulaire d'extraction prévu.

Lors de la génération du fichier de logs, un fichier XML est créé dans l'espace personnel de l'administrateur. Ce fichier contient l'ensemble des logs applicatifs (échecs de connexion, envois de fichiers, détections de virus, etc.).

7.5 Visualisation des statistiques

Pour l'instant, deux types de statistiques sont disponibles dans CyberHawk :

- Détections par module depuis installation CyberHawk
- Détections par module depuis 1 an

Ces statistiques évolueront dans le temps en fonction des besoins.

7.6 Paramétrage des modules

Ce nouvel onglet permet de paramétrer l'ensemble des modules après avoir réalisé l'installation. Il permet de réaliser les actions suivantes :

- Activation / Désactivation d'un module
- Ajout / Suppression d'éléments dans les Whitelist / Blacklist
- Modification du délai d'alertes (pour les mises-à-jour antivirales uniquement)
- Ajout de nouveaux modules (antivirus / scripts / etc.)

7.7 Paramétrage général

Ce nouvel onglet permet de paramétrer CyberHawk après avoir réalisé l'installation. Il permet de réaliser les actions suivantes :

- Changer le langage par défaut
- Activer / Désactiver les modules pour l'administrateur
- Activer / Désactiver le compte « Générique / Invité »
- Etc.

7.8 Paramétrage contact

Ce nouvel onglet permet de paramétrer la page « Contact » de CyberHawk après avoir réalisé l'installation.

7.9 Application manuelle des mises-à-jour

Bien que conseillée de façon automatique via un serveur relai de mises à jour (en interne), la mise à jour manuelle des moteurs antiviraux reste possible.

Elle ne peut se faire que depuis le compte administrateur en suivant les étapes suivantes :

1. Téléchargement manuel du package de mises à jour depuis le serveur miroir.
   Le serveur miroir met ce package à disposition pour chacun de nos clients CyberHawk.
   a. http://www.IP ou DNS/download.php?clientid=XXXXX-[...]-XXXXX
   b. Client ID (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX) : Numéro unique client, fourni lors de l'installation CyberHawk.
   c. Le fichier téléchargé est chiffré grâce à une clé unique dédiée pour chaque client. Il ne peut être déchiffré que par le serveur CyberHawk qui vérifiera son intégrité et la validité de son contenu.

2. Envoi du fichier téléchargé sur l'espace de partage du compte 'Administrator'.

3. Le fichier sera pris en compte automatiquement par CyberHawk lors de sa prochaine mise à jour, par défaut à minuit.

7. Compatibilités

L'application est compatible avec les navigateurs suivants :

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

Néanmoins, certaines fonctionnalités ne sont disponibles que sur certains navigateurs récents :

- Sélection et envoi multiple de fichiers
  - *Firefox 3.6+*
  - *Safari 5+*
  - *Google Chrome*
  - *Opera 11+*

- Glisser-Déposer (Drag & Drop)
  - *Firefox 4+*
  - *Safari 5+*
  - *Google Chrome*

- Progression du téléchargement (barre de progression)
  - *Firefox 4+*
  - *Safari 5+*
  - *Google Chrome*

- Prévisualisation des images
  - *Firefox 4+*
  - *Google Chrome*
  - *Opera 11+*