

Confix 2.4.2

Manuel, version 2.4.2 – 21 août 2020

1. Ouverture du programme

L'ouverture du programme peut être protégée par un mot de passe qui est défini dans le menu Outils / Options.

Première configuration

fff

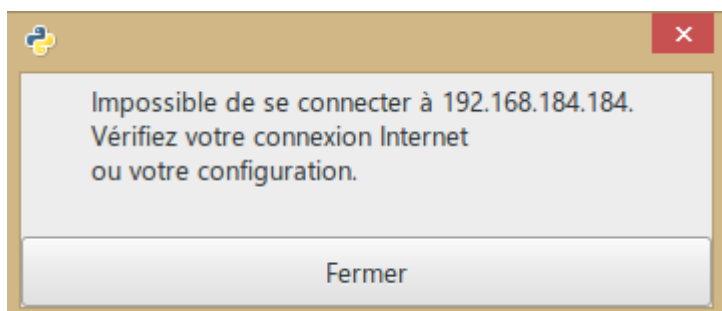
S'il n'a pas été préconfiguré, ou si la connexion automatique n'est pas activée, Confix s'ouvre avec une interface vide.

Choisir le menu *Connexion / Connecter...* pour sélectionner une connexion définie.

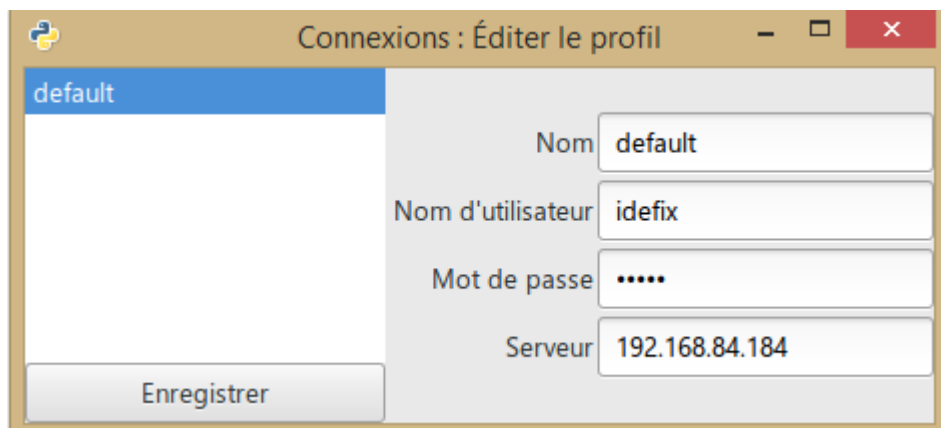
La première fois que le programme est utilisé, seule la connexion *default* est définie. Elle utilise les paramètres par défaut d'Idéfix :

- Nom d'utilisateur : idefix
- Mot de passe : admin
- Serveur : 192.168.84.184

Si la connexion échoue, la fenêtre suivante s'ouvre :

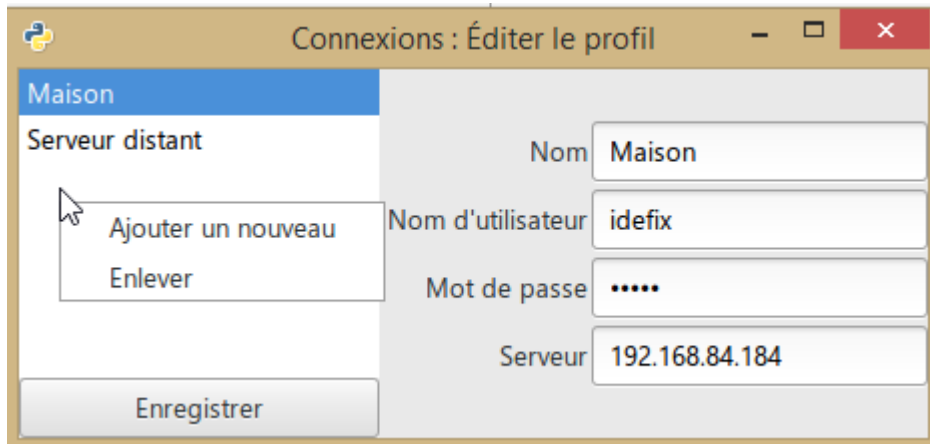


Il faut corriger le profil de connexion, on en crée un nouveau en utilisant le menu : *Connexions / profils de connexion...*



Mettre à jour le profil avec vos paramètres de connexion (information à demander au technicien qui supervise l'installation). Pour plus de détails, voir la section « profils de connexion », ci-dessous.

Un clic droit sur la liste de gauche permet d'ajouter ou d'effacer un profil :

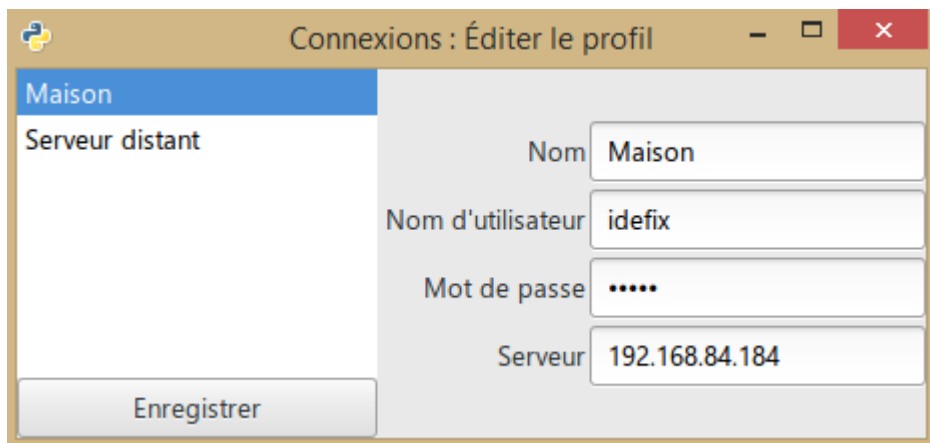


Enregistrer, fermer le programme et le rouvrir.

Profils de connexion

Confix peut se connecter sur différents profils. Ordinairement deux suffisent, l'un pour la connexion directe à idéfix, l'autre pour la connexion au serveur distant.

L'édition des profils se fait avec le menu Connexion / profils de connexion



Nom : uniquement informatif. Ce que vous voulez.

Les trois paramètres suivants sont ceux de la connexion ftp.

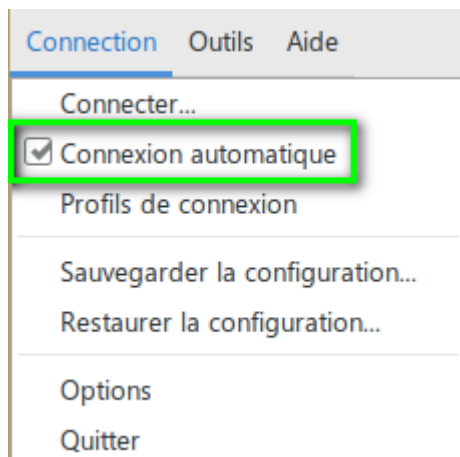
1. Pour une connexion directe à Idéfix :
 - a) **Nom d'utilisateur doit impérativement être idéfix**, sans majuscule et sans accent
 - b) Le mot de passe par défaut est admin. Ce mot de passe peut être modifié dans Supervix, le même mot de passe étant utilisé pour Supervix et pour la connexion à Idéfix
 - c) Serveur : l'adresse IP d'Idéfix (définie dans Supervix).

2. Pour la connexion à un serveur distant : les trois paramètres doivent être ceux du compte ftp, à demander au technicien. *Serveur* ne sera pas une adresse IP (numérique) mais une url comme par exemple : ftp.online.net

Il est possible de se connecter sur plusieurs comptes ftp, ce qui permet de paramétrer à distance les autorisations d'un module Idéfix.

Connexion automatique

Comme l'utilisateur standard n'utilise généralement qu'une seule connexion, la connexion directe à son module Idefix, Confix peut se connecter automatiquement au démarrage sur la dernière connexion utilisée. Il suffit de cocher la case correspondante dans le menu :



2. Configuration à distance

Le filtrage Internet est une technique qui peut être complexe. Les groupes représentent la première solution pour faciliter le filtrage. Mais l'aide d'une personne compétente peut s'avérer nécessaire de manière ponctuelle ou habituelle. Idéfix peut être administré entièrement à distance par une personne se trouvant n'importe où dans le monde. Le principe est le suivant.

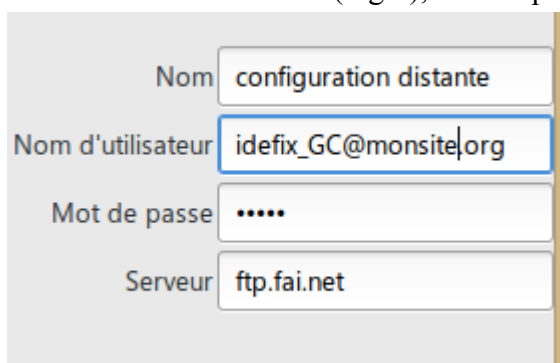
Un compte ftp dédié doit être défini quelque part. Confix et Idéfix doivent être paramétrés pour pouvoir accéder à ce compte. Tous les quart d'heures, Idéfix synchronise sa configuration, ce qui veut dire que si sa configuration est la plus récente, il l'envoie sur le site FTP, si celle du site FTP est plus récente, il met à jour sa propre configuration.

Pour le technicien à distance ou pour la personne qui utilise Confix sur le réseau local, il n'y a aucune différence dans le fonctionnement de Confix. La seule différence qui doit être notée est le délai. Lorsque l'ordinateur où tourne Confix est directement connecté à Idéfix, c'est-à-dire se trouve sur le réseau local, lorsqu'on clique sur enregistrer, il faut seulement quelques secondes pour que les changements soient pris en compte. Lorsque le technicien à distance fait la même chose, l'enregistrement sur le site FTP est immédiat, mais la mise à jour d'Idéfix ne se fera qu'au quart d'heure suivant (heure juste, 15, 30 ou 45).

Cela peut créer une difficulté si deux personnes travaillent en même temps. Celle qui est sur le réseau local aura en général la priorité et pourra éventuellement écraser les modifications que le technicien serait en train de faire en même temps qu'elle. Il serait sans doute possible d'ajouter un mécanisme qui bloquerait l'ouverture de la configuration si quelqu'un est déjà en train de travailler, mais ce n'est pas encore fait. \$\$

Configuration de Confix

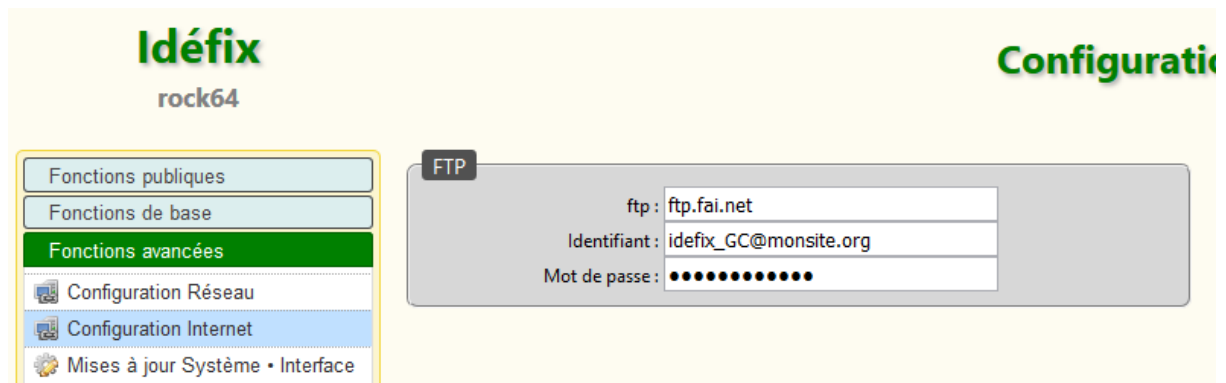
La configuration du site FTP sur Confix se fait dans les profils de connexion. Il faut créer un nouveau profil, lui donner un nom et mettre les trois paramètres classiques d'une connexion : nom d'utilisateur (login), mot de passe (password) et l'adresse du serveur.



The image shows a screenshot of a web-based configuration interface for Confix. It contains four input fields arranged vertically. The first field is labeled 'Nom' and contains the text 'configuration distante'. The second field is labeled 'Nom d'utilisateur' and contains the text 'idefix_GC@monsie|org'. The third field is labeled 'Mot de passe' and contains five dots. The fourth field is labeled 'Serveur' and contains the text 'ftp.fai.net'. The interface has a light gray background and a thin vertical orange bar on the right side.

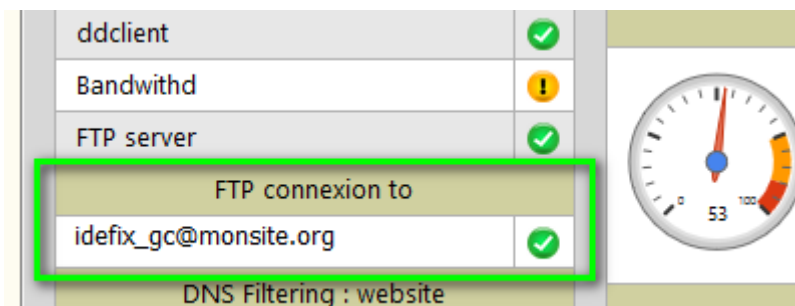
Configuration d'Idéfix

La configuration d'Idéfix se fait dans son interface (Supervix), dans les fonctions avancées (protégées par mot de passe), Configuration Internet.



Un message avertit que le changement de configuration ftp peut être dangereux (c'est-à-dire pourrait écraser une configuration existante). Pour un premier paramétrage, il n'y a pas de risque.

A partir de ce moment, dans l'état du système, la connexion ftp devrait être indiquée active :



3. Le filtrage par thème (DNS externe)

Le filtrage interne d'Idéfix fonctionne sur la base classique des listes blanches, et éventuellement noires, quoique ce soit moins utilisé, avec en plus les conditions temporelles. Cependant il y a bien des cas où une connexion ouverte est indispensable, par exemple pour des recherches sur Internet. Un filtrage par thème est souhaitable dans ce cas pour éviter des contenus indésirables comme par exemple la pornographie. Des entreprises spécialisées proposent ce type de service, comme par exemple SafeDNS. Ces services sont ordinairement payant, car il faut des employés pour maintenir à jour une base de données de plusieurs centaines de milliers de site. Un service gratuit existe aussi, OpenDNS. Ces sites permettent donc d'éliminer avec une réelle efficacité des catégories indésirables. Voir page suivante les catégories utilisées par SafeDNS. Les catégories cochées sont bloquées.

L'utilisation de ce type de filtrage au niveau d'un ordinateur personnel est peu efficace car il est très facile pour l'utilisateur de le désactiver, il suffit qu'il modifie ses paramètres réseau. Idéfix, lorsqu'il est paramétré pour cela, peut forcer toutes les connexions sortantes à passer par un tel filtre.

Ce filtre sera appliqué à tous les ordinateurs de la maison sans exception possible.

Le paramétrage de ce filtrage est une question assez complexe qui est renvoyée au manuel d'installation. Il y a cependant deux cas assez simples. Certains sites sont préconfigurés, actuellement SafeDNS et OpenDNS. Il suffit alors de les sélectionner dans les paramètres réseau.

The screenshot shows a web-based configuration interface for Idéfix. It features two main sections: 'Filtrage DNS' and 'IP dynamique ou fixe'. In the 'Filtrage DNS' section, there is a dropdown menu labeled 'Gestion par :' with 'SafeDNS' selected. The 'IP dynamique ou fixe' section contains two radio buttons for 'Adresse IP :', with 'dynamique' selected, and another dropdown menu labeled 'Gestion par :' with 'SafeDNS' selected. At the bottom of the interface is a green button with a checkmark icon and the text 'Enregistrer'.

Il existe également une option « automatique » qui exige que la connexion ftp soit configurée et qu'un technicien ait préparé la configuration sur le site ftp.

☒ Security

- | | |
|---|--|
| <input checked="" type="checkbox"/> Botnets | <input checked="" type="checkbox"/> Phishing |
| <input checked="" type="checkbox"/> Virus Propagation | |

☐ Illegal Activity

- | | |
|--|---|
| <input checked="" type="checkbox"/> Academic Fraud | <input checked="" type="checkbox"/> Child Sexual Abuse (Arachnid) |
| <input checked="" type="checkbox"/> Child Sexual Abuse (IWF) | <input type="checkbox"/> Crypto Mining |
| <input checked="" type="checkbox"/> Drugs | <input checked="" type="checkbox"/> German Youth Protection |
| <input checked="" type="checkbox"/> Hate & Discrimination | <input type="checkbox"/> Parked Domains |
| <input type="checkbox"/> Proxies & Anonymizers | <input checked="" type="checkbox"/> Tasteless |

☒ Adult Related

- | | |
|---|---|
| <input checked="" type="checkbox"/> Adult Sites | <input checked="" type="checkbox"/> Alcohol & Tobacco |
| <input checked="" type="checkbox"/> Astrology | <input checked="" type="checkbox"/> Dating |
| <input checked="" type="checkbox"/> Gambling | <input checked="" type="checkbox"/> Pornography & Sexuality |

☐ Bandwidth Hogs

- | | |
|---|--|
| <input type="checkbox"/> File Storage | <input checked="" type="checkbox"/> Movies & Video |
| <input checked="" type="checkbox"/> Music & Radio | <input type="checkbox"/> Photo Sharing |
| <input type="checkbox"/> Torrents & P2P | |

☐ Time Wasters

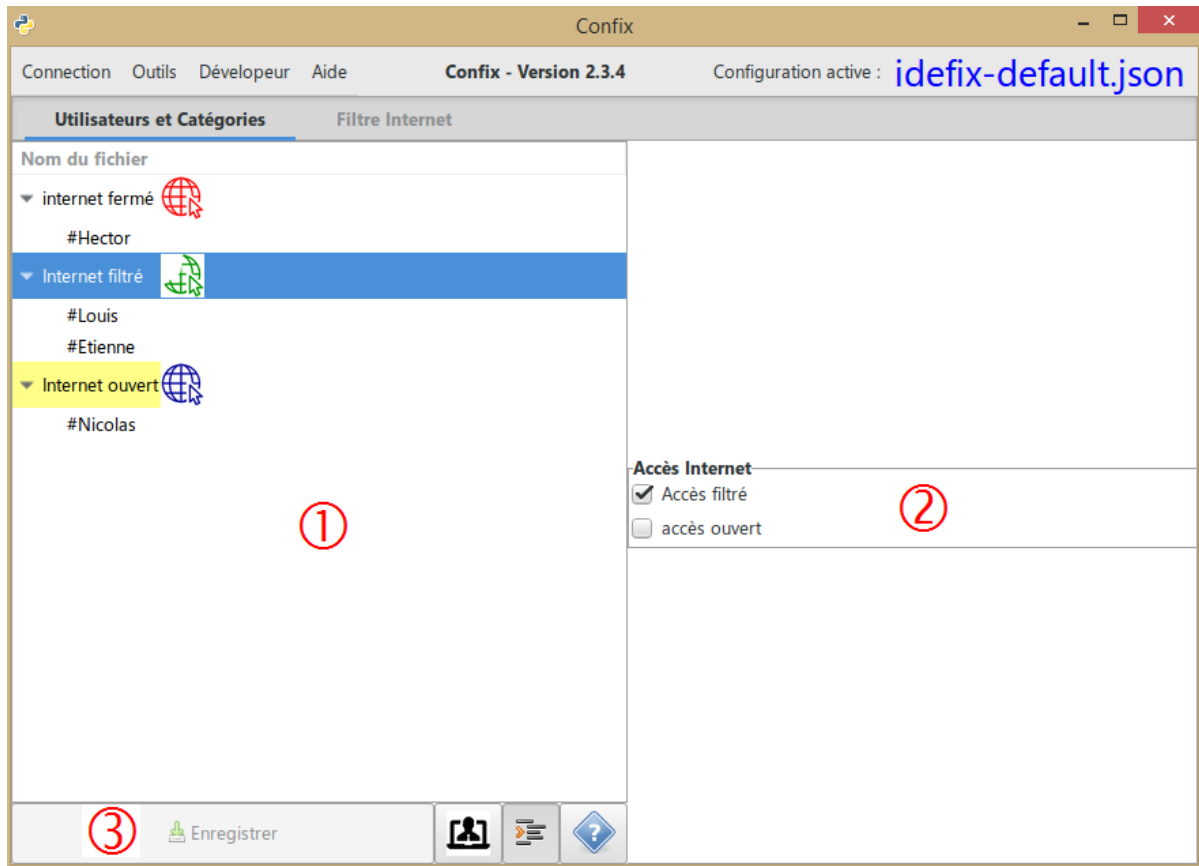
- | | |
|--|---|
| <input type="checkbox"/> Chats & Messengers | <input type="checkbox"/> Entertainment |
| <input type="checkbox"/> Forums | <input checked="" type="checkbox"/> Games |
| <input checked="" type="checkbox"/> Online Ads | <input checked="" type="checkbox"/> Social Networks |

☐ General Sites

- | | |
|---|--|
| <input type="checkbox"/> Arts | <input type="checkbox"/> Automotive |
| <input type="checkbox"/> Blogs | <input type="checkbox"/> Business |
| <input type="checkbox"/> Classifieds | <input type="checkbox"/> Computers & Internet |
| <input type="checkbox"/> Corporate Sites | <input type="checkbox"/> E-commerce |
| <input type="checkbox"/> Education | <input type="checkbox"/> Finances |
| <input type="checkbox"/> Government | <input type="checkbox"/> Health & Fitness |
| <input type="checkbox"/> Home & Family | <input type="checkbox"/> Humor |
| <input type="checkbox"/> Jobs & Career | <input type="checkbox"/> Kids |
| <input type="checkbox"/> News & Media | <input type="checkbox"/> Non-profit |
| <input type="checkbox"/> Online Libraries | <input type="checkbox"/> Politics, Society and Law |
| <input type="checkbox"/> Portals | <input type="checkbox"/> Real Estate |
| <input type="checkbox"/> Religious | <input type="checkbox"/> Science & Technology |
| <input type="checkbox"/> Search Engines | <input type="checkbox"/> Shopping |
| <input type="checkbox"/> Sports | <input type="checkbox"/> Trackers & Analytics |
| <input type="checkbox"/> Travel | <input type="checkbox"/> Weapons |
| <input type="checkbox"/> Webmail | |

4. Premier onglet : Utilisateurs et catégories

Une fois ouverte, l'interface présente un menu et trois onglets (les images ci-dessous n'en présentent généralement que deux, le troisième onglet étant apparu plus tard (V. 2.3.6).



Le premier onglet permet de donner les autorisations globales.

① La liste de gauche permet de définir un certain nombre de catégories, à l'intérieur desquels viendront se placer les utilisateurs.

Lorsqu'une catégorie est sélectionnée à gauche

Trois situations peuvent être définies pour elle :

- Aucun accès à Internet ou au courrier électronique
- Accès à un nombre de sites limités (accès filtré)
- Accès à tout Internet.

Ces autorisations peuvent être activées ou désactivées par les cases à cocher qui se trouvent à droite. ②

– Les images à la droite du nom des catégories permettent de voir d'un seul coup d'œil quelles sont les autorisations globales données à chaque catégorie :



Aucun accès



Accès filtré

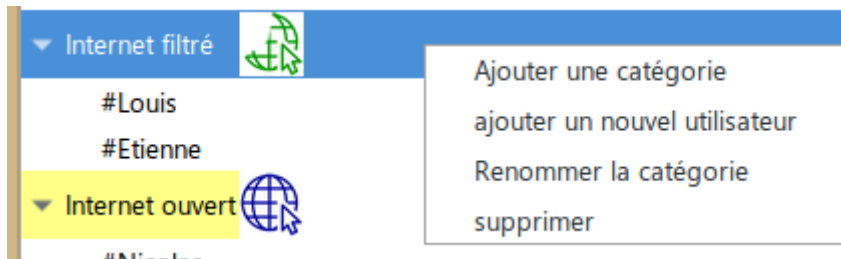


Accès ouvert

Ces images ne sont pas actives mais uniquement informatives.

– Pour rendre bien visible les catégories qui ont un accès Internet ouvert, elles sont surlignées en jaune.

– Un clic droit sur une catégorie donne accès à un menu contextuel :



– La liste des catégories peut être réorganisée avec la souris. [il y a un bug, ça ne marche pas bien]

③ La barre de boutons donne accès aux commandes :

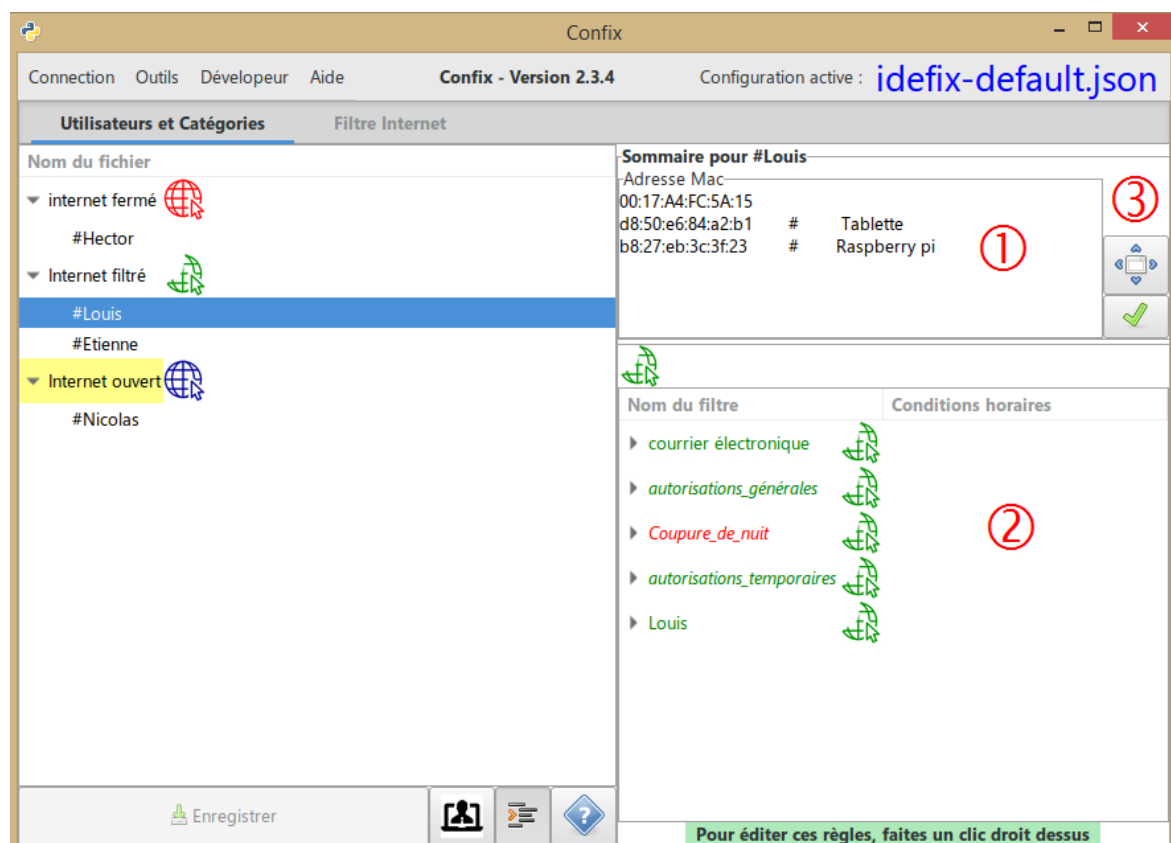
- Enregistrer : Enregistre la configuration dans Idéfix ou sur le site FTP auquel on est connecté.
- Développer / réduire l'arborescence

Enregistrement

Lors de l'enregistrement, si on est connecté sur un serveur distant, la configuration sera activée sur le module Idefix au quart d'heure suivant. Si on est connecté directement sur Idefix, elle est active immédiatement.

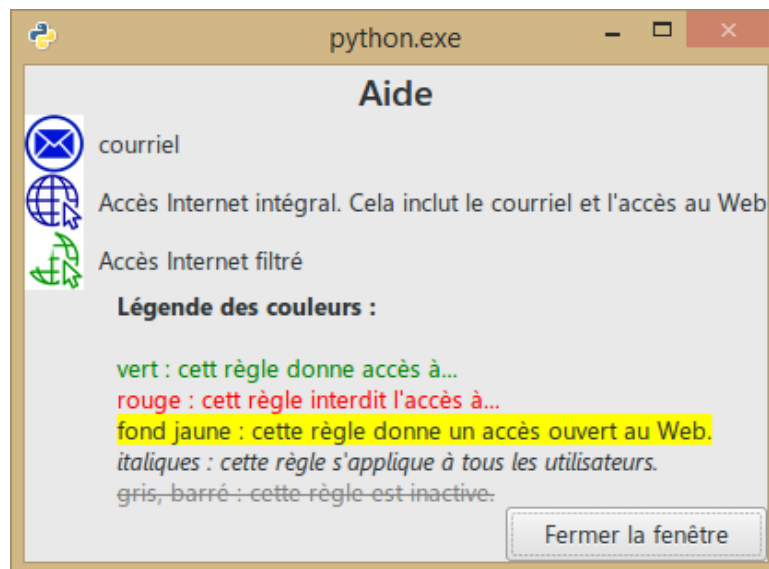
Lorsqu'un utilisateur est sélectionné à gauche

L'affichage de droite change pour montrer les données de cet utilisateur.



- 1) Tout appareil connecté sur un réseau possède une ou plusieurs adresses qui permettent de l'identifier sur le réseau. Un utilisateur ayant plusieurs appareils pourra avoir plusieurs adresses. Elles doivent être enregistrées ici pour que l'utilisateur puisse avoir accès à Internet. On peut insérer un commentaire après un #
Il est possible d'entrer des adresses Mac (cas le plus général) ou des adresses IP.
- 2) Le cadre en bas à droite donne les règles de filtrage auxquelles est soumis un utilisateur. On peut éditer ces règles en faisant un clic droit dessus. [Ce tableau n'est pas tout à fait au point, car il n'indique pas l'accès ouvert].
La typographie a une signification :
 - Vert = autorisation
 - Rouge = interdiction
 - Italique = il s'agit d'une règle générale qui s'applique à tout le monde. C'est pourquoi, dans l'exemple ci-dessus, Louis n'est mentionné explicitement que dans la règle qui le concerne (la dernière), mais les trois premières s'appliquent à lui aussi.
 - S'il y a des conditions horaires définies, elles sont indiquées à droite.

Pour rappeler la signification des couleurs, cliquer sur le bouton d'aide.



3) Les boutons à droite permettent de :

- Agrandir la taille du cadre du haut, pour travailler plus confortablement s'il y a plusieurs adresses. Cliquer de nouveau pour ramener à la taille initiale.
- Vérifier si la syntaxe des adresses est valide. L'existence réelle sur le réseau de ces adresses n'est pas vérifiée, seulement leur validité.

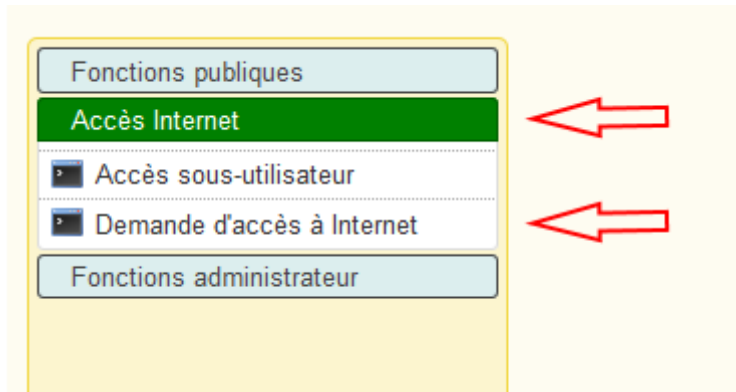
Le détail des permissions sera défini dans le deuxième onglet, Filtre Internet, dont il va être question maintenant.

Créer un nouvel utilisateur

Bien qu'il soit possible de créer un nouvel utilisateur en utilisant les commandes ci-dessus, la solution la plus simple consiste à utiliser l'Assistant (menu Outils / Assistant) qui vous guidera pas à pas. Il existe deux procédures.

Avec demande d'accès faite par l'utilisateur

La plus simple consiste à demander au nouvel utilisateur de se connecter à partir de son ordinateur personnel sur Supervix (en version 2.5.0 ou plus), et de prendre le menu *Accès Internet / Demande d'accès à Internet*



Cette option du menu donne accès à un écran simple :

A screenshot of a web form. At the top, it says 'Entrez un nom pour votre demande d'accès à Idéfix'. Below this is a text input field. At the bottom, there is a button labeled 'Envoyer la demande'.

L'utilisateur doit entrer un nom qui est uniquement destiné à le reconnaître, comme on le verra plus bas. Ce nom ne sera pas utilisé par la suite. Supposons qu'il ait entré :

A screenshot of the same web form as before. The text input field now contains the name 'Pierre Martin'. The button 'Envoyer la demande' is still there. Below the button, the text 'Demande envoyée' is displayed in red.

Pour lui, c'est tout ce qu'il a à faire. Mais maintenant une demande d'accès à Internet au nom de Pierre Martin est enregistrée dans Idéfix. Quand l'administrateur va ouvrir l'assistant, il verra la liste des demandes, parmi lesquelles celle de Pierre Martin :

Cet assistant vous aidera à créer un nouvel utilisateur :

☒ Choisissez une demande d'accès dans la liste

Ask your user visit: http://192.168.1.184/request_account_json.php
then refresh this list to automatically add them.

Rafraîchir la liste

| Nom d'utilisateur | Adresse Mac |
|-------------------|-------------------|
| aplusbegalix | 60:a4:4c:7b:1d:5a |
| Pierre Martin | 50:68:2c:0b:ad:aa |

Il lui suffit de sélectionner la ligne, de cliquer sur le bouton « suivant » et de se laisser guider par l'assistant. Il n'aura donc pas besoin de chercher l'adresse mac de l'ordinateur.

Il faut noter toutefois que si l'ordinateur de Pierre Martin a plusieurs accès au réseau, par exemple par câble et par WiFi, s'il veut utiliser les deux, il devra faire deux fois l'opération, de demande d'accès, une quand il est connecté par câble (avec le WiFi arrêté) et l'autre quand il est connecté en WiFi (avec le câble débranché). Il devra prendre deux noms différents, par exemple « Pierre Martin WiFi » pour le deuxième.

Méthode manuelle

L'autre méthode consiste à entrer les données manuellement.

Deux conditions à remplir avant de l'utiliser :

1. Connaître la ou les adresses MAC de l'utilisateur
2. Avoir une idée précise des autorisations que vous voulez lui donner.

Accédez à l'assistant par le menu « Outils », ou par le bouton en bas de l'écran, dans le premier onglet.

Choisissez l'option *créez un nouveau nom d'utilisateur*.

Cet assistant vous aidera à créer un nouvel utilisateur :

☐ Choisissez une demande d'accès dans la liste

Ask your user visit: http://192.168.1.184/request_account_json.php
then refresh this list to automatically add them.

Rafraîchir la liste

| Nom d'utilisateur | Adresse Mac |
|-------------------|-------------------|
| aplusbegalix | 60:a4:4c:7b:1d:5a |
| Pierre Martin | 50:68:2c:0b:ad:aa |

☒ Ou créez un nouveau nom d'utilisateur

Jean Gabin

Choisissez une option,
sélectionnez une ligne ou tapez un nom,
et cliquez sur "suivant"

Cliquez sur suivant.

Précédent

Annuler

Nouvel Utilisateur

Suivant

Introduction

Nouvel Utilisateur

Accès Internet filtré

Confirmation

Nom du nouvel utilisateur

Entrez le nom du nouvel utilisateur :

Zoé

Maintenant vous devez ajouter son adresse Mac.
Si vous ne la connaissez pas, il sera possible de l'ajouter plus tard dans l'onglet "Utilisateurs et Catégories".

00 : 4b : 65 : f9 : 12 : 88

Ajouter une autre adresse

Cliquez sur le bouton pour valider vos données, puis cliquez sur "suivant"

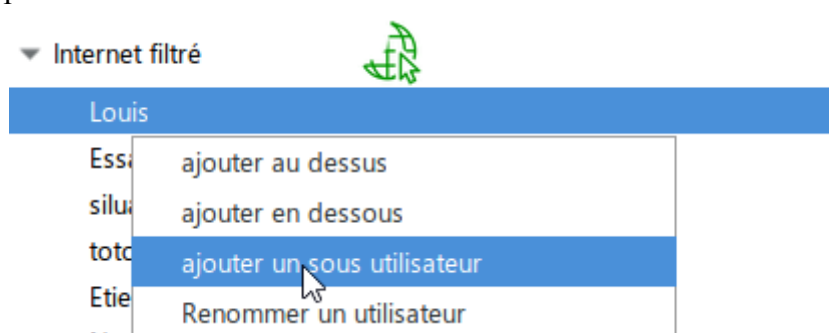
Entrez la ou les adresses Mac, cliquez sur suivant et laissez-vous guider.

5. Les sous-utilisateurs

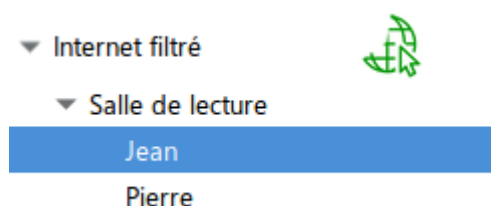
Idéfix peut gérer des permissions différentes pour plusieurs utilisateurs sur un même ordinateur. Il faut pour cela créer un compte normal pour l'ordinateur en question, et lui donner les autorisations qu'il aura de manière habituelle. Les sous-utilisateurs hériteront de ces autorisations.

Créer un sous-utilisateur

Il faut ensuite créer un ou plusieurs sous-utilisateurs, ce qui se fait par un clic droit sur le compte de l'ordinateur :

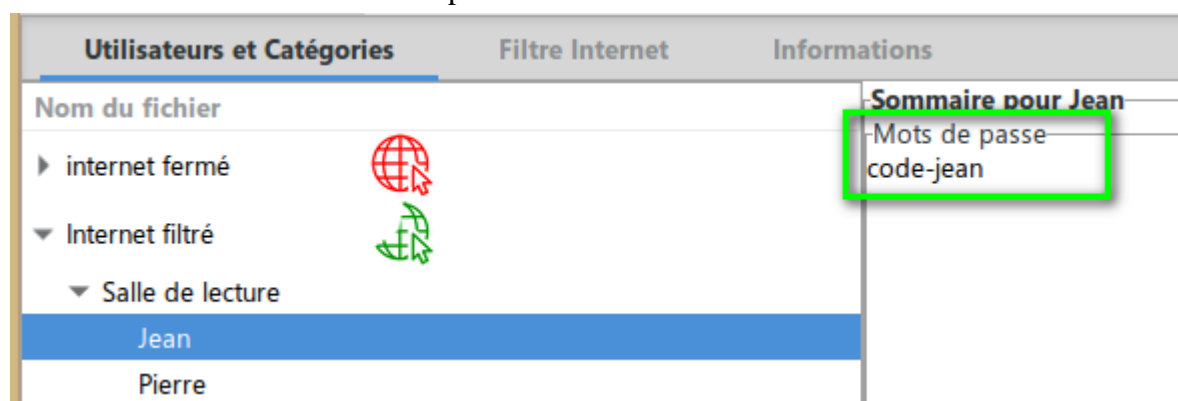


Ce qui pourrait donner :



Dans cet exemple, l'ordinateur *Salle de lecture* a deux sous-utilisateurs.

Un sous-utilisateur est identifié par un code d'accès qui lui est personnel et qui est entré dans le cadre utilisé normalement pour les adresses mac¹.



Les permissions d'un sous-utilisateurs sont définies exactement de la même manière qu'un utilisateur ordinaire.

¹ Sur l'image, le terme utilisé est « Mot de passe ». C'est la même chose. Nous essayerons d'harmoniser la terminologie.

Activer les permissions d'un sous-utilisateur

Pour que Jean ou Pierre puissent activer leurs permissions sur l'ordinateur défini, ils doivent entrer une adresse :

<adresse IP d'Idéfix>/subuser.php. Par exemple :

192.168.84.184/subuser.php

Il est recommandé de faire un raccourci pour cette adresse sur l'ordinateur.

Une page s'ouvre qui leur permet d'entrer leur code d'accès :

Entrez votre code pour accéder au Web :



Après avoir cliqué sur « Connecter », les roues se mettent à tourner. Les permissions sont activées et le resteront aussi longtemps que les roues tourneront.

Pour fermer les autorisations, il suffit de cliquer sur le même bouton qui porte alors le texte « Déconnecter ». Les roues s'arrêtent et les permissions sont suspendues.

Si l'utilisateur oublie de déconnecter et ferme simplement la page ou le navigateur, les permissions continueront à être actives jusqu'au quart d'heure suivant.

Il faut bien expliquer au sous-utilisateur qu'il doit laisser cette page ouverte tout le temps qu'il travaille, et donc qu'il doit ouvrir un autre onglet pour son travail.

Sessions Windows

Si l'ordinateur partagé tourne sous Windows, et que chaque sous-utilisateur a une session personnelle, il est possible de lier les permissions à la session, ce qui dispense le sous-utilisateur d'avoir à entrer son code. La procédure est la suivante :

Un service spécial doit être installé sur l'ordinateur. Ce service informera Idéfix toutes les minutes de la session actuellement ouverte et ainsi Idéfix pourra appliquer les permissions correspondantes. Pour que ceci fonctionne, il est nécessaire que le code d'accès qui est entré dans la configuration du sous-utilisateur soit le nom de sa session Windows, écrit exactement avec majuscules et minuscules. Il s'agit bien du nom de la session et non du mot de passe, car l'API Windows est incapable de récupérer le mot de passe d'une session.

Salle de lecture

Dans le cas d'une salle de lecture où plusieurs ordinateurs seraient mis à disposition, si les permissions sont les mêmes quel que soit l'ordinateur utilisé, il n'est pas utile de créer un

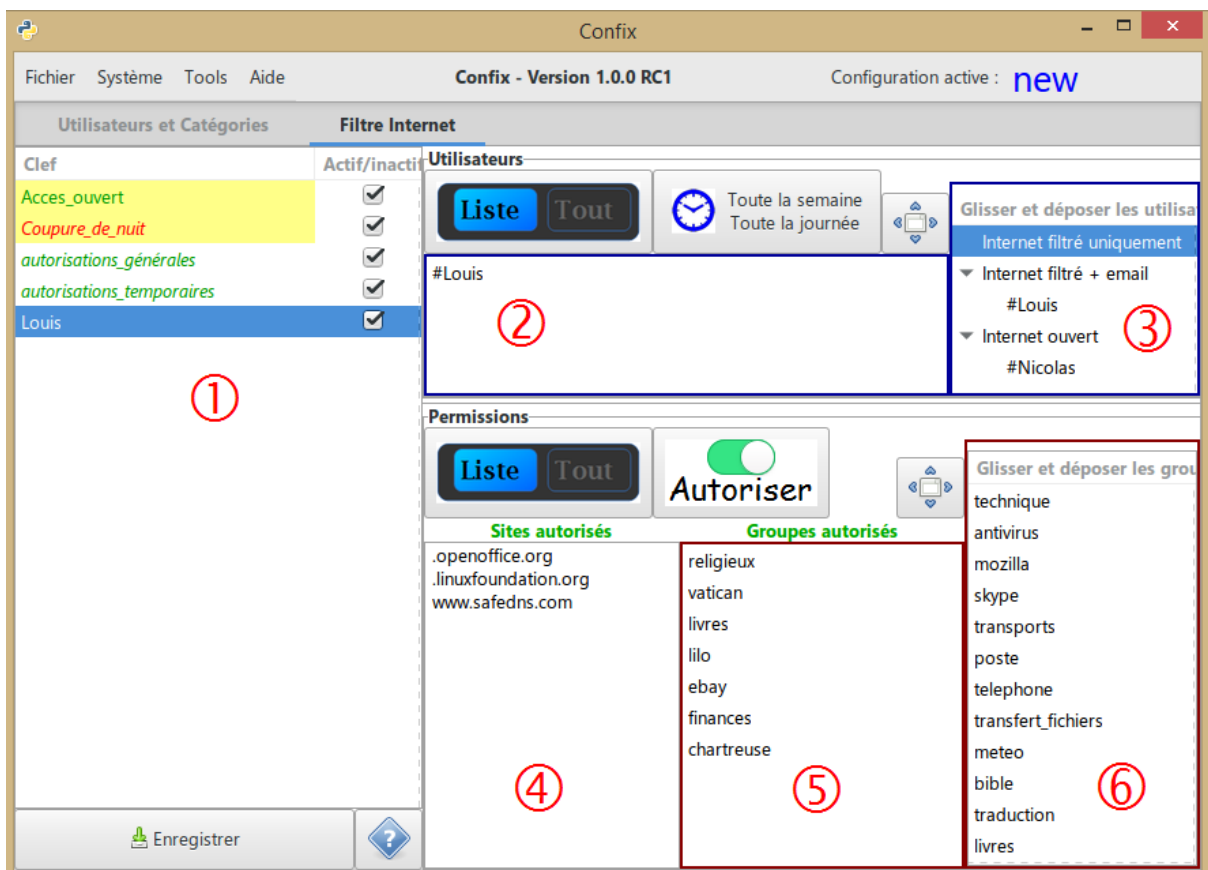
compte par ordinateur, il suffit de mettre dans le compte *Salle de lecture* (par exemple) les adresses Mac de tous les ordinateurs de la salle.

6. Deuxième onglet : Le filtre Internet

Le filtre Internet permet de définir des règles d'accès des utilisateurs.
L'interface est composée de six listes et cinq commandes.

Les listes

- À gauche, la liste des règles
- Au centre, les listes 2, 4 et 5 définissent le contenu des règles, c'est-à-dire :
 - Qui (liste 2)
 - peut accéder à quels sites web (liste 4)
 - ou à quels groupes de sites web (liste 5).
- À droite deux listes d'aide (3 et 6) qui permettent de glisser-déposer les utilisateurs ou les groupes, ce qui évite les erreurs de frappe. [Bug à corriger : attention à faire glisser des utilisateurs et non des noms de catégories].



Pour effacer un utilisateur de la liste utiliser le menu clic droit.

Dans la liste **Sites autorisés**, on peut entrer les sites auxquels on veut donner accès et qui n'appartiennent pas déjà à un groupe.

Pour définir tous les sous domaines d'une adresse, commencer par un point :

- **chapitre.com** : donnerait accès uniquement à cette adresse, mais pas à *images.chapitre.com*, *livres.chapitre.com* etc. et le site ne marchera que partiellement ou pas du tout.

- ***.chapitre.com** donne accès à tout ce qui se termine ainsi. La règle générale est donc d'avoir un point au commencement. [une prochaine version rappellera cela à l'utilisateur qui entrerait une adresse sans *. (étoile suivi d'un point) au début].

Liste des groupes

Pour plus de commodité, des groupes de sites sont définis. L'utilisateur peut en ajouter, les supprimer ou les modifier.

Pour ajouter des groupes dans la liste 5, il faut les faire glisser depuis la liste 6.

Pour effacer un groupe ou pour le modifier, utiliser le menu contextuel ouvert par un clic droit.

Cependant, pour modifier des groupes, il sera préférable d'utiliser le gestionnaire de groupes (dans le menu Outils).

En maintenant la souris sur un groupe son contenu s'affiche.



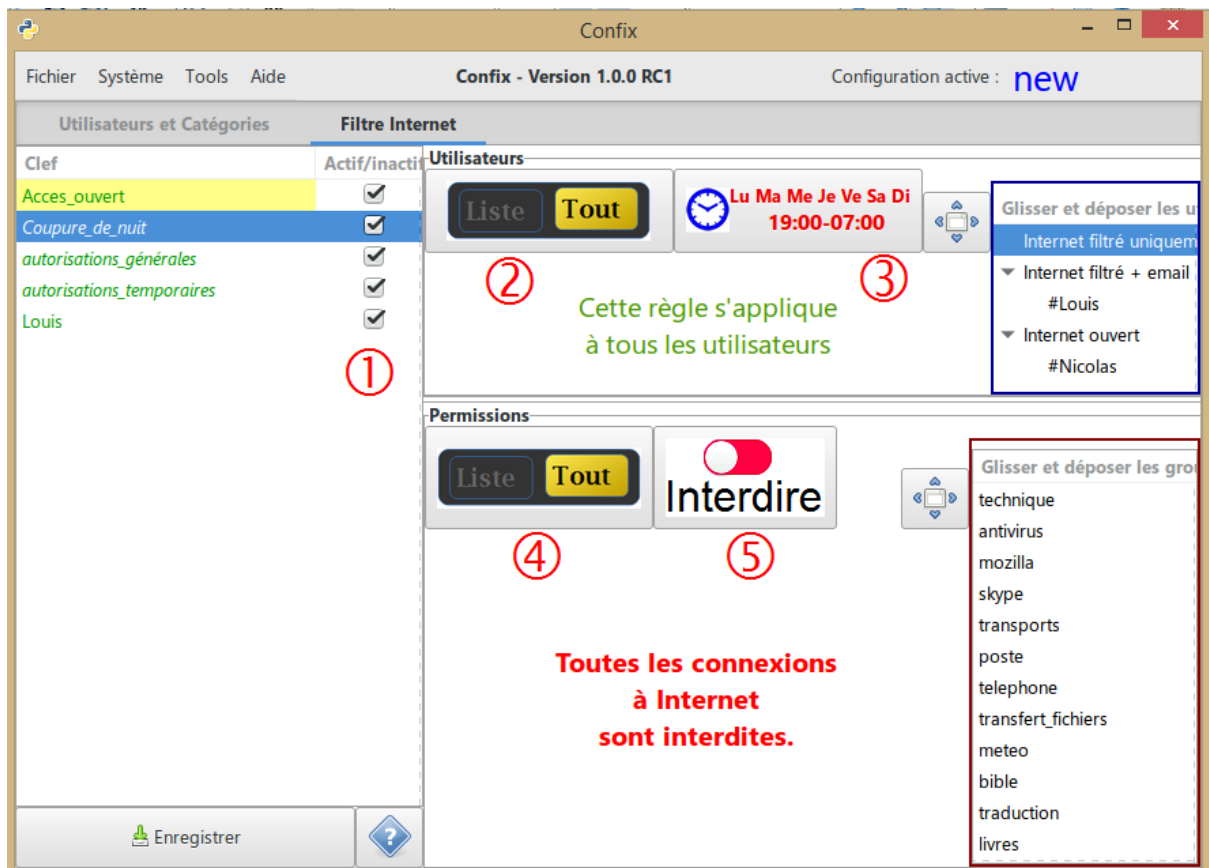
Les commandes

Dans l'image ci-dessous, les boutons de commande du centre sont dans un état différent de l'image précédente, ce qui permet de montrer leurs états :

Liste ou Tout

Autoriser ou Interdire

Toute la semaine et toute la journée, ou jours et horaires définis.



- 1) Les cases à cocher permettent d'activer ou désactiver une règle.
- 2) Le bouton Liste/Tout permet de définir si une règle s'applique à un utilisateur ou à tous, **ATTENTION : si vous mettez le bouton de la liste d'utilisateurs ET le bouton des permissions sur « Tout » (les deux boutons en fond jaune), vous ouvrez tout Internet à tout le monde. Cette possibilité sera interdite dans une prochaine version.**
- 3) Ce bouton permet de définir les conditions temporelles, jours et heures où la règle est active.
- 4) Le bouton Liste/Tout permet de définir si une règle concerne une liste de sites web ou tout accès Internet.
- 5) Bouton qui définit si on autorise ou interdit les sites ou groupes choisis.

Ainsi, dans le premier exemple, la règle *Louis* définit que :

#Louis (dans la liste 1) a accès aux sites web (liste 4) :

.openoffice.org
 .linuxfoundation.org
 www.safedns.com

Et aux groupes de sites (liste 5) :

Religieux
 Vatican
 Livres
 Lilo
 Ebay
 Finances
 Chartreuse

Cette règle est active car la case (commande 1) est cochée.

Dans le deuxième exemple la règle *Coupure de nuit* définit que :

Tout le monde (2) est interdit d'accès (5) pour tous les sites Internet (4), tous les jours de 19h00 à 7h00 (3)

Il faut noter que le filtre est conçu de telle façon que tout ce qui n'est pas explicitement autorisé est bloqué.

L'ordre des règles

L'ordre des règles est important car il peut avoir une influence sur l'autorisation ou non d'un site. Quand un ordinateur demande une connexion, le filtre examine les règles une par une, du haut en bas. Si une règle remplit toutes les conditions (utilisateur, destination et temps), cette règle est appliquée, et le filtre n'examine pas les règles qui suivent.

Dans une configuration où il n'y aurait que des règles qui autorisent, l'ordre n'aurait pas d'importance. Mais si une ou plusieurs règles interdisent, leur position est significative. Dans la configuration prise en exemple, la première règle autorise tout pour les utilisateurs définis pour elle, la suivante, la coupure de nuit, interdit tout pour tout le monde dans un créneau horaire défini.

| Clef | Actif/inactif |
|---------------------------|-------------------------------------|
| Acces_ouvert | <input checked="" type="checkbox"/> |
| Coupure_de_nuit | <input checked="" type="checkbox"/> |
| autorisations_générales | <input checked="" type="checkbox"/> |
| autorisations_temporaires | <input checked="" type="checkbox"/> |
| Louis | <input checked="" type="checkbox"/> |

Le résultat est que les utilisateurs définis pour la règle *Acces_ouvert* auront accès à Internet même la nuit. En effet, puisque la première règle autorise toutes leurs demandes à passer, le filtre ne va pas plus loin et la coupure de nuit n'est pas examinée.

Si maintenant on passait la coupure de nuit en première place, elle aurait alors la précedence sur *Acces_ouvert* et les utilisateurs définis dans cette règle n'auraient pas d'accès la nuit.

Cette fonctionnalité permet de distinguer le cas des familles qui pourraient avoir un accès Internet par la connexion du monastère, et auxquelles on voudrait donner un accès sans limite. Elles seraient mises dans une règle au-dessus de la coupure de nuit.

Il existe pourtant une dernière règle implicite qui interdit tout ce qui n'a pas été autorisé avant elle.

Conditions horaires

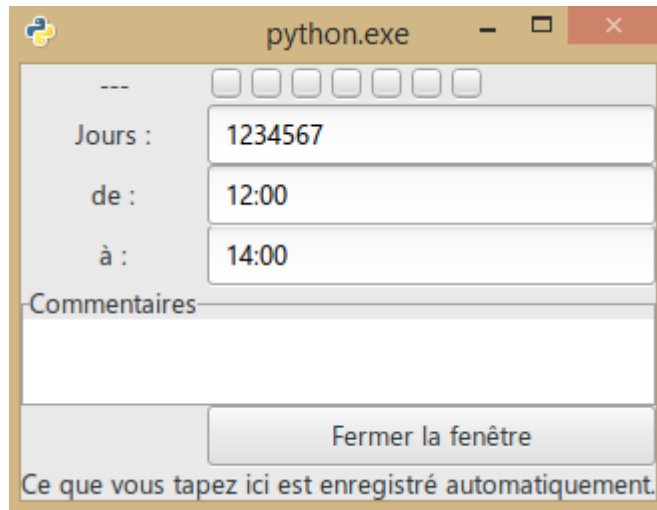
Utilisateurs

Liste

Tout

 Toute la semaine
Toute la journée

En cliquant sur le bouton avec l'horloge, on accède aux conditions horaires qui permettent de limiter la plage de temps pendant laquelle la règle est active.



python.exe

Jours : 1234567

de : 12:00

à : 14:00

Commentaires

Fermer la fenêtre

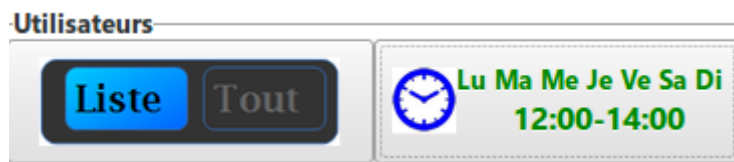
Ce que vous tapez ici est enregistré automatiquement.

\$\$ La programmation de cette fenêtre n'est pas terminée : les cases à cocher en haut ne sont pas utilisées, les commentaires ne sont pas enregistrés, la syntaxe n'est pas vérifiée.

Il faut entrer les heures avec : comme séparateur

Les jours sont représentés par les chiffres, en commençant par le lundi.

Une fois les données entrées, on peut fermer la fenêtre, la prise en compte des modifications est automatique, comme en témoigne le changement du bouton :



Utilisateurs

Liste Tout

Lu Ma Me Je Ve Sa Di
12:00-14:00

Pour des conditions horaires complexes, il suffira de créer plusieurs règles pour le même utilisateur, et de combiner intelligemment ce qui autorise et ce qui interdit, selon ce qui a été dit plus haut sur l'ordre des règles.

7. Le troisième onglet : Informations

£££

Disponible depuis la version 2.3.5, cet onglet donne des informations qui peuvent donner une aide pour la rédaction des règles et le configuration des utilisateurs. Cela a déjà été vu plus haut à propos des adresses Mac. Il en sera question plus bas à propos de la découverte des sites à autoriser.

| Utilisateurs et Catégories | | Filter Internet | Informations |
|----------------------------|--|-----------------|--------------|
| Log Unbound | commande | | |
| Log Squid | Dec 03 10:52:30 : allowed ==> emupdate.avcdn.net. / 192.168.1.200 - allowed by autorisa | | |
| Connected Users | Dec 03 10:52:30 : allowed ==> analytics.ff.avast.com. / 192.168.1.200 - allowed by auto | | |
| Versions | Dec 03 10:53:13 : allowed ==> ncc.avast.com. / 192.168.1.200 - allowed by autorisations | | |
| Diagnostic | Dec 03 10:54:38 : validation failure <lem.nouvelobs.com. A IN>: no DNSSEC records from 1 | | |
| Search | Dec 03 10:54:58 : validation failure <cdn.permutive.com. A IN>: no DNSSEC records from 1 | | |
| | Dec 03 10:55:51 : allowed ==> config.edge.skype.com. / 192.168.1.200 - allowed by D.Dys | | |
| Mac Address | Dec 03 10:56:13 : validation failure <cdf-anon.xboxlive.com. A IN>: no DNSSEC records fr | | |
| | Dec 03 10:56:17 : validation failure <activate.api.stardock.net. A IN>: no DNSSEC record | | |
| Domain | Dec 03 10:57:25 : denied ==> users.freemake.com. / 192.168.1.200 - no match | | |
| | Dec 03 10:57:40 : allowed ==> uib.ff.avast.com. / 192.168.1.200 - allowed by autorisati | | |
| Start Search | Dec 03 10:57:40 : allowed ==> ns1.ff.avast.com. / 192.168.1.200 - allowed by autorisations de nuit | | |
| | Dec 03 10:57:47 : allowed ==> fonts.googleapis.com. / 192.168.1.200 - allowed by autori | | |
| Technical data | Dec 03 10:57:47 : allowed ==> adservice.google.fr. / 192.168.1.200 - allowed by D.Dysma | | |
| | Dec 03 10:57:47 : denied ==> pagead46.l.doubleclick.net. / 192.168.1.200 - no match | | |
| Apache log | Dec 03 10:57:47 : denied ==> pagead46.l.doubleclick.net. / 192.168.1.200 - no match | | |
| | Dec 03 10:57:47 : allowed ==> fonts.googleapis.com. / 192.168.1.200 - allowed by autori | | |
| Show | Dec 03 10:57:48 : allowed ==> ssl.gstatic.com. / 192.168.1.200 - allowed by autorisatio | | |
| | Dec 03 10:57:48 : denied ==> lh3.googleusercontent.com. / 192.168.1.200 - no match | | |
| | Dec 03 10:57:48 : denied ==> lh3.googleusercontent.com. / 192.168.1.200 - no match | | |
| | Dec 03 10:57:48 : allowed ==> ssl.gstatic.com. / 192.168.1.200 - allowed by autorisatio | | |
| | Dec 03 10:57:48 : allowed ==> detectportal.firefox.com. / 192.168.1.200 - allowed by au | | |
| | Dec 03 10:57:48 : allowed ==> a1089.dscd.akamai.net. / 192.168.1.200 - allowed by autor | | |
| | Dec 03 10:57:48 : allowed ==> a1089.dscd.akamai.net. / 192.168.1.200 - allowed by autor | | |
| | Dec 03 10:57:49 : ns1.ff.avast.com. / 192.168.1.200 - allowed by autorisations de nuit | | |
| | Dec 03 10:57:49 : allowed ==> clients5.google.com. / 192.168.1.200 - allowed by D.Dysma | | |
| | Dec 03 10:57:49 : allowed ==> clients1.google.com. / 192.168.1.200 - allowed by D.Dysm | | |
| | Dec 03 10:57:49 : allowed ==> clients1.google.com. / 192.168.1.200 - allowed by D.Dysm | | |
| | Dec 03 10:57:56 : validation failure <cdn.permutive.com. A IN>: no DNSSEC records from 1 | | |
| | Dec 03 10:58:03 : denied ==> curl.haxx.se. / 192.168.1.200 - no match | | |
| | Dec 03 10:58:03 : denied ==> curl.haxx.se. / 192.168.1.200 - no match | | |
| | Dec 03 10:58:03 : denied ==> curl.haxx.se. / 192.168.1.200 - no match | | |
| | Dec 03 10:58:05 : allowed ==> support.mozilla.org. / 192.168.1.200 - allowed by autoris | | |
| | Dec 03 10:58:05 : denied ==> prod-tp.sumo.mozit.cloud. / 192.168.1.200 - no match | | |
| | Dec 03 10:58:05 : denied ==> prod-tp.sumo.mozit.cloud. / 192.168.1.200 - no match | | |

- 1) **Log Unbound** : Liste des 150 dernières connexions faites par votre ordinateur, avec l'état de la connexion et la raison de ce refus :
 - a) **allowed** = connexion acceptée (vert)
 - b) **denied** = connexion refusée (rouge)
 - c) **No match** = aucune règle n'a été trouvée pour la connexion demandée (bleu)
 - d) **Validation failure** = connexion refusée par le filtre DNS externe
- 2) **Log Squid** : Liste des connexions faites par votre ordinateur à travers le proxy Squid, avec indication de l'état :
 - a) **DENIED** : connexion refusée
 - b) **TUNNEL**, **MISS** et autres : connexion acceptée

Normalement Squid n'est pas utilisé. C'est une option avancée, et pour la plupart des utilisateurs cette page restera vide.
- 3) **Utilisateurs connectés** : voir plus haut la section *Trouver dans Confix l'adresse Mac d'un utilisateur*

- 4) **Versions** : versions des programmes
- 5) **Diagnostic** : cette commande va récolter dans un fichier toutes les informations qui se trouvent dans les différentes commandes de cette page, et proposer de les enregistrer sur le disque. Ceci permet d'envoyer à un technicien une quantité d'informations qui lui seront utiles pour dépanner un problème.
- 6) **Search** : fonction de recherche dans la configuration active. Il suffit d'entrer une séquence de caractères et de cliquer sur le bouton *Start Search* toutes les lignes contenant cette séquence seront affichées. Très utile pour savoir à qui appartient une adresse mac, ou pour savoir quel utilisateur a droit d'accès à tel site, et cela en vertu de quelle règle.
 - a) **Mac Address** : recherche uniquement dans les adresses Mac
 - b) **Domain** : recherche dans les règles du filtre et dans les groupes
ATTENTION : cette recherche a précedence sur la suivante. Si vous voulez rechercher une adresse mac, veuillez à ce que ce champ soit vide.
- 7) **Technical Data** : Informations techniques utiles pour diagnostiquer un problème. Tout ce qui est présenté ici est inclus dans le fichier de diagnostic.
 - a) Log d'Apache
 - b) Log de cron (exécution périodique de la synchronisation d'Idéfix)
 - c) Log du système (liste des 150 dernières entrées)
 - d) Principaux répertoires d'Idéfix
 - e) Principaux fichiers de configuration d'Idéfix
 - f) Configuration réseau
 - g) Résultat du ping (ping google.com)
 - h) État des services

8. Comment rédiger les adresses des sites web

Le nom de domaine

Quand on se connecte à un site, la barre d'adresse du navigateur indique une adresse qui est constituée de plusieurs éléments :

<http://www.meteofrance.com/previsions-meteo-france/saint-pierre-de-chartreuse/38380>

Pour l'utiliser dans Idéfix, il faut extraire de cette adresse le nom de domaine, marqué ci-dessus en rouge. Il faut donc éliminer le protocole (http:// ou https://) et éliminer la / et tout ce qui se trouve à sa droite. Il reste alors deux éléments : le préfixe, ou sous-domaine, et le nom de domaine, incluant l'extension (comme pour un nom de fichier).



Le nom de domaine complet, avec son extension doit toujours être indiqué. Le préfixe peut être présent, absent, ou remplacé par *. Cela correspond à trois types d'autorisations différents.

Le nom sans préfixe : mon-site-internet.fr

Seule cette adresse précise sera autorisée. Aucun préfixe ne sera autorisé. C'est une forme très restrictive et généralement non désirée car, par exemple, www.mon-site-internet.fr ne marchera pas.

En règle générale, c'est une très mauvaise idée parce que peu de sites fonctionneront avec une telle autorisation. La plupart du temps un site utilise aussi des sous-domaines dans le genre :

images.mon-site-internet.fr

static.mon-site-internet.fr

Etc.

Seule une raison particulière pourra normalement amener à formuler ainsi une autorisation.

Le nom avec le préfixe : www.mon-site-internet.fr

Si on veut limiter l'accès à une partie d'un site qui peut être définie par un préfixe, ce sera la forme à adopter. Exemple : **translate.google.fr**. Si on veut donner accès à la fonction de traduction de google mais pas à la source de programmes et de jeux **play.google.fr** et à tous les autres services de google, cette forme le permet. www, translate et play sont appelés des sous-domaines.

Le nom avec un joker : *.mon-site-internet.fr

C'est la forme la plus couramment employée. Elle autorise tous les préfixes, donc tous les sous-domaines et donne donc accès au site entier, avec une grosse restriction qui sera expliquée après.

Les sites à tiroir

Ils représentent la principale difficulté lors de l'autorisation de sites web. Certains sites complexes, pour fonctionner, utilisent d'autres sites qui ne sont pas des sous-domaines. Ils s'agit en général de très gros sites, comme par exemple ebay. Pour faire fonctionner entièrement le site français d'ebay il faut autoriser :

- *.ebay.fr
- *.ebay.com
- *.ebayimg.com
- *.ebaydesc.fr
- *.ebaydesc.com
- *.ebaystatic.com

Pour les autres langues, il faudrait d'autres extensions. Une future version d'Idéfix devrait permettre de réduire cette liste à :

- *.ebay.*
- *.ebayimg.com
- *.ebaydesc.*
- *.ebaystatic.com

Et ceci autoriserait toutes les langues.

L'existence d'autorisations manquantes se manifeste par fait qu'une fois que l'adresse principale (*.ebay.fr) est autorisée, le site s'ouvre mais avec une allure étrange : les images manquent, la structure de la page est complètement éclatée. Un autre symptôme est le refus d'accès : vous cliquez sur un bouton et une page vous dit que le site n'est pas accessible. Ce bouton ou ce lien vous envoient en fait sur un autre site. C'est particulièrement critique pour les sites sur lesquels on veut payer. Plus insidieux, car plus difficile à découvrir, des sites peuvent avoir recours à des sites externes pour vérifier le certificat nécessaire à une connexion https.

Ces sites à tiroir créent deux difficultés : C'est lourd à autoriser, c'est laborieux de trouver tous les sites à autoriser. Plusieurs outils ont été développés pour répondre à cette difficulté :

1. Les groupes (dans Confix)
2. Le log du filtre Internet (accessible dans Confix)
3. L'analyse des blocages (intégrée à Supervix)

La première solution est la plus simple, utilisable par n'importe qui. Les deux autres sont nettement plus techniques et destinées au technicien qui pourra répondre à votre problème en créant un groupe. Elles sont développées dans le chapitre suivant *Découvrir les sites à autoriser*.

9. Découvrir les sites à autoriser.

Si un groupe n'existe pas pour le site que l'on veut autoriser, un outil a été ajouté à Supervix pour faciliter la découverte des autorisations qui manquent pour qu'une page s'affiche correctement. Pour découvrir ces adresses bloquées, deux procédures se complètent.

Le log du filtre Internet

Dans l'onglet *Informations*, un bouton permet d'accéder à la liste des accès de l'ordinateur dans la dernière heure. Dans l'exemple suivant, un accès à meteofrance avait été ouvert et fonctionnait assez bien. Les sites autorisés par le groupe étaient meteofrance.com et meteofrance.fr. Si cependant on ouvre le log du filtre, il montre ceci :

```
Dec 01 19:59:38 : allowed ==> services.meteofrance.com. / 192.168.1.200 - allowed by autorisations_générales
Dec 01 19:59:38 : allowed ==> education.meteofrance.fr. / 192.168.1.200 - allowed by autorisations_générales
Dec 01 19:59:38 : allowed ==> donneespubliques.meteofrance.fr. / 192.168.1.200 - allowed by autorisations_générales
Dec 01 19:59:39 : allowed ==> vigilance.meteofrance.com. / 192.168.1.200 - allowed by autorisations_générales
Dec 01 19:59:39 : denied ==> aviation.meteo.fr. / 192.168.1.200 - no match
Dec 01 19:59:39 : denied ==> aviation.meteo.fr. / 192.168.1.200 - no match
Dec 01 19:59:39 : denied ==> aviation.meteo.fr. / 192.168.1.200 - no match
Dec 01 19:59:39 : denied ==> www.drias-climat.fr. / 192.168.1.200 - no match
Dec 01 19:59:39 : denied ==> www.drias-climat.fr. / 192.168.1.200 - no match
Dec 01 19:59:39 : denied ==> www.drias-climat.fr. / 192.168.1.200 - no match
Dec 01 19:59:39 : denied ==> pluiesextremes.meteo.fr. / 192.168.1.200 - no match
Dec 01 19:59:39 : denied ==> pluiesextremes.meteo.fr. / 192.168.1.200 - no match
Dec 01 19:59:39 : denied ==> pluiesextremes.meteo.fr. / 192.168.1.200 - no match
Dec 01 19:59:39 : allowed ==> tempestes.meteofrance.fr. / 192.168.1.200 - allowed by autorisations_générales
Dec 01 19:59:39 : allowed ==> www.vigilance.meteofrance.com. / 192.168.1.200 - allowed by autorisations_générales
Dec 01 19:59:39 : allowed ==> www.vigilance.meteofrance.com. / 192.168.1.200 - allowed by autorisations_générales
Dec 01 19:59:39 : denied ==> bibliotheque.meteo.fr. / 192.168.1.200 - no match
Dec 01 19:59:39 : denied ==> bibliotheque.meteo.fr. / 192.168.1.200 - no match
Dec 01 19:59:39 : denied ==> www.meteo.fr. / 192.168.1.200 - no match
Dec 01 19:59:39 : denied ==> bibliotheque.meteo.fr. / 192.168.1.200 - no match
Dec 01 19:59:39 : denied ==> www.meteo.fr. / 192.168.1.200 - no match
```

Les lignes vertes sont autorisées, les lignes bleues montrent les sites pour lesquels aucune autorisation n'a été trouvée. On voit tout de suite qu'il faudrait impérativement ajouter au groupe **.meteo.fr*. Pour *www.drias-climat.fr*, il faudrait vérifier le site pour voir de quoi il s'agit. Les lignes suivantes, non affichées dans l'exemple, montrent que d'autres sites encore seraient souhaitables :

*.meteo-spaciale.fr

*.vigimeteo.com

*.vigicrues.gouv.fr

Cette page montre encore les blocages issus de Confix (ligne en texte rouge), comme par exemple la coupure de nuit :

```
Dec 01 19:19:01 : denied ==> isatap.localdomain. / 192.168.1.200 - Coupure de nuit
Dec 01 19:19:02 : denied ==> wpad.localdomain. / 192.168.1.200 - Coupure de nuit
Dec 01 19:19:02 : denied ==> wpad.localdomain. / 192.168.1.200 - Coupure de nuit
Dec 01 19:19:05 : allowed ==> ncc.avast.com. / 192.168.1.200 - allowed by autorisations de nuit
Dec 01 19:19:31 : allowed ==> pop.gmx.com. / 192.168.1.200 - allowed by courrier électronique
Dec 01 19:19:31 : allowed ==> pop.orange.fr. / 192.168.1.200 - allowed by courrier électronique
Dec 01 19:19:31 : allowed ==> pop.orange.fr. / 192.168.1.200 - allowed by courrier électronique
Dec 01 19:19:31 : allowed ==> pop.gmx.com. / 192.168.1.200 - allowed by courrier électronique
Dec 01 19:19:36 : denied ==> shavar.services.mozilla.com. / 192.168.1.200 - Coupure de nuit
Dec 01 19:19:36 : denied ==> detectportal.firefox.com. / 192.168.1.200 - Coupure de nuit
Dec 01 19:19:36 : denied ==> detectportal.firefox.com. / 192.168.1.200 - Coupure de nuit
Dec 01 19:20:17 : denied ==> wpad.localdomain. / 192.168.1.200 - Coupure de nuit
Dec 01 19:20:17 : denied ==> wpad.localdomain. / 192.168.1.200 - Coupure de nuit
```

Elle montre enfin les blocages issus du filtre DNS externe, surlignées en rouge. Dans l'exemple suivant on voit des pages qui avaient été autorisées par Idéfix et qui ont été bloquées par SafeDNS (pages de publicités).

```
Dec 01 18:48:56 : allowed ==> cdn.taboola.com. / 192.168.1.200 - allowed by D.Dysmas
Dec 01 18:48:57 : validation failure <cdn.taboola.com. A IN>: no DNSSEC records from 195.46.39.39 for DS taboola.com. while building chain of trust
Dec 01 18:48:57 : allowed ==> widgets.outbrain.com. / 192.168.1.200 - allowed by D.Dysmas
Dec 01 18:48:57 : allowed ==> onclickads.net. / 192.168.1.200 - allowed by D.Dysmas
Dec 01 18:48:57 : validation failure <widgets.outbrain.com. A IN>: no DNSSEC records from 195.46.39.39 for DS outbrain.com. while building chain of trust
Dec 01 18:48:57 : validation failure <onclickads.net. A IN>: no DNSSEC records from 195.46.39.39 for DS onclickads.net. while building chain of trust
Dec 01 18:48:57 : allowed ==> popcash.net. / 192.168.1.200 - allowed by D.Dysmas
Dec 01 18:48:57 : allowed ==> cdn.engine.4dsply.com. / 192.168.1.200 - allowed by D.Dysmas
Dec 01 18:48:57 : validation failure <popcash.net. A IN>: no DNSSEC records from 195.46.39.39 for DS popcash.net. while building chain of trust
Dec 01 18:48:58 : validation failure <cdn.engine.4dsply.com. A IN>: no DNSSEC records from 195.46.39.39 for DS 4dsply.com. while building chain of trust
```

Analyse des blocages de sites

Un autre outil d'analyse a été intégré à Supervix. Partant de la même source (le log du filtre Internet), le contenu va être analysé et les lignes regroupées. Le résultat est moins détaillé mais plus rapidement lisible. Procédure à suivre :

Comme les ordinateurs sont extrêmement bavards, il vaut mieux laisser le vôtre tranquille pendant cinq minutes au moins après l'avoir démarré afin qu'il se calme un peu.

- Ouvrez votre navigateur
- Connectez-vous sur Idéfix avec son adresse IP, par exemple 192.168.84.184.
- Ouvrez l'option « Analyse des blocages de sites » dans les "Fonctions utilisateur".
- Dans un deuxième onglet préparez vous à vous connecter sur le site que vous voulez tester.
- Quand vous êtes prêt, dans le premier onglet cliquez sur le bouton « Heure de début », et sans attendre, dans le deuxième onglet, faites l'opération qui provoque le blocage.
- Sans attendre, revenez au premier onglet et cliquez sur le bouton Analyser. Vous verrez apparaître un résultat dont voici un exemple :

Votre adresse IP :

192.168.1.222

Heure de début :

18:15:48

☒ Proxy

☐ Firewall

Analyser

Heure de fin :

hh:mm:ss

| URL | DENIED | ALLOWED | Total |
|-----------------------------|--------|---------|-------|
| mozilla.com | | 4 | 4 |
| firefox.com | | 2 | 2 |
| pki.goog | 1 | | 1 |
| france-chauffage-solaire.fr | 1 | | 1 |

Si nous disons *sans attendre*, ce n'est pas parce que nous sommes des gens pressés, mais pour éviter, autant que possible, l'affichage des sites avec lesquels l'ordinateur a l'habitude de bavarder.

Dans cet exemple, deux adresses ont été bloquées (dans la colonne DENIED) : pki.goog et france-chauffage-solaire.fr

- Faire une copie d'écran, ou copier les adresses bloquées. Pour éviter les erreurs, vous pouvez sélectionner et coller dans le presse papier.
- Envoyer cette information au responsable d'Idéfix, en lui indiquant le site que vous vouliez ouvrir et ce qui vous était refusé, afin qu'il puisse faire le nécessaire.

Une fois que les adresses bloquées auront été autorisées, il n'est pas certain que votre site marchera correctement, peut-être qu'il essayera de se connecter à une autre adresse qui serait elle aussi bloquée. Il vous faudra donc refaire le même test. Il peut y avoir ainsi plusieurs étapes. On ne peut en découvrir qu'un seul à la fois. Cliquer sur *Heure de début* puis *Analyser* pour vider la liste.

Remarques importantes

Agir rapidement

On l'a dit, les ordinateurs sont extrêmement bavards. C'est la raison pour laquelle, afin d'éviter de mélanger leurs bavardages impénitents avec le test que vous voulez faire, il importe d'agir relativement vite et donc d'enchaîner assez rapidement la séquence :

- cliquer sur heure de début,
- faire le test,
- cliquer sur analyser.

C'est pour la même raison qu'il peut être utile de le refaire le test une deuxième fois, si les résultats qui apparaissent sont un peu différents, le technicien saura choisir ce qui est important.

Le problème du cache

1) Le cache du navigateur :

Votre navigateur possède un cache qui mémorise les connexions. Si vous faites le test ci-dessus et que vous essayez de vous connecter sur un site autorisé, seule la première fois où vous vous connecterez pourra apparaître dans le tableau. Si vous essayez une deuxième fois, vous ne verrez plus l'adresse du site. Ce n'est pas une anomalie, cela tient au fonctionnement du cache. Mais quand un site est bloqué, il ne sera normalement pas mémorisé dans votre navigateur et vous le verrez apparaître pour chaque tentative.

2) Le cache du filtre :

Le filtre a aussi son cache, qui a un effet supplémentaire : Si vous essayez d'accéder à un site bloqué, puis que vous faites une modification pour le débloquent, si vous essayez immédiatement de vous connecter de nouveau, le blocage sera toujours présent, car il est mémorisé pendant deux minutes. Il faut donc attendre au moins deux minutes entre deux essais, pour être sûr que le cache ne va pas s'interposer dans vos essais.

10. Les groupes

Les groupes sont simplement des listes d'autorisations qu'on peut attribuer ensemble en donnant à un utilisateur l'autorisation d'utiliser ce groupe.

Les sites techniques

Parmi les difficultés précédentes, celles liées à un aspect technique (paiement, certificats) sont résolues en autorisant les deux groupes correspondants. Ces sites techniques peuvent être autorisés sans inconvénient, personne n'ira s'amuser à jouer avec.

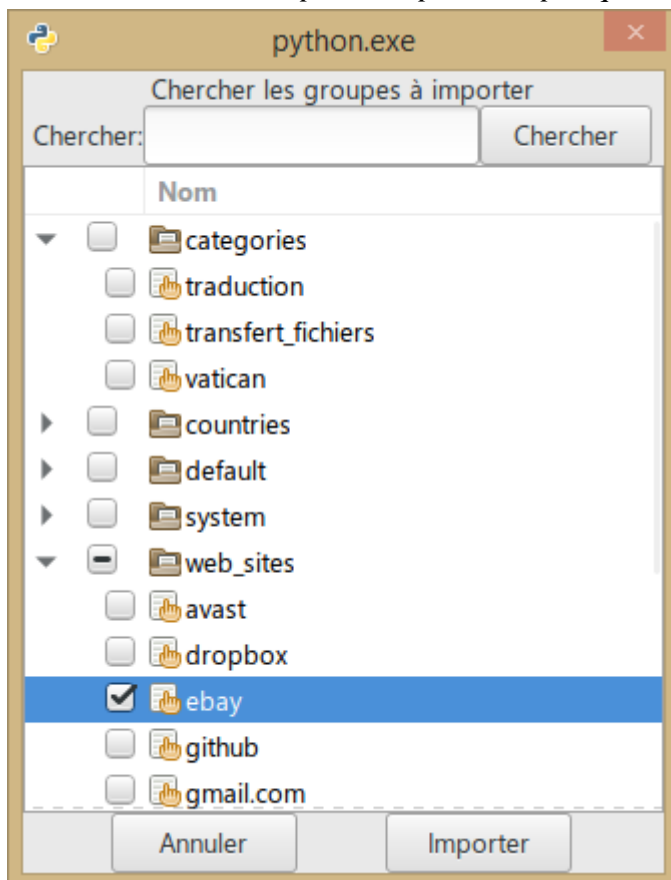
Comme de nouveaux sites apparaissent régulièrement, ils seront mis à jour régulièrement dans la base de données, et une procédure de mise à jour des groupes locaux sera mise en place (elle n'est pas encore active).

Les antivirus nécessitent souvent plusieurs adresses pour leur mise à jour. Des groupes seront créés progressivement pour chacun.

Les sites webs connus

Pour autoriser en une seule opération l'accès à ebay, un groupe a été créé qui contient toutes les autorisations nécessaires. Les groupes peuvent être personnels (créés par l'utilisateur pour son usage personnel) ou partagés.

Les groupes partagés sont stockés dans une base de données, sur le site idefix64.fr et on peut accéder au contenu de cette base depuis Confix, en ouvrant le gestionnaire de groupes et en prenant la commande *Importer depuis le dépôt* qui va ouvrir la fenêtre :



Sélectionner (par exemple) le groupe ebay et cliquer sur importer. Le groupe apparaît alors dans la liste des groupes d'Idéfix et on peut glisser déposer le groupe dans les permissions d'un utilisateur.

La base de donnée est encore toute neuve et ne contient que très peu de groupes, mais elle pourra grandir avec l'aide des utilisateurs, car l'utilisateur qui a créé un groupe pourra le soumettre sur le site, et après vérification de sa pertinence, il sera intégré à la base.

Les catégories

Il peut être pratique d'avoir un groupe qui regroupe les différents sites concernant un thème, par exemple les sites météo en France. Le groupe fr/meteo a été créé pour cela. Il contient actuellement :

- *.meteofrance.com
- *.meteofrance.fr
- *.vigimeteo.com
- *.meteociel.fr
- *.meteosuisse.admin.ch
- *.meteosuisse.ch

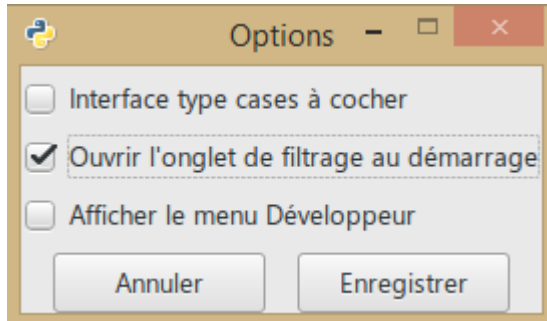
Meteosuisse a été ajouté parce que le site est en français et fournit des informations utiles pour l'Est de la France.

Le gestionnaire de groupes

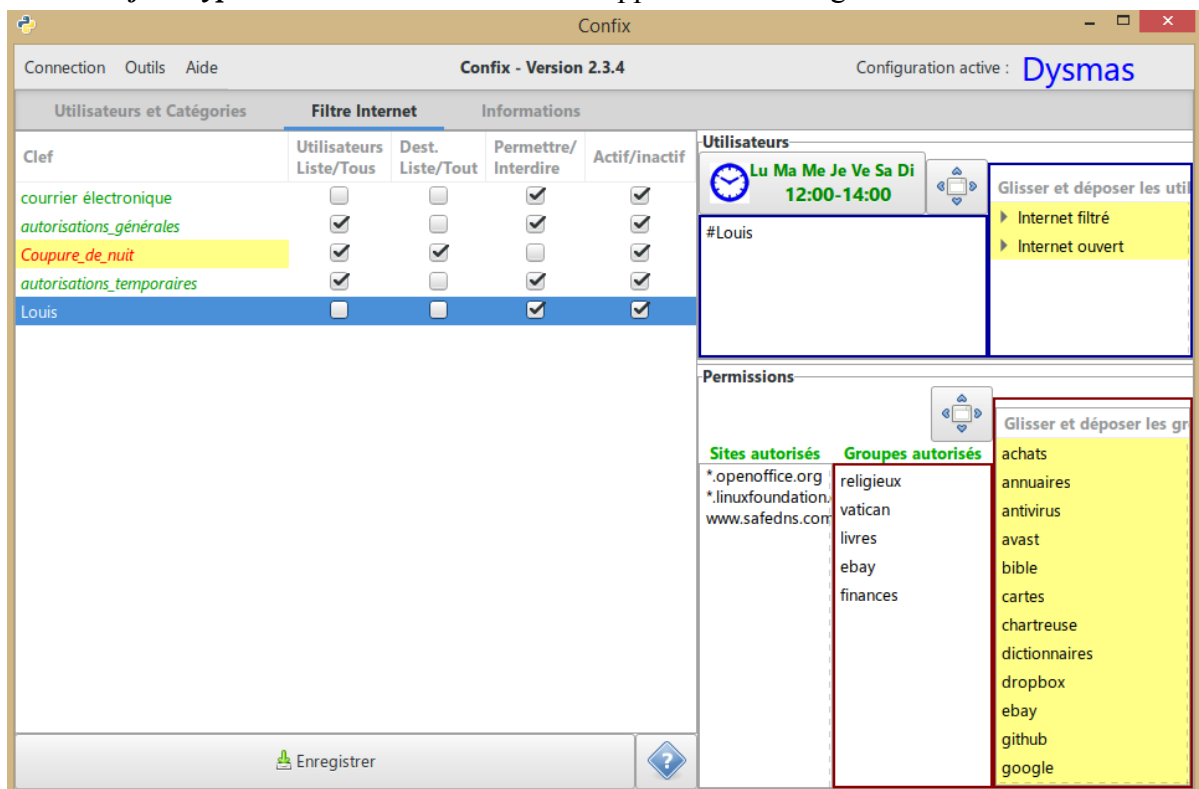
Cette partie n'est pas encore rédigée. ££

11. Les options

Les fenêtre des options est accessible à partir du menu Connexion / Options.
Peu nombreuses pour l'instant, elles se développeront sans doute plus tard.



Interface type cases à cocher : Modifie l'apparence de l'onglet filtre Internet :



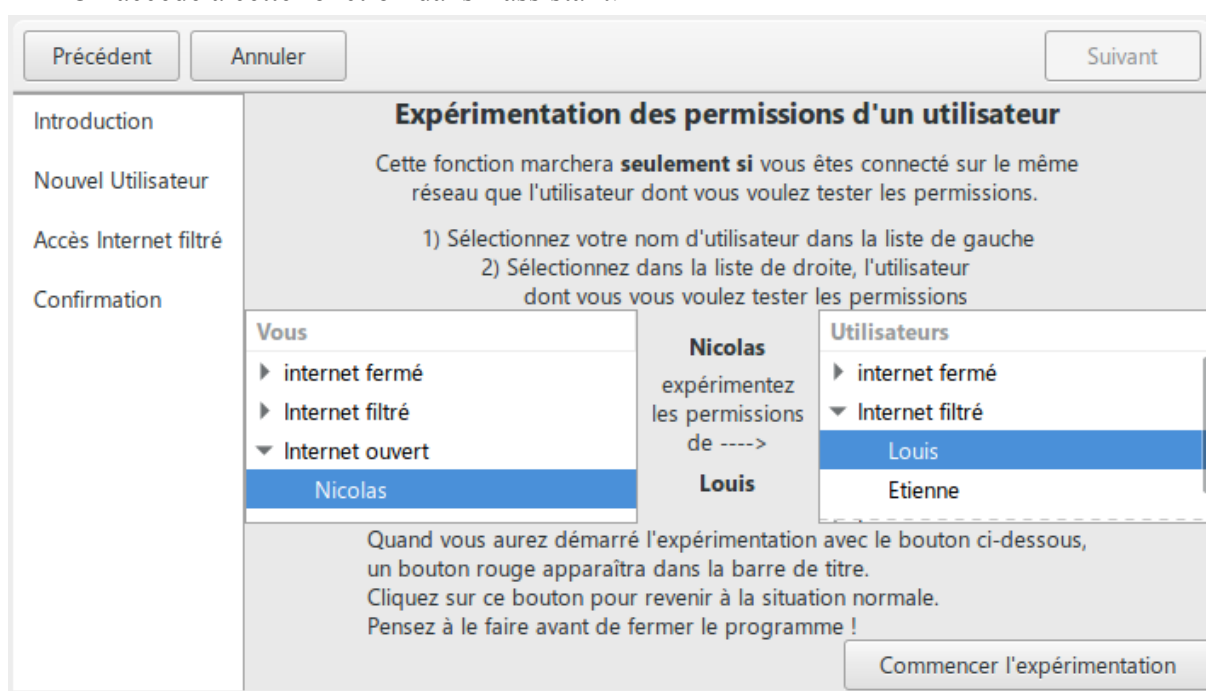
Ouvrir l'onglet de filtrage au démarrage : Comme on ne touche qu'assez peu souvent aux utilisateurs, cocher cette option permet d'ouvrir automatiquement l'onglet Filtre Internet lorsqu'on démarre Confix.

Afficher le menu Développeur : Cette option affiche un menu supplémentaire avec des options plus techniques qui permettent de modifier une configuration en dehors d'une connexion. Voir plus bas la section *Mode développeur*. Le changement de cette option nécessite un redémarrage pour prendre effet.

12. Expérimenter les permissions d'un autre utilisateur

Cette fonction permet à un utilisateur directement connecté sur le réseau local, d'expérimenter les permissions d'un autre utilisateur. Elle est destinée au responsable des permissions qui veut vérifier s'il n'a pas fait d'erreur et si l'utilisateur concerné a bien les autorisations qu'il souhaite et seulement celles-là. Cette fonction est malheureusement passablement perturbée par les caches qu'il faudrait, idéalement, vider tous avant de l'utiliser.

On accède à cette fonction dans l'assistant.



Dans cet exemple, Nicolas va expérimenter les autorisations de Louis. Il faut évidemment que ce soit vrai, c'est-à-dire que ce soit bien Nicolas qui travaille et qu'il choisisse bien le compte de l'ordinateur qu'il utilise. Tout autre choix n'aurait pas de sens.

Quand il aura cliqué sur le bouton *commencer l'expérimentation*, un message apparaîtra dans la barre de titre :



ATTENTION : actuellement, ce ne sera réellement actif que lorsqu'il aura enregistré la modification.

Pour annuler, cliquer sur le bouton « Expérimentation de... » et enregistrer.

13. Sauvegarder et restaurer

Sauvegarder

Idéfix enregistre automatiquement sa configuration tous les jours dans deux emplacements : sur son disque (/var/spool/ idéfix/backup) et sur le serveur FTP s'il est défini, dans le sous répertoire *backup*. L'effacement progressif de ces backup est automatique selon la procédure suivante :

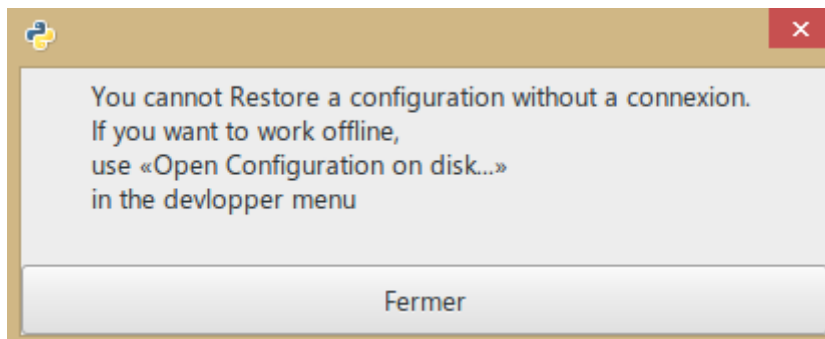
- Les dix derniers backups quotidiens sont conservés.
- Durant le mois précédent, un backup par semaine est conservé.
- Durant les onze mois précédents, un backup par mois est conservé.
- Avant cela, un backup par an est conservé.

Ces backup ne conservent pas seulement la configuration du filtrage, ils conservent tous les fichiers essentiels d'Idéfix et permettent de le ramener à un état précédent en cas de difficulté.

Si l'utilisateur veut faire une sauvegarde sur son disque ou sur une clef USB de la configuration du filtre, qui se trouve dans un fichier nommé *idéfix.json*, il peut le faire par le menu *Sauvegarder la configuration...*

Restaurer

Le menu Restaurer à une fonction bien précise : il est destiné à importer dans un module Idéfix, ou sur un site ftp distant, une configuration enregistrée sur le disque. Cela peut être utilisé pour la première configuration d'un appareil, ou pour revenir en arrière si une modification récente s'avérait dommageable. Ce menu ne peut être utilisé que lorsqu'il y a une connexion existante. Si Confix n'est pas connecté, le message suivant apparaît :

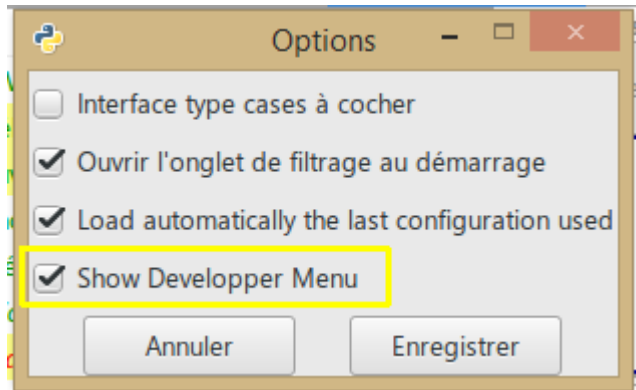


Une fois que la configuration à restaurer est chargée dans Confix, elle sera enregistrée dans l'appareil ou sur le site ftp par le bouton enregistrer, comme d'habitude.

Il est possible de travailler sur une configuration enregistrée sur disque, en dehors d'une connexion. Il faut dans ce cas utiliser le menu développeur, dont il est question ci-après.

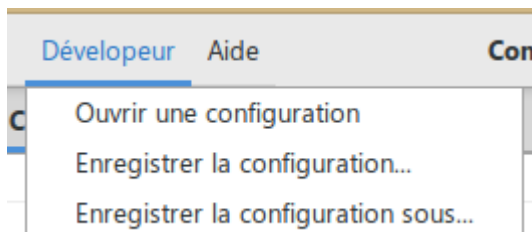
14. Menu développeur

Ce menu est normalement caché. Pour y accéder cocher la case nécessaire dans les options :

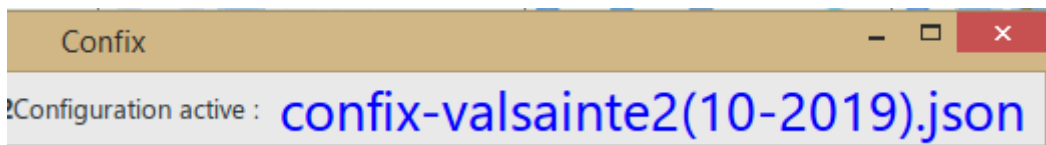


Travailler hors connexion

Ceci fait apparaître au prochain démarrage un menu qui permet de travailler sans avoir de connexion avec un module Idéfix. Une configuration peut être ouverte et enregistrée sur fichier.



Ouvrir une configuration sur le disque fait automatiquement passer le programme en mode fichier. Rien ne sera envoyé par FTP et le bouton *enregistrer* devient inactif. On travaille sur un fichier, et les commandes *ouvrir*, *enregistrer* et *enregistrer sous* ont leur signification habituelle. Le nom du fichier ouvert apparaît dans le titre.



La différence majeure entre Ouvrir une configuration et Restaurer est que la restauration ne quitte pas la connexion ouverte et ne désactive pas le bouton enregistrer. Si la configuration ouverte était une connexion directe sur un Idéfix, l'opération qui consiste à Restaurer un fichier, puis à enregistrer normalement va **remplacer** la configuration interne d'Idéfix par le contenu du fichier. C'est bien ce qu'on appelle restaurer.

Quand par contre on travaille sans connexion, on se contente de modifier un fichier. Si plus tard on estime qu'il est valable, il faudra suivre les opérations suivantes :

1. Connecter Idéfix sur l'appareil ou le site ftp visé
2. Prendre la commande Restaurer pour charger le fichier dans Confix, ce qui remplace dans Confix la configuration ouverte à l'étape 1 par celle du fichier choisi

3. Enregistrer. La configuration qui se trouvait dans le module Idéfix ou sur le site ftp est alors écrasée. Cette opération est sans retour.

Respecter les procédures

Quand on travaille hors connexion, il ne faut jamais utiliser les options du menu *Connexion*, il faut utiliser exclusivement les trois options du menu développeur, pour ouvrir et enregistrer un fichier.

Si en cours de travail hors connexion on se connecte sur un appareil ou sur un site, la configuration sur laquelle on travaillait sera remplacée dans Confix par celle de l'appareil ou du site sur lequel on vient de se connecter. Il est donc indispensable d'enregistrer d'abord son travail avant de se connecter. [Ce n'est pas encore demandé par le programme. \$\$]

15. Trouver les adresses Mac

Adresses Mac

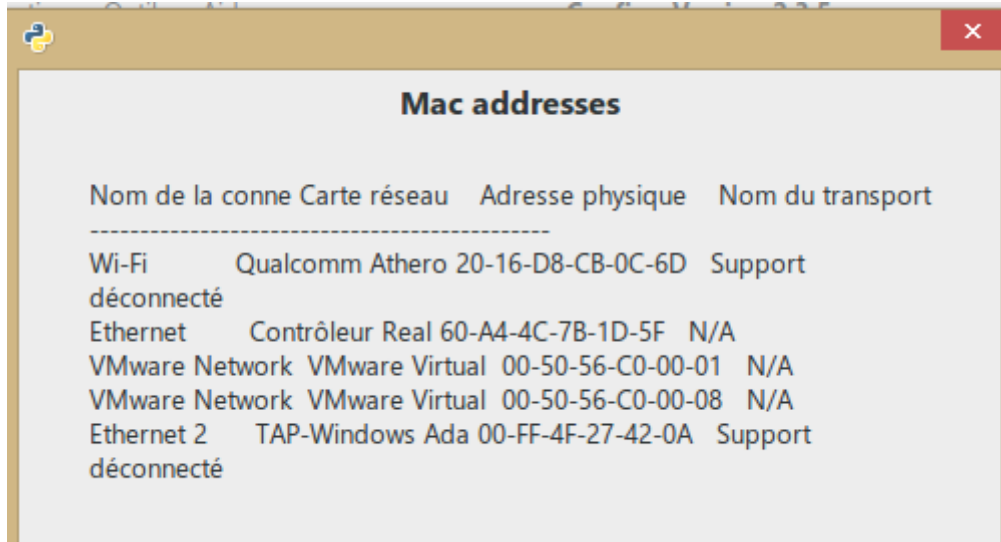
L'adresse Mac est l'identifiant unique d'un appareil sur le réseau. Plus précisément, identifiant d'un module de communication d'un appareil sur le réseau. Un ordinateur portable a généralement deux modules de communication, un par fil et l'autre sans fil (WiFi). Chacun a son adresse Mac personnelle.

Elle se présente comme une séquence de douze chiffres et lettres, séparés par : ou par un tiret tous les deux caractères. Par exemple :

60:a4:4c:7b:45:e4

Trouver l'adresse mac de l'ordinateur sur lequel Confix est exécuté

Confix a une commande pour cela dans le menu outils. Elle présente toutes les adresses de toutes les interfaces. Les deux utiles sont en général les deux premières, ethernet et WiFi (si l'ordinateur est équipé d'un WiFi).



| Nom de la conne | Carte réseau | Adresse physique | Nom du transport |
|-----------------|-----------------|-------------------|--------------------|
| Wi-Fi | Qualcomm Athero | 20-16-D8-CB-0C-6D | Support déconnecté |
| Ethernet | Contrôleur Real | 60-A4-4C-7B-1D-5F | N/A |
| VMware Network | VMware Virtual | 00-50-56-C0-00-01 | N/A |
| VMware Network | VMware Virtual | 00-50-56-C0-00-08 | N/A |
| Ethernet 2 | TAP-Windows Ada | 00-FF-4F-27-42-0A | Support déconnecté |

Trouver dans Confix l'adresse Mac d'un ordinateur connecté au réseau

Dans l'onglet *Informations*, le bouton *Utilisateurs connectés* donne une liste des ordinateurs qui sont ou ont été récemment connectés au réseau. Ensuite il donne une deuxième liste qui est celle des ordinateurs qui se sont connectés au réseau en mode automatique (DHCP), c'est-à-dire qui n'avaient pas une adresse fixe. Il faut seulement pouvoir reconnaître le nom réseau de l'utilisateur. Les lignes marquées « expired » correspondent à des utilisateurs qui se sont connectés dans le passé et ne le sont plus actuellement.

| | |
|-----------------|---|
| Connected Users | 192.168.1.48 - 00:21:70:f8:58:f1 (Etienne) |
| Versions | 192.168.1.50 - 48:5b:39:4a:40:be (Jean-Thomas) |
| Search | 192.168.1.53 - 64:00:6a:02:4e:37 (Sebastien) |
| Mac Address | 192.168.1.54 - fc:aa:14:28:de:e0 (Laurent BORNE) |
| Domain | 192.168.1.57 - 14:da:e9:28:06:70 (Syméon) |
| Start Search | 192.168.1.58 - dc:85:de:72:96:d9 (Dominique) |
| Technical data | 192.168.1.59 - 40:8d:5c:5f:28:72 (Serafico) |
| | 192.168.1.61 - aa:94:40:6e:38:49 (Joseph-Marie) |
| | 192.168.1.62 - d8:50:e6:84:a2:b1 (Joseph-Marie) |
| | 192.168.1.63 - 24:b6:fd:26:72:38 (Roman) |
| | 192.168.1.83 - 30:85:a9:f1:e3:6b (Thierry Pont) |
| | Active or expired automatic connections : |
| | 2019-12-02 12:09:44.889687 |
| | 192.168.1.200 - 60:a4:4c:7b:1d:5f - active - "Dysmas" (RP Dysmas) |
| | 192.168.1.205 - dc:ef:09:ee:4b:03 - active - "WNR2000v5" () |
| | 192.168.1.206 - 00:21:70:f8:58:f1 - expired (Etienne) |
| | 192.168.1.207 - a0:ce:c8:30:03:3d - expired (Dom Lorenzo) |
| | 192.168.1.208 - 3c:18:a0:04:a6:64 - expired (Dom Norbert) |

Cette commande est disponible à partir de la version 2.3.5

Supervix

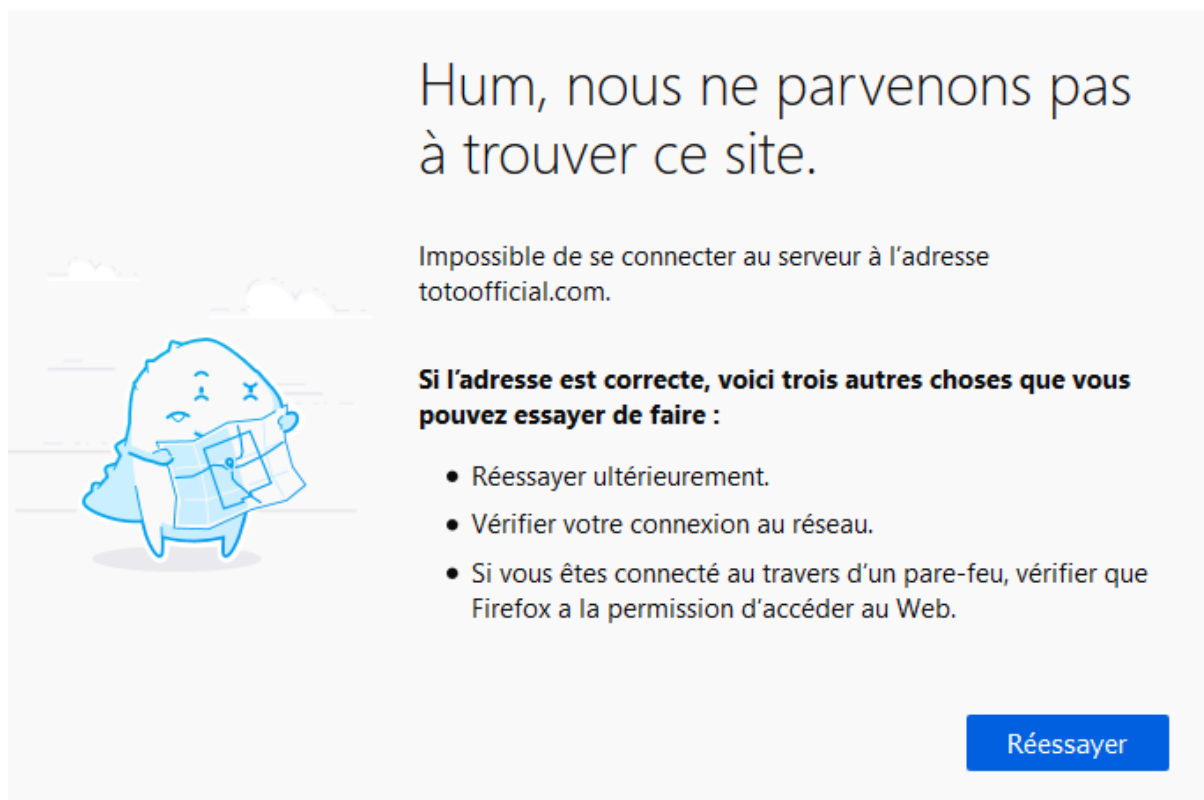
Supervix possède la même commande qui donne les mêmes informations.

| | |
|--------------------------------|--|
| Informations techniques | 192.168.1.208 - 3c:18:a0:04:a6:64 - expired (Dom Norbert) |
| Bandwidthd : Activité réseau | 192.168.1.209 - 54:04:a6:03:b5:80 - expired (Pierre-Marie Flach) |
| Utilisateurs connectés | 192.168.1.210 - b0:eb:57:85:42:66 - active - "HUAWEI_MediaPad_M5-a63580" |
| Visualiser les fichiers *.conf | 192.168.1.211 - 00:23:df:fe:25:8e - expired (Père Vianney) |
| Visualiser le fichier syslog | 192.168.1.212 - 08:60:6e:b6:9c:cb - expired (Dom Moses) |
| Visualiser les fichiers *.log | 192.168.1.226 - 40:16:7e:6b:51:54 - active - "DESKTOP-5KPCAFF" (Jose-Luis) |
| Enregistrer les fichiers *.log | 192.168.1.227 - 98:4b:e1:a7:44:ed - expired () |
| État du réseau Ping | 192.168.1.228 - f8:32:e4:3b:ccfd - expired (Dom Piero) |
| | 192.168.1.229 - 98:83:89:4b:dc:4a - expired (Marie-Christine) |
| | 192.168.1.230 - 00:40:d0:65:1e:5c - expired (Mere Blanca) |

16. Messages affichés en cas de blocage

Le message affiché par le navigateur en cas de blocage indique simplement que la page n'existe pas. Ce serait bien d'avoir une page qui dise explicitement que c'est Idéfix qui refuse, mais nous ne savons pas encore le faire.

Firefox renvoie cette page :



SafeDNS

Pour les blocages de SafeDNS, la situation n'est pas très stable. Normalement le même message apparaît, mais cela peut parfois varier.

Internet Explorer

Dans Internet Explorer, le message de blocage est ordinairement :

Cette page ne peut pas s'afficher

- Vérifiez que l'adresse Web <https://www.youtube.com> est correcte.
- Recherchez la page avec votre moteur de recherche.
- Actualisez la page dans quelques minutes.

Résoudre les problèmes de connexion

Un autre navigateur donnera des messages différents mais de même signification.