

CTparental sous PrimTux

à noter que ce Contrôle parental peut s'installer sur de nombreux systèmes informatiques

Installer Primtux 7

PrimTux est une distribution GNU/Linux spécialisée pour l'école primaire. Elle est construite avec à partir de Ubuntu ou Debian et intègre, en plus des logiciels de bureautique, internet, multimédia classiques, un nombre important d'applications éducatives ou adaptées à l'enseignement élémentaire.

Démarrer Firefox de **tous les bureaux mini à maxi et administrateur**,
Faire apparaître la Barre de menu et la barre personnelle

Installer les modules complémentaires suivants

Firefox → Outils → Modules complémentaires →

Un anti-cookie

Cookie AutoDelete =

Supprime automatiquement les cookies lorsqu'ils ne sont plus utilisés par les onglets ouverts du navigateur. Avec les cookies, les sessions persistantes, ainsi que les informations utilisées pour vous espionner, seront effacées.

Configurer aller dans les préférences, clique carré noir du haut, cocher les lignes et régler à 3 secondes et cookies

<https://addons.mozilla.org/firefox/addon/cookie-autodelete>

Un anti-espion

Privacy-Badger = bloque les données collectées au travers de cookies tiers. Il protège votre vie privée en bloquant les publicités d'espionnage et les traqueurs invisibles. Empêche la prise d'empreintes digitales sur toile, (comme CanvasBlocker), les supercookies (comme Click&Clean), et les cookies uniques qui contiennent des ID de suivi. C'est un excellent outil pour cacher les adresses IP lors de visioconférence en WebRTC avec le navigateur interne, à paramétrer dans les préférences. Ajouter les URL désirés dans la liste blanche.

<https://www.eff.org/fr/privacybadger>

Privacy Settings = Permet de régler la confidentialité de Firefox.

Cliquer sur l'icône de Privacy-settings dans la barre d'outils du navigateur puis sur le réglage ; il permet de régler les variables de Firefox dans la confidentialité, une fois installé cliquer sur l'icône dans la barre de menu puis *Enhanced Privacy (améliorer la confidentialité)*

<https://addons.mozilla.org/fr/firefox/addon/privacy-settings/>

Répondre non sur le changement de langue

Le module anti-publicité est installé mais pas paramétré

uBlock Origin = antipub le + puissant

<https://addons.mozilla.org/fr/firefox/addon/ublock-origin/?src=ss>

Préférences → Afficher le tableau de bord → Listes de filtres → cliquer sur + → cocher toutes les cases Publicités, confidentialité, réseaux sociaux, domaines malveillants, nuisances → Appliquer.

Corriger l'indiscrétion dans le navigateur Firefox

Essayons de corriger tout cela. Il y a donc plusieurs choses à faire :

Écrivez dans la barre d'adresse de votre navigateur Firefox: ***about:config***

Évidemment Cliquer **je ferai attention, promis**



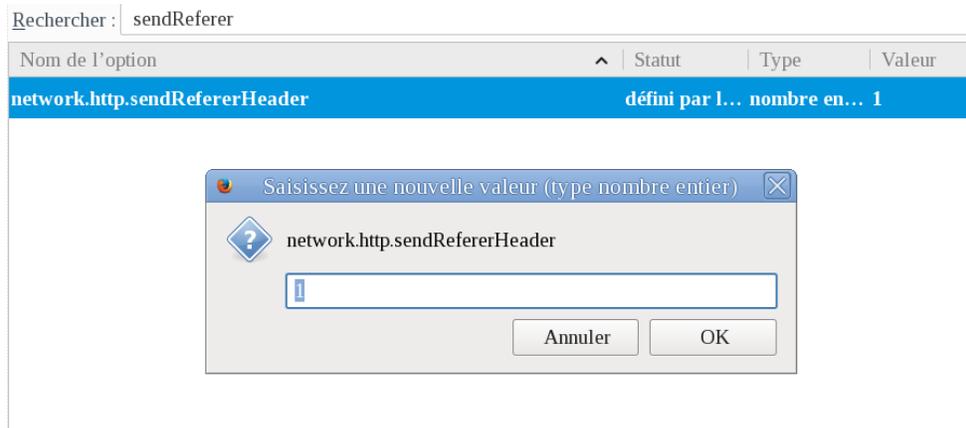
Attention, danger !

La modification de ces préférences avancées peut être dommageable pour la stabilité, la sécurité et les performances de cette application. Ne continuez que si vous savez ce que vous faites.

Afficher cet avertissement la prochaine fois

Je ferai attention, promis !

Masquer la dernière page visitée : modifiez la chaîne **network.http.sendRefereHeader**, Cette chaîne permet au navigateur de mémoriser les pages visitées auparavant ; double clic sur cette ligne, en lui assignant la valeur **1**. valider



Désactiver la télémétrie :

browser.newtabpage.activity-stream.telemetry = false

browser.newtabpage.activity-stream.feeds.telemetry = false

browser.newtabpage.activity-stream.telemetry.structuredIngestion.endpoint =
effacer <https://incoming.telemetry.mozilla.org/submit>

browser.newtabpage.activity-stream.telemetry.ut.events = false

browser.ping-centre.telemetry = false

datareporting.policy.dataSubmissionEnabled = false

datareporting.healthreport.service.enabled = false

datareporting.healthreport.uploadEnabled = false

security.identitypopup.recordEventTelemetry = false

security.certerrors.recordEventTelemetry = false

toolkit.telemetry.archive.enabled = false

toolkit.telemetry.bhrPing.enabled = false

toolkit.telemetry.enabled = false

toolkit.telemetry.rejected = true

toolkit.telemetry.shutdownPingSender.enabled = false

toolkit.telemetry.server = effacer <https://incoming.telemetry.mozilla.org>

toolkit.telemetry.unified = false

toolkit.telemetry.unifiedIsOptIn = false

Mettre à jour les paquets en faisant
sudo apt-get update && sudo apt-get dist-upgrade && sudo apt-get clean &&
sudo apt-get autoclean && sudo apt-get autoremove

Redémarrer l'ordinateur

- Installation des logiciels non libres, cela s'installe parfois et d'autres fois non
(1 ordinateur sur 4)

<https://forum.primtux.fr/showthread.php?tid=1711&pid=18827#pid18827>

Alternative pour installer Libdvdcss et lire les DVD cryptés du commerce sans
les menottes numériques

```
sudo apt-get install libdvd-pkg
```

```
sudo dpkg-reconfigure libdvd-pkg
```

CTparental

Télécharger CTParental

<https://gitlab.com/ctparentalgroup/CTparental/-/releases>

Première méthode

https://gitlab.com/marsat/CTparental/uploads/eee3b06208e977cdf4f7fad57051c70c/ctparental_ubuntu20.04_lighttpd_5.0.8-1.0_all.deb

Pour la 2022.04 ce sera ce lien

https://gitlab.com/ctparentalgroup/CTparental/uploads/5e5b99b9b23521719b7bc65c188f1dde/ctparental-alt_debian11_ubuntu21.10_5.1.03-1.0_all.deb

Se mettre dans le dossier dans lequel le fichier est téléchargé

```
$ cd Téléchargements
```

```
sudo dpkg -i ctparental_ubuntu20.04_lighttpd_5.0.8-1.0_all.deb
```

Seconde méthode

```
sudo -i
```

mot de passe

```
# wget -c
```

```
https://gitlab.com/marsat/CTparental/uploads/eee3b06208e977cdf4f7fad57051c70c/ctparental\_ubuntu20.04\_lighttpd\_5.0.8-1.0\_all.deb
```

```
sudo apt-get update
```

```
sudo gdebi ctparental_ubuntu20.04_lighttpd_5.0.8-1.0_all.deb
```

Si problèmes de dépendances dans les deux cas, faire :

```
sudo apt-get -f install
```

Si **le CT Parental est installé et a échoué**, purger les paquets qui posent problème

```
sudo apt-get autoremove --purge ctparental clamav-* privoxy lighttpd* nginx*  
dnsmasq e2guardian
```

```
sudo rm -rf /etc/Ctparental
```

```
sudo rm -rf /etc/lighttpd/
```

```
sudo rm -rf /etc/nginx/
```

refaire une mise à jour complète

```
sudo apt-get update && sudo apt-get dist-upgrade && sudo apt-get clean &&  
sudo apt-get autoclean && sudo apt-get autoremove
```

ou par Synaptic → Recharger → Ajouter → Appliquer → Appliquer

Paramétrer le Contrôle parental

Aller sur l'interface d'administration de CTparental en se rendant à l'adresse <https://admin.ct.local/>

Lors de l'installation, il sera demandé de définir le nom d'**utilisateur (au moins 5 caractères)** et le mot de passe, de les saisir et de les saisir à nouveau pour confirmer. Noter que le mot de passe doit être composé d'au moins **8 caractères minimum** dont **1 chiffre, 1 majuscule et 1 caractère spécial**.

Paramétrer tous les onglets du CTparental

Filtrage Blacklist

on coche ce que l'on veut en plus

The screenshot shows the 'Filtrage par BlackList' configuration page. At the top, there's a navigation bar with 'filtrage web' and a status indicator 'Le filtrage de noms de domaine est actuellement activé'. A red button 'Désactiver le filtrage' and a 'Déconnexion' button are also present. The main content area is titled 'Filtrage par BlackList' and includes a sidebar with navigation links like 'extensions à filtrer', 'type MIME à filtrer', and 'Safesearch configuration'. The main panel shows the current version '05-10-2022 16:03:51' and buttons for 'Télécharger la dernière version' and 'Init Catégories'. Status messages indicate that the Toulouse blacklist update and the default Privoxy filtering are active, with 'Désactiver' buttons for each. The core section, 'Choisir les catégories filtrées à appliquer.', contains a grid of 32 categories, each with a checkbox. Most are checked, including 'adult', 'adultsearchengine', 'agressif', 'associations_religieuses', 'astrology', 'financial', 'forums', 'gambling', 'games', 'hacking', 'special', 'audio-video', 'bitcoin', 'blog', 'celebrity', 'cryptojacking', 'malware', 'manga', 'marketingware', 'mixed_adult', 'mobile-phone', 'strong_redirector', 'ct_doh_dot_doq', 'ctparental', 'dangerous_material', 'dating', 'ddos', 'phishing', 'press', 'publicite', 'radio', 'reaffected', 'warez', 'dialer', 'doh', 'drogue', 'exceptions_liste_bu', 'filehosting', 'redirector', 'sect', 'shopping', 'shortener', and 'social_networks'.

CTparental DNS filtering — Mozilla Firefox

CTparental DNS filtering x +

https://admin.ct.local/index.php?dgfile=Blacklist filtering

filtrage web Le filtrage de noms de domaine est actuellement activé ✓

Désactiver le filtrage Déconnexion

Filtrage par BlackList

Version actuelle : 05-10-2022 16:03:51

Télécharger la dernière version Init Catégories

La mise à jour de la blacklist de Toulouse tous les 7 jours est activée ✓

Désactiver

Le filtrage par défaut de Privoxy est activé. ✓

Désactiver

Basculer en Whitelist

Choisir les catégories filtrées à appliquer.

<input checked="" type="checkbox"/> adult	<input type="checkbox"/> audio-video	<input type="checkbox"/> ct_doh_dot_doq	<input type="checkbox"/> dialer
<input checked="" type="checkbox"/> adultsearchengine	<input checked="" type="checkbox"/> bitcoin	<input checked="" type="checkbox"/> ctparental	<input checked="" type="checkbox"/> doh
<input checked="" type="checkbox"/> agressif	<input type="checkbox"/> blog	<input checked="" type="checkbox"/> dangerous_material	<input checked="" type="checkbox"/> drogue
<input type="checkbox"/> associations_religieuses	<input type="checkbox"/> celebrity	<input checked="" type="checkbox"/> dating	<input type="checkbox"/> exceptions_liste_bu
<input type="checkbox"/> astrology	<input checked="" type="checkbox"/> cryptojacking	<input checked="" type="checkbox"/> ddos	<input type="checkbox"/> filehosting
<input type="checkbox"/> financial	<input checked="" type="checkbox"/> malware	<input checked="" type="checkbox"/> phishing	<input checked="" type="checkbox"/> redirector
<input type="checkbox"/> forums	<input type="checkbox"/> manga	<input type="checkbox"/> press	<input checked="" type="checkbox"/> sect
<input checked="" type="checkbox"/> gambling	<input checked="" type="checkbox"/> marketingware	<input checked="" type="checkbox"/> publicite	<input type="checkbox"/> shopping
<input type="checkbox"/> games	<input checked="" type="checkbox"/> mixed_adult	<input type="checkbox"/> radio	<input type="checkbox"/> shortener
<input checked="" type="checkbox"/> hacking	<input type="checkbox"/> mobile-phone	<input type="checkbox"/> reaffected	<input type="checkbox"/> social_networks
<input type="checkbox"/> special	<input checked="" type="checkbox"/> strong_redirector	<input checked="" type="checkbox"/> warez	

CTparental DNS filtering — Mozilla Firefox

CTparental DNS filtering x +

https://admin.ct.local/index.php?dfile=Blacklist filtering

CTparental DNS fit...

filtrage web Le filtrage de noms de domaine est actuellement activé ✓

Désactiver le filtrage Déconnexion

filtrage par BlackList

extensions à filtrer

type MIME à filtrer

*ip **ips ...

Groupe privilégié

Safesearch configuration

Heures de connexion autorisées

special strong_redirector warez

sports tor_nodes

stalkerware tricheur

steven_black ultrasurf_nodes

strict_redirector vpn

Noms de domaine, adresses ip ou réseaux réhabilités

1-Entrez ici des noms de domaine, adresses ip ou réseaux bloqués par la liste noire que vous souhaitez réhabiliter. Entrez un nom de domaine, adresse ip ou réseau par ligne (exemple : .domain.org ou 10.0.0.0/24 ou 2001::32)

Noms de domaine, adresses ip ou réseaux filtrés

Entrez un nom de domaine, adresse ip ou réseau par ligne (exemple : .domain.org ou 10.0.0.0/24 ou 2001::32)

http://fr-fr.facebook.com/
http://twitter.com/?lang=fr
http://www.google.fr/
http://www.bing.com

Enregistrer les modifications Une fois validées, 30 secondes sont nécessaires pour traiter vos modifications

Activer la liste de Toulouse, écrire dans la liste noire les sites indésirables, Google, Facebook, Twitter, Bing ... valider

Configuration de e2guardian

CTparental DNS filtering — Mozilla Firefox

CTparental DNS filtering x +

https://admin.ct.local/index.php?dfile=extensions to be filtered

CTparental DNS fit...

filtrage web Le filtrage de noms de domaine est actuellement activé ✓

Désactiver le filtrage Déconnexion

filtrage par BlackList

extensions à filtrer

type MIME à filtrer

*ip **ips ...

Groupe privilégié

Safesearch configuration

Heures de connexion autorisées

Configuration de e2guardian

Sélectionnez les extensions à filtrer

Attention ce filtre ne fonctionne qu'avec les sites en HTTP (connexion non chiffrée) mais pas avec les sites en HTTPS (connexion chiffrée entre le site web et l'utilisateur).

/etc/e2guardian/lists/bannedextensionlist

Select all

Unselect all

.ade # Microsoft Access project extension .cab # Windows setup file

.adp # Microsoft Access project .chm # Compiled HTML Help file

.asx # Windows Media Audio / Video .cmd # Microsoft Windows NT Command script

.bas # Microsoft Visual Basic class module .com # Microsoft MS-DOS program

.bat # Batch file .cpl # Control Panel extension

.cert # Security certificate .hta # HTML program

.dll # Windows system file .inf # Setup Information

.exe # Program .ins # Internet Naming Service

.hlp # Help file .isp # Internet Communication settings

.ini # Windows system file .js # JavaScript file - often needed in web pages

.jse # Jscript Encoded Script file - often needed in web pages .mdt # Microsoft Access workgroup information

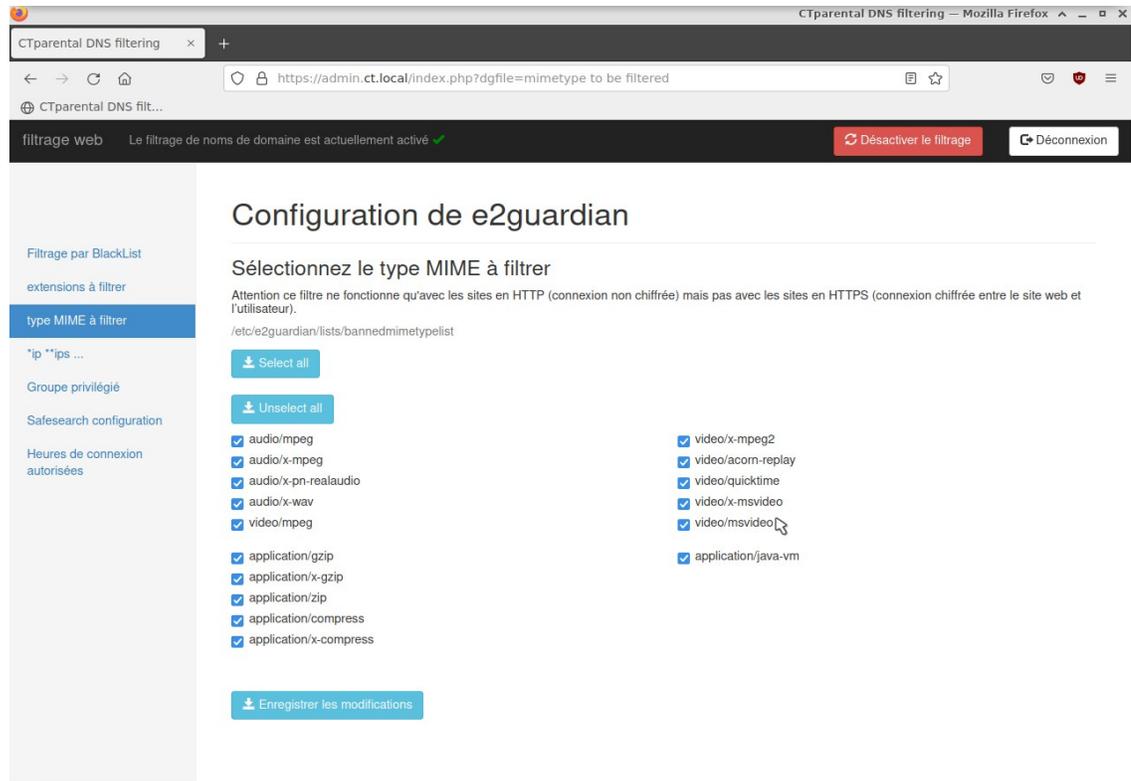
.lnk # Windows Shortcut .mdw # Microsoft Access workgroup information

.mda # Microsoft Access add-in program .mdz # Microsoft Access wizard program

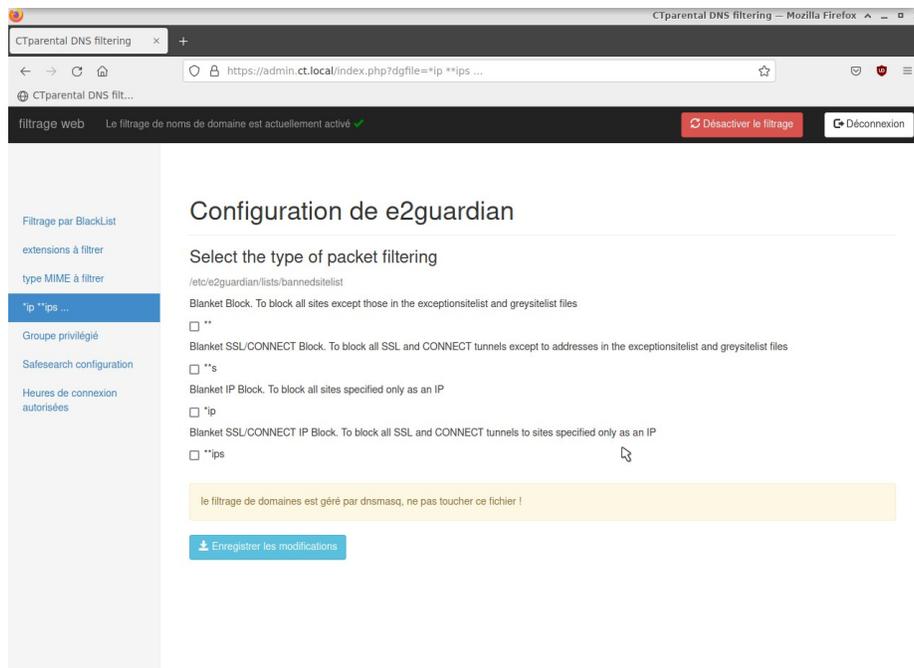
.mdb # Microsoft Access program .msc # Microsoft Common Console document

.mde # Microsoft Access MDF database .msi # Microsoft Windows Installer package

Filtrage Par extensions et par type MIME

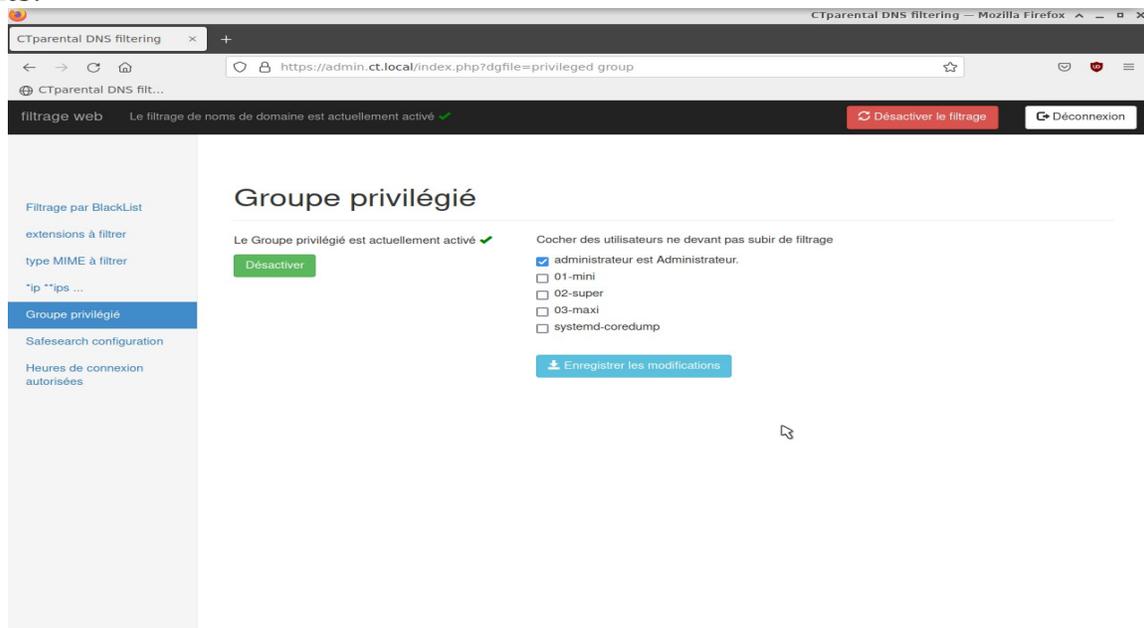


Filtrage IP



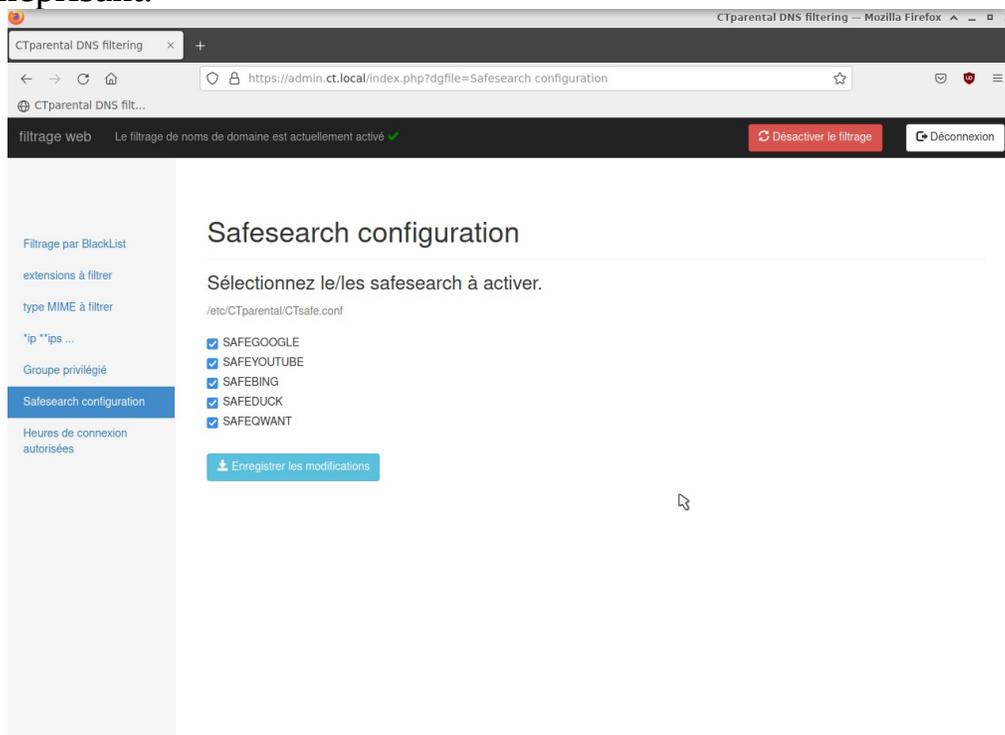
Groupe privilégié

Administrateur → aucun filtre, c'est l'enseignant ou le parent qui gère l'ordinateur ; la session est protégée par un mot de passe, à ne pas divulguée aux enfants.



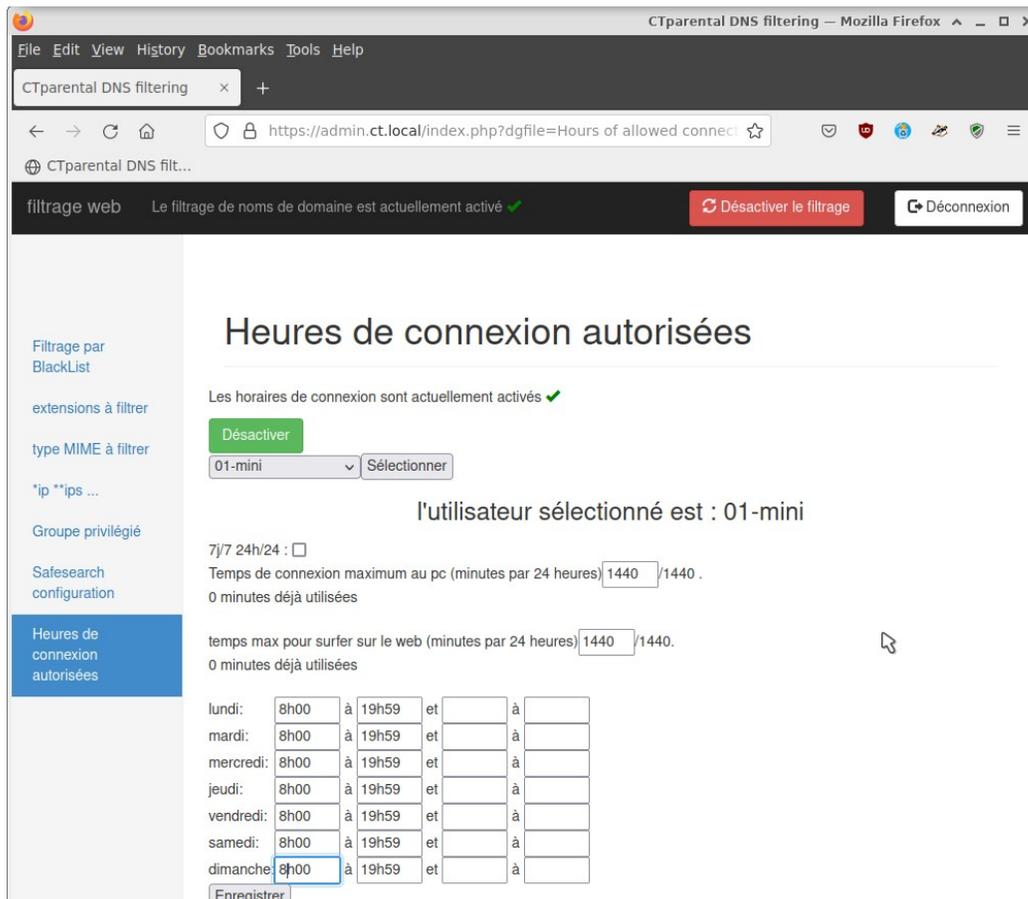
SafeSearch configuration

Autre possibilité de filtrage, CTparental permet d'activer la fonctionnalité SafeSearch de Google, mais aussi de Bing, DuckDuckGo et Qwant. Il s'agit d'une fonctionnalité visant à filtrer les résultats explicites en terme de pornographie et de contenu méprisant.



Horaires de connexion

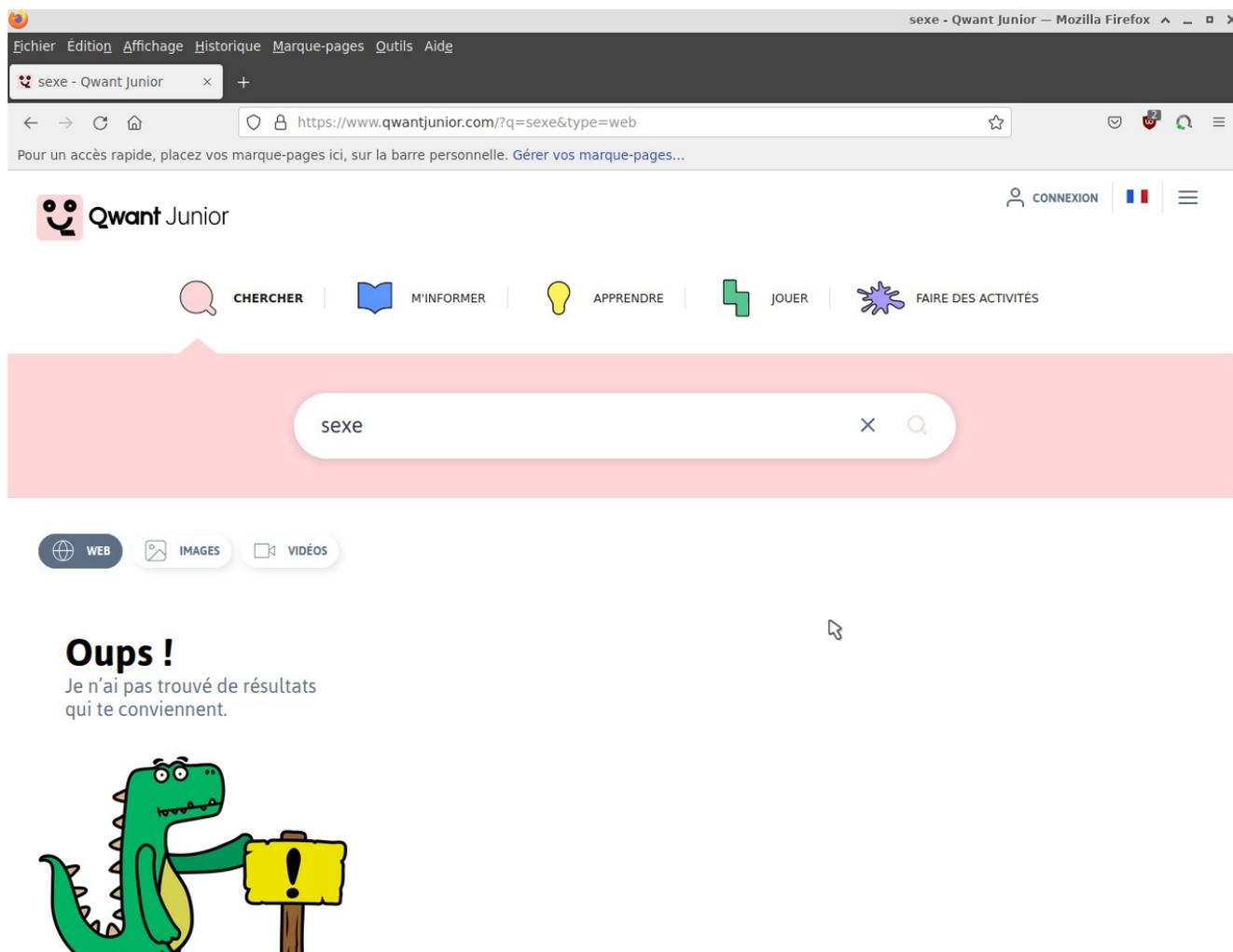
On peut programmer le réglage des heures de connexion (et donc le temps passé sur Internet), et ce jour par jour à la maison... A l'école, on peut régler selon les jours de classes et les horaires de la garderie. Le réglage se fait utilisateur par utilisateur ce qui permet par exemple d'accorder des horaires différents pour enfants d'âges différents.



Redémarrer l'ordinateur

Voir si cela fonctionne. Si on a accès à l'interface sur les bureaux enfants.

Le filtrage est effectif avec un avis de domaine bloqué sur les recherches interdites.



L'accès Internet non filtré doit fonctionner dans la session administrateur.

Biographie

message de Philippe sur le Forum de Primtux

<https://forum.primtux.fr/showthread.php?tid=1244&pid=14341#pid14341>

<https://gitlab.com/ctparentalgroup/CTparental>

<https://gitlab.com/ctparentalgroup/CTparental/-/wikis/home>

Remarque :

J'aimerais que le développeur de ce logiciel prenne en compte également le **https**, puisque de nos jours, nombreux sites débutent leurs adresses ainsi.

--

Ledatux 27, Rue de la Mairie 47300-Lédat

Club informatique - Mardi et Samedi de 9 à 12 h, Jeudi de 20 à 22 h

05 53 40 83 83

courriel → ledatux@netcourrier.com>

<https://www.pari47.fr/ledatux/>

<http://www.net1901.org/association/LEDATUX,871303.html>