Val de Marne
Le Département

CONTRÔLE PARENTAL

Procédure et guide d'utilisation à destination des familles
Ordinateur Ordival

Document mis à jour le 01/08/2026.

Ce guide est également consultable en ligne, dans sa version la plus récente : https://www.econocom.com/fr/lp/sav-pc-94-collegiens.

Sommaire

1 Qu'est-ce qu'un logiciel de contrôle parental ?
2 Conseils aux familles avant utilisation
3 Le contrôle parental sur Ordival
4 Prise en main du tableau de bord SafeDNS
5 Gérer les politiques de filtrage
6 Configurer les paramètres de filtrage
7 Listes d'autorisation et de blocage
8 Sécuriser la navigation
9 Limiter les horaires d'utilisation
10 Consulter les statistiques
11 Questions fréquentes (FAQ)

1. Qu'est-ce qu'un logiciel de contrôle parental ?

Un logiciel de contrôle parental permet d'encadrer l'usage qu'un enfant fait d'un ordinateur. Il se paramètre librement, en fonction des limites que vous souhaitez fixer.

Il permet notamment :

- La limitation des horaires d'utilisation de l'ordinateur ;
- La limitation de l'accès aux applications ;
- La maîtrise de l'accès aux sites Internet (filtrage) ;
- La gestion des listes d'autorisation et de blocage ;
- La sécurisation de la navigation (SafeSearch et mode restreint de YouTube) ;
- La consultation des sites Internet et des logiciels installés consultés.

Le mode d'emploi détaillé de l'outil de contrôle parental est présenté dans les pages suivantes.

2. Conseils aux familles avant utilisation

Avant de configurer un logiciel de contrôle parental, quelques principes simples permettent d'en tirer le meilleur parti.

2.1 En parler avec son enfant

En complément de l'utilisation d'un logiciel de contrôle parental, il convient d'expliquer à vos enfants quelles sont les règles de navigation sur Internet et les risques auxquels ils pourraient être exposés. Ce type de logiciel doit seulement être considéré comme un outil d'aide pour l'éducation aux médias.

2.2 Adapter les réglages à l'âge de chaque enfant

Si vous avez des enfants d'âge différent, vous pourrez créer des comptes différents pour chaque enfant afin de personnaliser au mieux leur accès à l'ordinateur et à Internet (un enfant de 11 ans n'a pas les mêmes besoins et usages qu'un enfant de 15 ans). Il faut aussi que vous-même puissiez utiliser l'ordinateur sans être gêné par le contrôle parental.

2.3 Autres logiciels et ressources utiles

CONSEIL AU FILTRAGE

Aujourd'hui, tous les Fournisseurs d'Accès à Internet (FAI) ainsi que de nombreux éditeurs proposent un logiciel de contrôle parental. Vous en trouverez une présentation et un comparatif sur www.e-enfance.org
Ils vous proposent des listes blanches et noires constituées, auxquelles vous pourrez ajouter des sites Internet ou en supprimer.
Vous disposez également d'une aide pour mettre en place le contrôle pour chaque enfant.

CONSEIL CLASSIFICATION VIDEO / JEUX VIDEO

Pour en savoir plus sur la classification des jeux vidéo : www.pegi.info

LUTTE CONTRE LE HARCELEMENT ET LES VIOLENCE NUMERIQUE

> L'Association e-Enfance (www.e-enfance.org) opère le numéro national **3018** qui accompagne et prend en charge les jeunes victimes de harcèlement et de violences numériques et conseille sur la parentalité numérique.

3. Le contrôle parental sur Ordival

L'ordinateur Ordival est équipé du logiciel de contrôle parental, édité par SafeDNS. Ce système offre de multiples possibilités de personnalisation.

3.1 Fixer des limites horaires

Vous pouvez :

- Limiter les horaires d'ouverture de la session « Collégien » ;
- Limiter le temps d'accès à Internet.

En cas de dépassement de ces limites, la session de votre enfant se ferme automatiquement avec une alerte d'information s'affiche 5 minutes avant la déconnexion.

Interdire l'accès aux sites sensibles du web

Le contrôle parental permet de bloquer l'accès aux sites déconseillés ou choquants pour les enfants. Il ne remplace toutefois jamais la vigilance et les mises en garde : aucun outil ne peut garantir un blocage à 100 %.

Les différents niveaux de blocage permettent de :

- Définir une liste blanche de sites autorisés et une liste noire de sites interdits ;
- Contrôler l'accès aux sites selon des catégories autorisées ou interdites ;
- Bloquer ou autoriser les téléchargements et d'autres usages.

Ces restrictions s'appliquent également aux différents moteurs de recherche.

> **IMPORTANT**
> Les outils de contrôle parental aident à protéger les enfants en ligne, mais ne dispensent pas d'un dialogue régulier avec votre enfant sur ses usages numériques.

3.2 Paramétrage par défaut de l'ordinateur confié

L'ordinateur qui vous est confié est pré-paramétré : votre enfant est protégé de la manière suivante sur la session « Collégien » :

- Catégories bloquées : pornographie, violence, propos polémiques, jeux d'argent, armes, drogues/alcool/tabac, jeux -18, anorexie, rencontres, sectes, piratage, réseaux sociaux, enchères ;
- Utilisation de l'ordinateur autorisée de 7 h à 21 h (22 h les vendredis et samedis).

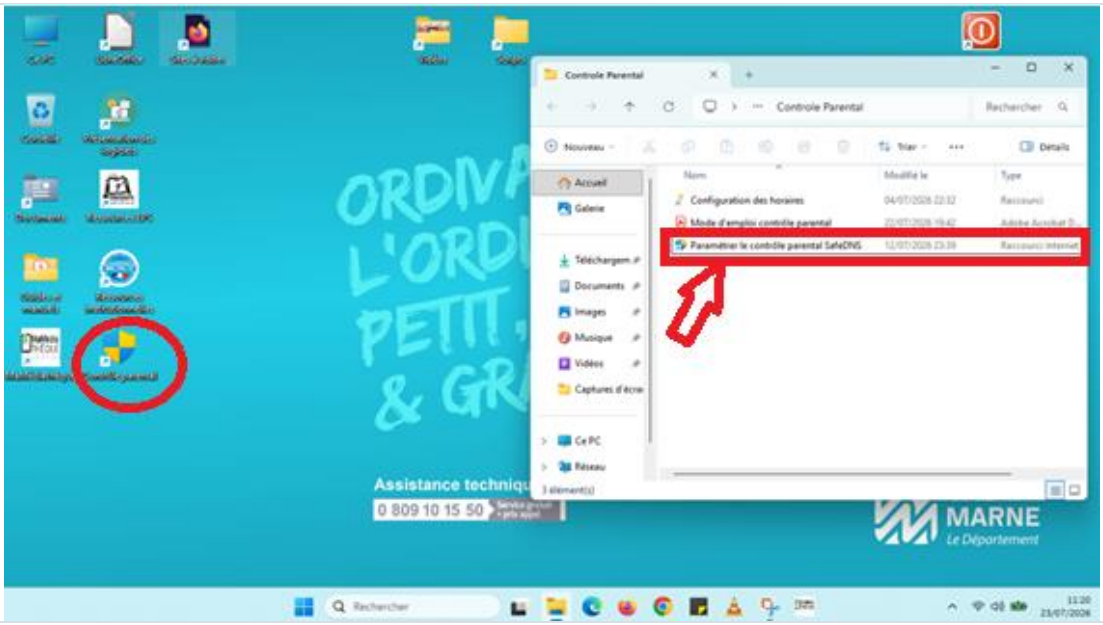
L'ensemble de ces paramètres, et bien d'autres, restent modifiables à tout moment. Les pages suivantes expliquent comment personnaliser le contrôle parental.

4. Prise en main du tableau de bord SafeDNS

4.1 Ouvrir le contrôle parental

1. Allumez l'ordinateur.

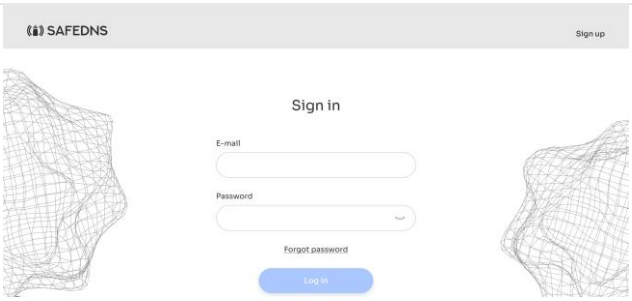
2. Ouvrez la session « Parents ».
3. Sur le bureau, ouvrez le dossier « Contrôle parental ».
4. Cliquez sur l'icône « Paramétrer le contrôle parental ».



Ouverture du dossier « Contrôle parental »

4.2 Se connecter au tableau de bord SafeDNS

En cliquant sur « Paramétrer le contrôle parental », le tableau de bord SafeDNS s'ouvre et donne accès aux paramètres de filtrage et de gestion du contrôle parental :



1. Saisissez votre identifiant dans le champ E-mail : CD94_suivi du numéro de série de votre ordinateur.
2. Le numéro de série (SN) figure sur l'étiquette collée sous le capot de l'ordinateur. Il commence généralement par « PW0 »



3. Saisissez le mot de passe :

   le numéro de série de votre ordinateur suivi de_valdemarne / exemple : PWONF1CF_valdemarne

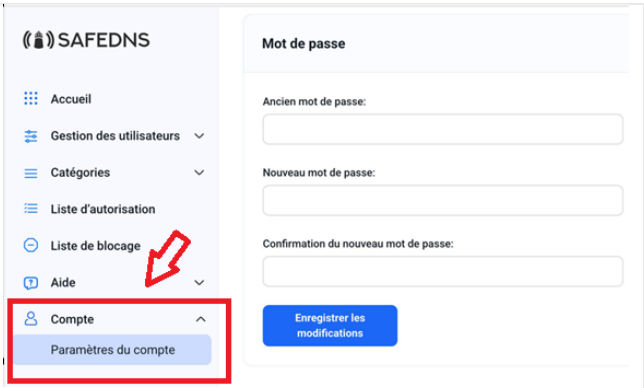
4. Cliquez sur « Log in ».

À NOTER

Le tableau de bord SafeDNS est également accessible depuis tout autre appareil connecté à Internet (ordinateur, smartphone, tablette) à l'aide des mêmes identifiants de connexion.

4.3 Modifier le mot de passe après la première connexion

Le mot de passe fourni est temporaire. Pour garantir la sécurité de votre compte, il est recommandé de le modifier dès la première connexion.



1. Accédez à « Compte » puis « Paramètres du compte ».
2. Faites défiler la page jusqu'à la section « Mot de passe ».
3. Saisissez votre mot de passe actuel.
4. Renseignez votre nouveau mot de passe.
5. Confirmez le nouveau mot de passe.
6. Cliquez sur « Enregistrer » pour valider la modification.

IMPORTANT

Toute personne disposant des identifiants du tableau de bord SafeDNS peut modifier les paramètres de filtrage et de protection. Conservez votre mot de passe confidentiel.

4.4 Mot de passe oublié

En cas d'oubli de votre mot de passe, contactez le service client pour en demander la réinitialisation.

Contacter l'assistance technique :

08 09 10 15 50 *(prix d'un appel local)*

Horaires : du lundi au vendredi de 8 h à 20 h, le samedi de 8 h à 16 h (hors jours fériés).

5. Gérer les politiques de filtrage

La maîtrise de l'accès aux sites Internet (filtrage).

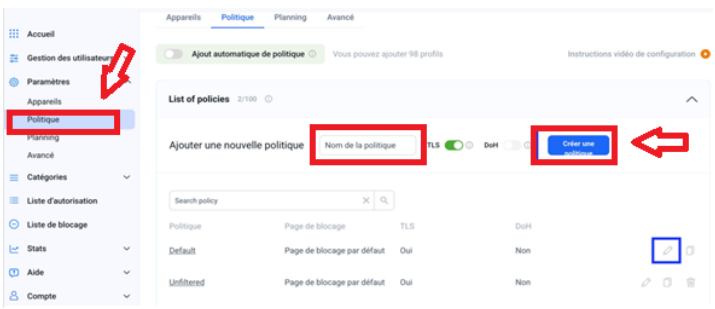
Une politique de filtrage définit les sites Internet autorisés ou bloqués pour votre enfant. Le compte est fourni avec deux politiques :

- **Default** — politique de filtrage standard, appliquée à la session « Collégien ».
- **Unfiltered** — politique sans filtrage, destinée à la session « Parent ».

Vous pouvez modifier la politique Default ou créer d'autres politiques adaptées à vos besoins.

> **IMPORTANT**
> La politique Unfiltered est réservée à la session « Parent ». Ne la modifiez et ne la supprimez pas, sauf si vous souhaitez restreindre l'accès Internet de cette session.

5.1 Créer ou modifier une politique de filtrage

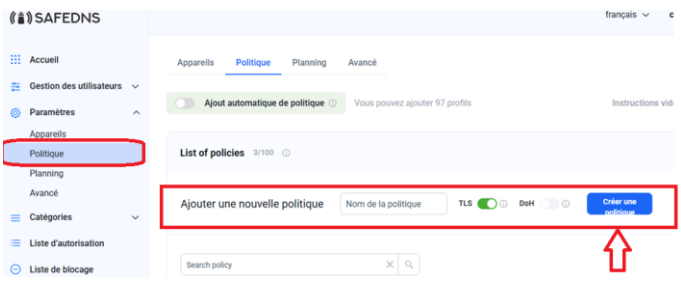


1. Ouvrez la section « Politiques » dans le tableau de bord SafeDNS.
2. Pour modifier une politique existante, cliquez sur l'icône crayon ✎ située à droite de celle-ci.
3. Pour créer une nouvelle politique, saisissez son nom dans le champ prévu à cet effet.
4. Cliquez sur « Créer une politique ».

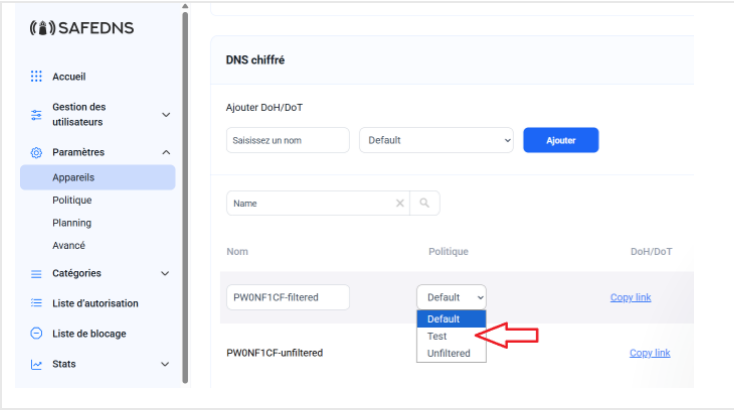
5.2 Attribuer une politique de filtrage

Pour personnaliser le filtrage de la session Collégien, créez une politique de filtrage puis attribuez-la à la session concernée afin que ses paramètres prennent effet.

Comment attribuer une politique ?



1. Accédez à « Paramètres », puis sélectionnez « Politiques ».
2. Saisissez le nom de la nouvelle politique, puis cliquez sur « Créer ».



3. Appliquez ensuite la politique créée à la session Collégien : sélectionnez l'appareil **<numéro de série>-filtered**, l'appareil filtré utilisé pour le compte « Collégien ».

À noter :

- **Modifier une politique** : changer ses règles de filtrage.
- **Attribuer une politique** : associer la session à une politique personnalisée afin de déterminer les règles de filtrage qui lui seront appliquées.

6. Configurer les paramètres de filtrage

Le contrôle parental SafeDNS classe les paramètres de filtrage en trois rubriques :

- **Catégories** : autoriser ou bloquer des catégories de sites Internet.
- **AppBlocker** : gérer l'accès à certaines applications.
- **Sécurité** : renforcer la protection contre les sites malveillants.

IMPORTANT

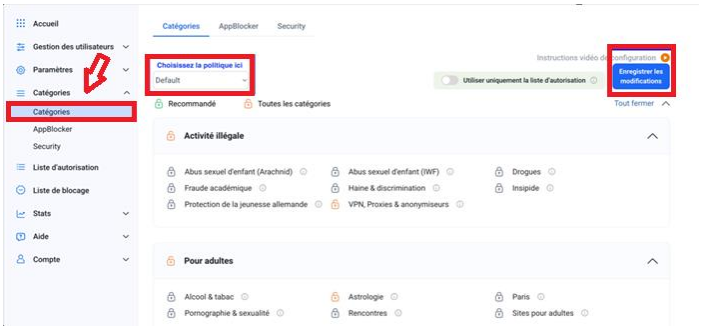
Les modifications s'appliquent uniquement à la politique sélectionnée. Les autres politiques ne sont pas modifiées.

6.1 Les catégories

Les catégories de contenu permettent de filtrer les sites Internet en fonction de leur thème. Parmi les principales catégories disponibles :

- Sites pour adultes ;
- Haine et discrimination ;
- Drogues, alcool et tabac ;
- Rencontres, réseaux sociaux et jeux ;
- VPN, proxys et outils d'anonymisation.

Comment modifier les catégories de contenu ?



1. Ouvrez la section « Catégories ».
2. Sélectionnez la politique que vous souhaitez modifier.
3. Autorisez ou bloquez les catégories selon vos besoins.
4. Cliquez sur « Enregistrer les modifications ».

IMPORTANT

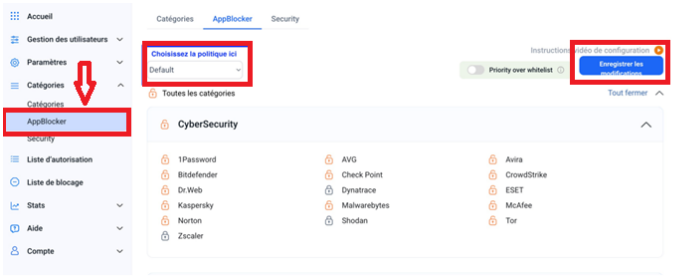
Activez uniquement les catégories que vous souhaitez bloquer, afin d'adapter le niveau de protection à l'âge et aux besoins de votre enfant.

6.2 AppBlocker

AppBlocker permet de contrôler l'accès à certaines applications et services en ligne, indépendamment des catégories de sites Internet. Vous pouvez notamment autoriser ou bloquer :

- Les applications de réseaux sociaux ;
- Les services de messagerie ;
- Les jeux en ligne ;
- Les plateformes de streaming vidéo ou musical.

Comment configurer AppBlocker ?



1. Ouvrez la section « AppBlocker ».
2. Sélectionnez la politique que vous souhaitez modifier.
3. Autorisez ou bloquez les applications et services selon vos besoins.
4. Cliquez sur « Enregistrer les modifications ».

IMPORTANT

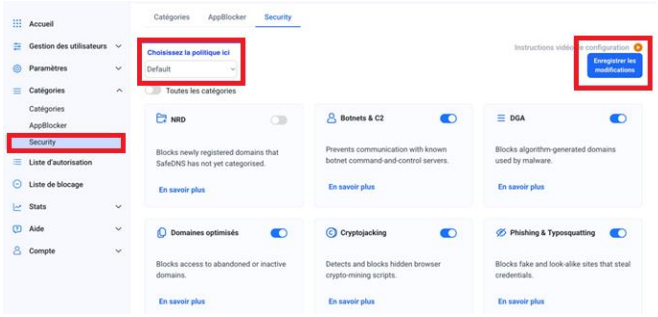
AppBlocker permet de limiter l'accès à certaines applications même si les sites Internet associés ne sont pas bloqués par les catégories de contenu.

6.3 Catégories de sécurité

Les catégories de sécurité protègent l'ordinateur contre les principales menaces informatiques, notamment :

- Les logiciels malveillants (malwares) ;
- Les téléchargements malveillants ;
- Les tentatives de phishing (vol d'informations personnelles) ;
- Les botnets (réseaux d'ordinateurs infectés contrôlés à distance) ;
- Les autres menaces de cybersécurité.
- Toutes ces catégories doivent normalement rester bloquées.

Comment configurer les catégories de sécurité ?



1. Ouvrez la section « Security ».
2. Sélectionnez la politique concernée.
3. Bloquez ou débloquez les catégories nécessaires.
4. Cliquez sur « Enregistrer les modifications ».

IMPORTANT

Il est fortement recommandé de laisser toutes les catégories de sécurité bloquées, afin de garantir une protection optimale de l'ordinateur et des données de votre enfant.

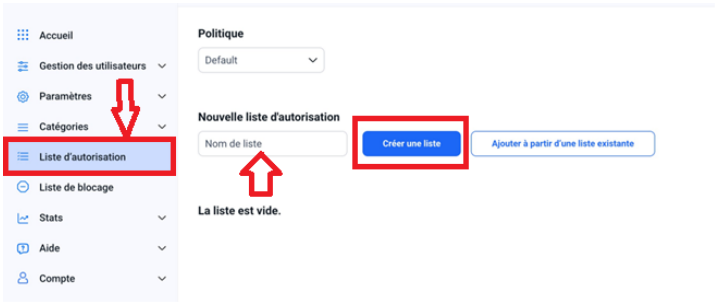
7. Listes d'autorisation et de blocage

Les listes d'autorisation et de blocage permettent de créer des exceptions aux règles de filtrage :

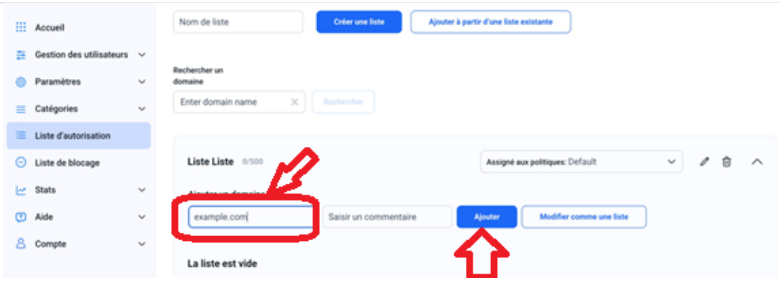
- La liste d'autorisation permet d'autoriser l'accès à des sites Internet spécifiques ;
- La liste de blocage permet de bloquer l'accès à des sites Internet spécifiques.

Exemple : si la catégorie Réseaux sociaux est bloquée, vous pouvez tout de même autoriser un réseau social précis en l'ajoutant à la liste d'autorisation.

7.1 Autoriser un site web



1. Ouvrez la section « Liste d'autorisation ».
2. Si aucune liste n'existe, saisissez un nom dans le champ prévu à cet effet, puis cliquez sur « Créer une liste ».



3. Ajoutez des domaines à la liste créée, puis cliquez sur « Ajouter ».

IMPORTANT

Saisissez uniquement le nom de domaine du site, au format exemple.fr, et non l'adresse complète d'une page telle que exemple.fr/page-specifique.

7.2 Bloquer un site web

4. Recherchez le domaine dans la liste existante.
5. Cliquez sur l'icône de la corbeille, à droite, pour le supprimer.

8. Sécuriser la navigation

Le contrôle parental SafeDNS propose deux fonctions complémentaires : la recherche sécurisée (SafeSearch) et le mode restreint de YouTube.

8.1 Activer la recherche sécurisée (SafeSearch)

La recherche sécurisée (SafeSearch) permet de limiter l'affichage de contenus explicites dans les résultats des moteurs de recherche.

Comment activer SafeSearch ?

1. Ouvrez la section « Paramètres > Avancé ».
2. Sélectionnez la politique que vous souhaitez modifier.
3. Activez l'option « Forcer la recherche sécurisée ».
4. Cliquez sur « Enregistrer les modifications ».

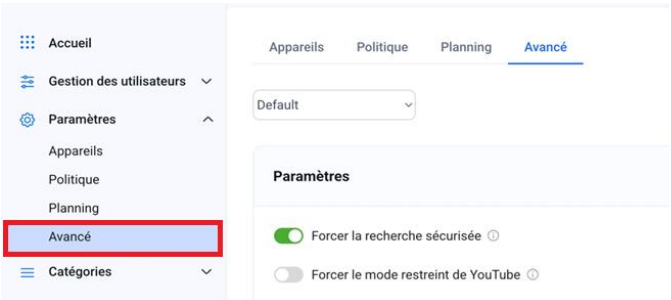
IMPORTANT

SafeSearch renforce la sécurité des résultats de recherche, mais ne remplace pas le filtrage des sites Internet par catégories.

8.2 Mode restreint YouTube

Le mode restreint de YouTube permet de limiter l'accès aux vidéos susceptibles d'être inadaptées aux mineurs.

Comment activer le mode restreint YouTube ?



1. Ouvrez la section « Paramètres > Avancé ».
2. Sélectionnez la politique que vous souhaitez modifier.
3. Activez l'option « Forcer le mode restreint de YouTube ».
4. Cliquez sur « Enregistrer les modifications ».

IMPORTANT

Ce mode ne bloque pas totalement l'accès à YouTube. Pour en bloquer l'accès, utilisez AppBlocker, bloquez la catégorie Films et vidéos, ou ajoutez les domaines de YouTube à une liste de blocage.

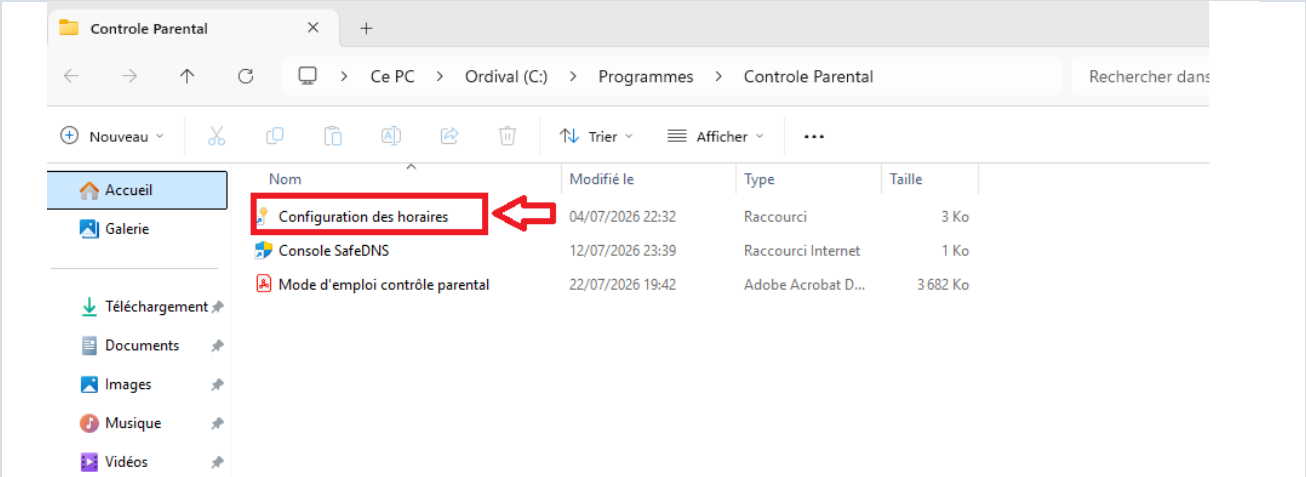
9. Limiter les horaires d'utilisation de l'ordinateur

9.1 Limitation de l'accès à la session

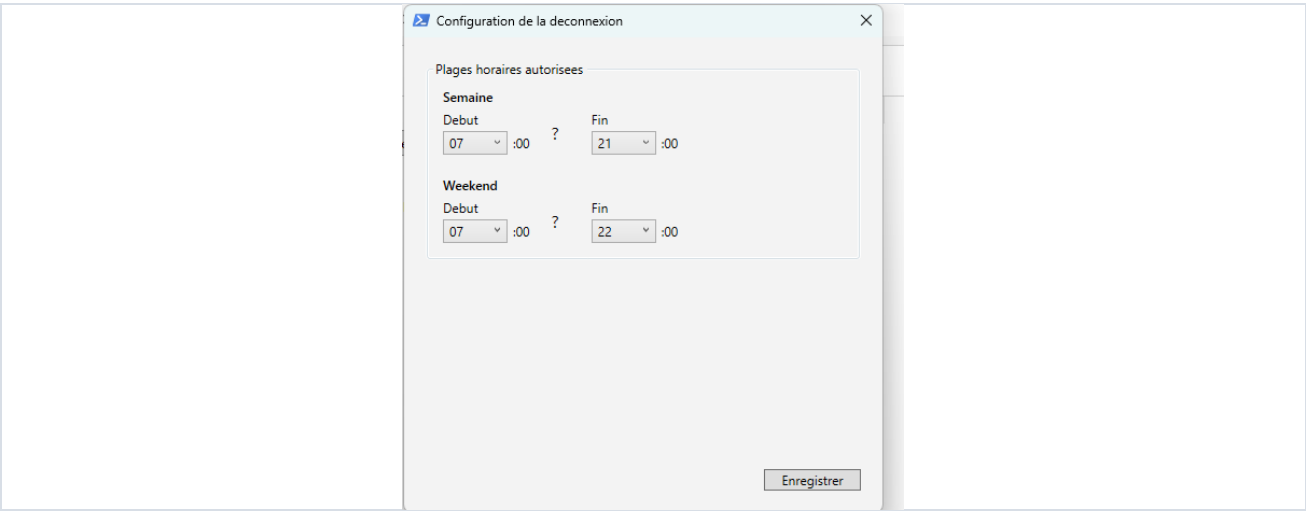
Fonctionnalité native au PC Ordival en dehors de la solution SafeDNS.
Par défaut, l'accès à la session “Collégien” est autorisé aux horaires suivants :

- **Du lundi au vendredi** : de 07 h 00 à 21 h 00.
- **Le week-end** : de 07 h 00 à 22 h 00.

Pour modifier ces horaires, utilisez l'outil « Configuration des horaires », disponible dans le dossier Contrôle parental sur le Bureau



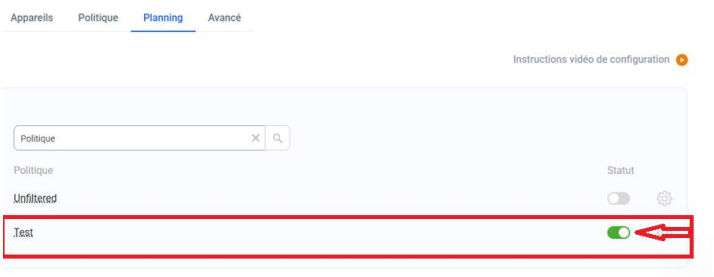
Pour les étendre ou les restreindre, modifiez la plage horaire puis enregistrez.



9.2 Limitation de la connexion à Internet

Une politique par défaut est déjà mise en place. Vous pouvez toutefois personnaliser le planning et le configurer selon vos besoins avec la solution SafeDNS

Comment créer un planning de plage horaire de connexion ?

<table>
<tr>
<td>
</td>
<td>1. Activez le planning sur la politique de filtrage souhaitée.</td>
</tr>
<tr>
<td>
</td>
<td>2. Sélectionnez les jours et les plages horaires souhaités,
3. Cliquez sur « Enregistrer ».</td>
</tr>
</table>

IMPORTANT

Vous devez sélectionner une politique de filtrage différente de « Default » pour pouvoir appliquer un planning.

Cette politique doit ensuite être attribuée à la session concernée afin que le planning soit pris en compte.

Pendant les plages horaires définies, le contrôle parental SafeDNS applique la politique de filtrage associée au planning. En dehors de ces plages, la politique Default est automatiquement appliqué.

N'attribuez jamais une politique de filtrage destinée à la session Collégien à l'appareil , réservé à la session Parent, afin de préserver un accès Internet non filtré pour les familles.

10. Consulter les statistiques dans le tableau de bord

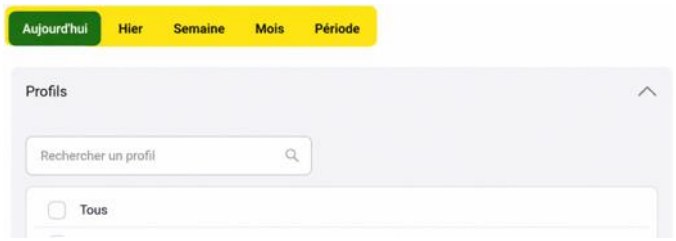
La section Stats présente l'activité Internet détectée sur la session « Collégien » protégée. Elle permet notamment de consulter :

- Les types de sites et de services en ligne sollicités ;
- Les requêtes bloquées par SafeDNS ;
- Les menaces de sécurité détectées et bloquées.

À NOTER

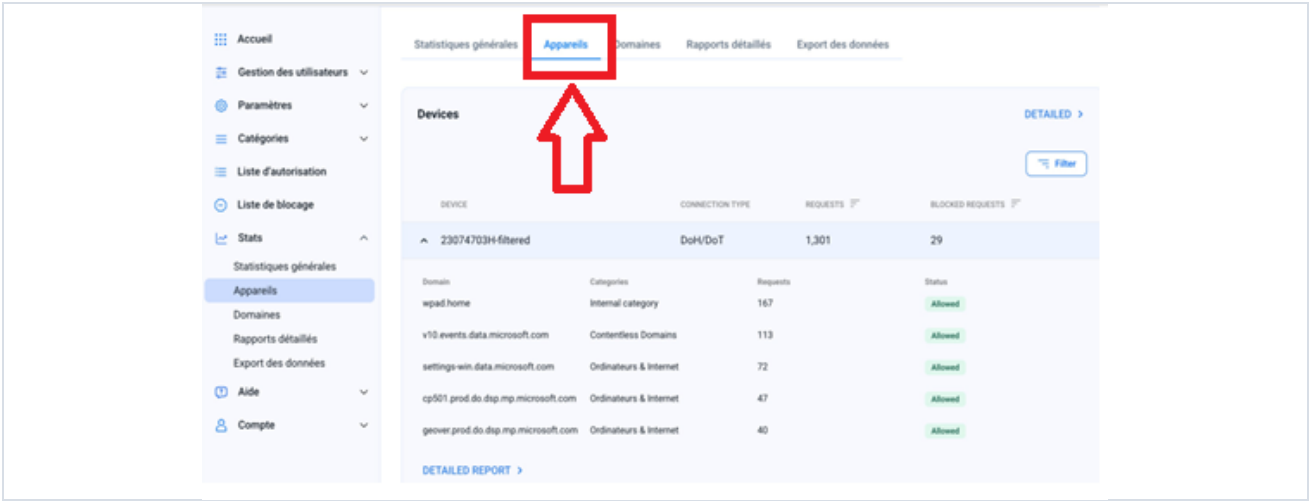
Le contrôle parental SafeDNS enregistre les demandes d'accès aux noms de domaine, et non les pages exactes consultées ni les informations saisies par l'utilisateur.

10.1 Statistiques générales

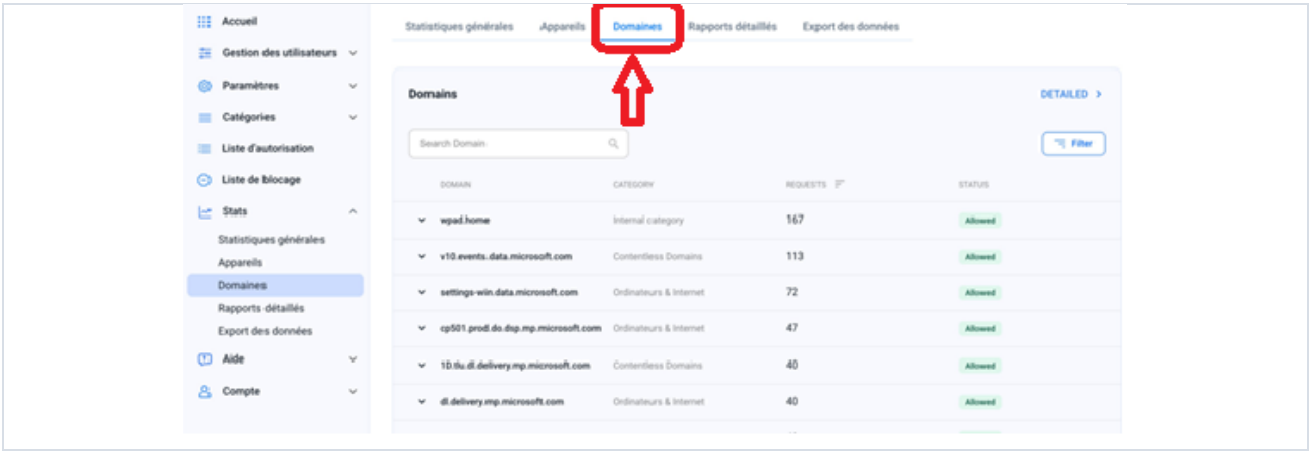
<table>
<tr>
<td>
</td>
<td>1. Ouvrez la section « Stats », puis sélectionnez « Statistiques générales ».
2. Dans la liste déroulante « Filter », choisissez le filtre que vous souhaitez appliquer.</td>
</tr>
<tr>
<td>
</td>
<td>3. Choisissez la période à afficher : Aujourd'hui (jour en cours), Hier (veille), Semaine (7 derniers jours), Mois (30 derniers jours) ou Période (période personnalisée avec date de début et de fin).
4. Dans « Profiles », sélectionnez une ou plusieurs politiques de filtrage afin de limiter le rapport aux politiques souhaitées.
5. Dans « Devices », sélectionnez l'appareil <numéro de série>-filtered pour afficher les statistiques de la session « Collégien ».
6. Cliquez sur « Show » pour afficher les résultats.</td>
</tr>
</table>

10.2 Statistiques détaillées

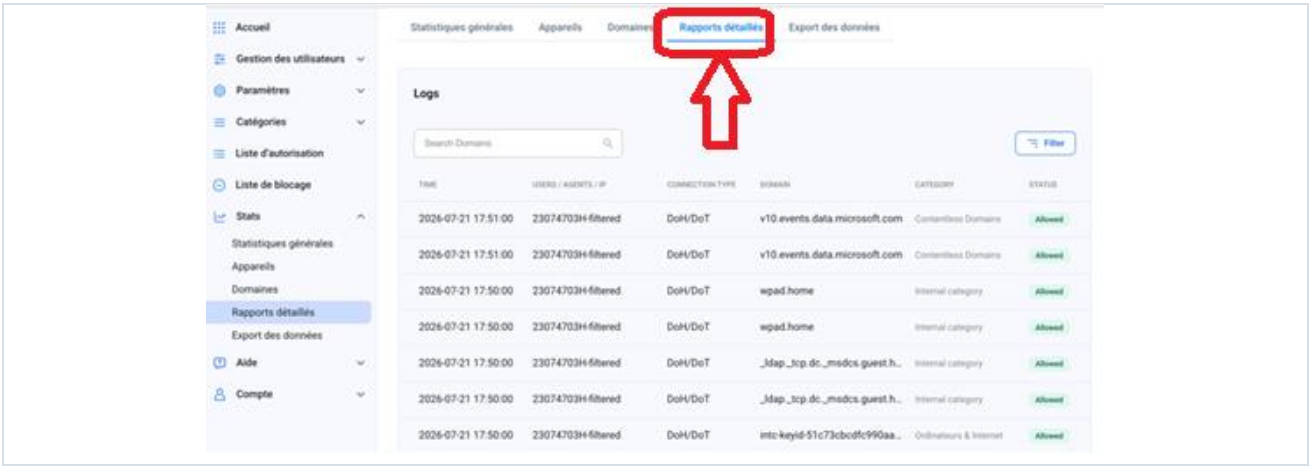
Par appareils : cliquez sur « Appareils ».



Par domaines : cliquez sur « Domaines ».

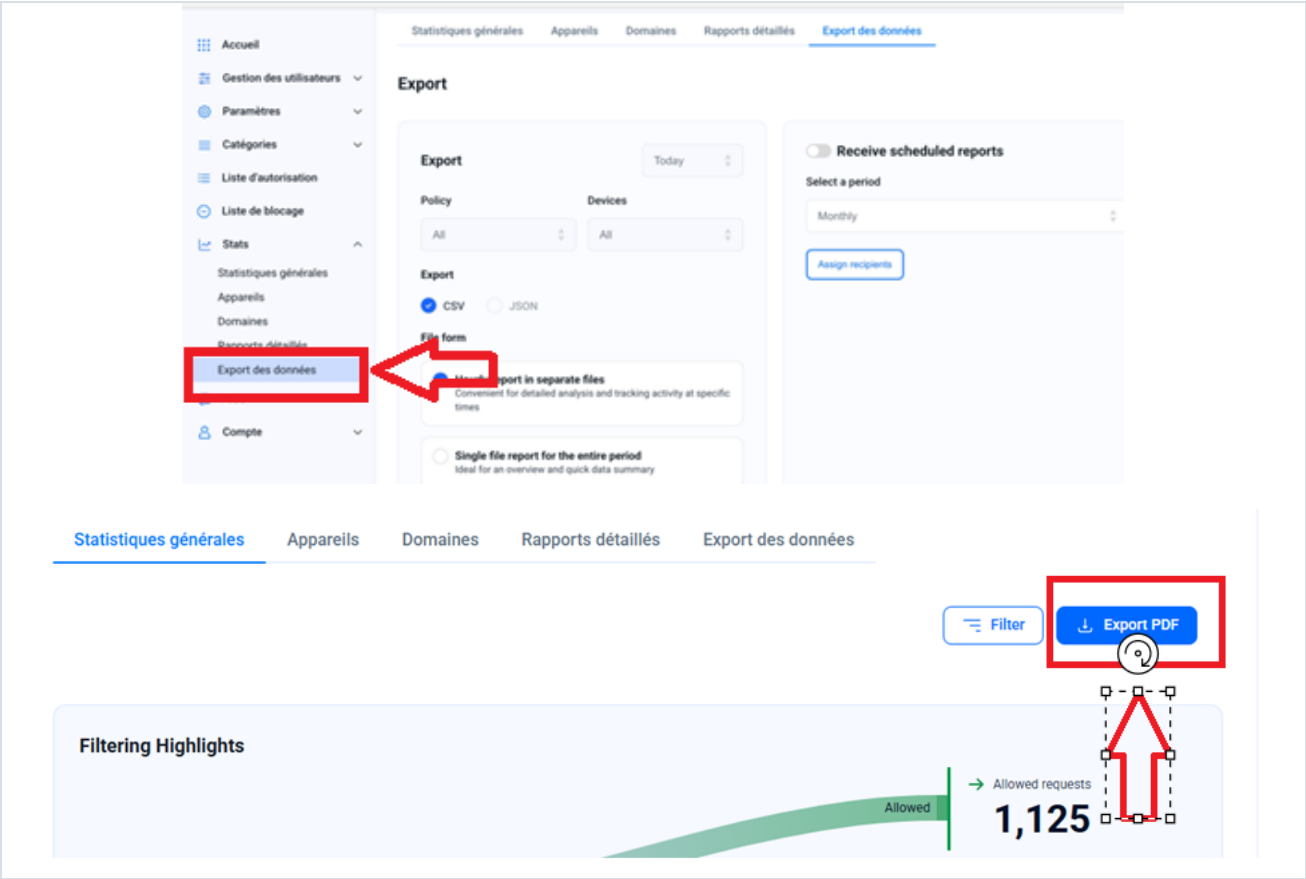


Rapports détaillés : permettent d'obtenir une vue détaillée des statistiques de filtrage.



10.3 Exporter les données statistiques

L'export permet de télécharger les statistiques pour une analyse ou un archivage, depuis la section « Export des données » ou depuis les statistiques générales.

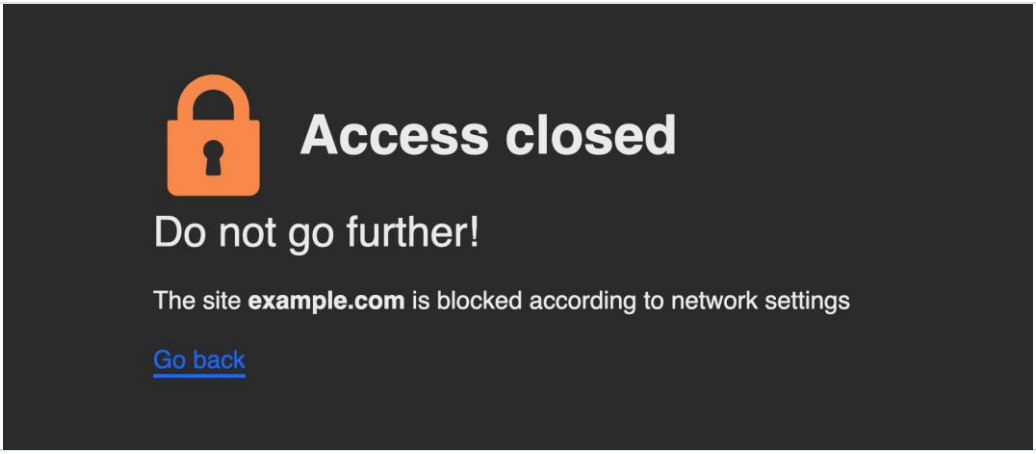


10.4 Interpréter les statistiques

- Les statistiques doivent être interprétées avec prudence.
- Un nombre élevé de requêtes ne signifie pas forcément qu'un site a été consulté de nombreuses fois : une seule page web ou une seule application peut générer plusieurs requêtes DNS.
- Certains domaines correspondent à des services de publicité, de mesure d'audience, de mise à jour ou de contenus intégrés, et non au site réellement consulté.
- Une requête bloquée signifie que le contrôle parental SafeDNS a empêché l'accès au domaine concerné ; cela ne signifie pas nécessairement que l'enfant a volontairement tenté d'y accéder.
- Une menace bloquée peut provenir d'un contenu intégré à une page web ou d'un logiciel fonctionnant en arrière-plan sur l'ordinateur.
- Les statistiques ne sont pas mises à jour instantanément : quelques instants peuvent être nécessaires avant que les nouvelles données n'apparaissent dans le tableau de bord.

11. Questions fréquentes (FAQ)

Exemple de page de blocage affichée lorsque vous essayez d'ouvrir un site bloqué :



Problème rencontré	Vérifications et actions à effectuer
Un site web bloqué reste accessible	• Vérifiez que vous avez modifié la bonne politique. • Vérifiez que la politique est attribuée au bon appareil. • Vérifiez si le site figure dans une liste d'autorisation. • Fermez puis rouvrez le navigateur. • Attendez quelques instants, puis testez à nouveau.
Un site web autorisé reste bloqué	• Vérifiez que le domaine a été correctement saisi. • Vérifiez que le site a été ajouté à la bonne politique et à la bonne liste. • Enregistrez les modifications, puis rouvrez le navigateur.
La politique activée ne semble pas être la bonne	• Vérifiez l'attribution de la politique. • Vérifiez si une politique planifiée est actuellement active. • Vérifiez la date, l'heure et le fuseau horaire de l'ordinateur.
Le planning ne s'active pas correctement	• Vérifiez les jours et les horaires sélectionnés. • Vérifiez la date, l'heure et le fuseau horaire de l'appareil. • La politique planifiée n'est active que pendant les périodes définies ; en dehors de ces plages, la politique Default s'applique.
Le problème persiste	Contacter l'assistance technique — 08 09 10 15 50 (prix d'un appel local) Horaires : du lundi au vendredi de 8 h à 20 h, le samedi de 8 h à 16 h (hors jours fériés).

BESOIN D'AIDE ?

Contacter l'assistance technique — 08 09 10 15 50 (prix d'un appel local)
Horaires : du lundi au vendredi de 8 h à 20 h, le samedi de 8 h à 16 h (hors jours fériés).