



Dr.WEB

Security Space pour les appareils mobiles
(Android)

Manuel Utilisateur



© **Doctor Web, 2024. Tous droits réservés**

Le présent document est un document d'information et de référence concernant le logiciel de la famille Dr.Web y spécifié. Ce document ne justifie pas les conclusions exhaustives sur la présence ou l'absence de tout paramètre fonctionnel et/ou technique dans le logiciel de la famille Dr.Web et ne peut pas être utilisé pour déterminer la conformité du logiciel de la famille Dr.Web aux exigences, tâches techniques et/ou paramètres quelconques ainsi qu'aux autres documents de tierces personnes.

Ce document est la propriété de Doctor Web et peut être utilisé uniquement à des fins personnelles de l'acheteur du produit. Aucune partie de ce document ne peut être reproduite, publiée ou transmise sous quelque forme que ce soit, par quelque moyen que ce soit et dans quelque but que ce soit sinon pour une utilisation personnelle de l'acheteur sans attribution propre.

Marques déposées

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-Desk, KATANA et le logo Dr.WEB sont des marques déposées et des marques commerciales de Doctor Web en Russie et/ou dans d'autres pays. D'autres marques déposées, marques commerciales et noms de société utilisés dans ce document sont la propriété de leurs titulaires respectifs.

Limitation de responsabilité

En aucun cas Doctor Web et ses revendeurs ne sont tenus responsables des erreurs/lacunes éventuelles pouvant se trouver dans cette documentation, ni des dommages directs ou indirects causés à l'acheteur du produit, y compris la perte de profit.

Dr.Web Security Space pour les appareils mobiles (Android)

Version 12.9

Manuel Utilisateur

08/11/2024

Doctor Web, Siège social en Russie

Adresse : 2-12A, 3e rue Yamskogo polya, 125124 Moscou, Russie

Site web : <https://www.drweb.com/>

Téléphone : +7 (495) 789-45-87

Vous pouvez trouver les informations sur les bureaux régionaux sur le site officiel de la société.

Doctor Web

Doctor Web — éditeur russe de solutions de sécurité informatique.

Doctor Web propose des solutions antivirus et antispam efficaces pour les institutions publiques, les entreprises, ainsi que pour les particuliers.

Les solutions antivirus Dr.Web sont connues depuis 1992 pour leur excellence en matière de détection des programmes malveillants et leur conformité aux standards internationaux de sécurité.

Les certificats et les prix attribués, ainsi que l'utilisation de nos produits dans le monde entier sont les meilleurs témoins de la confiance qui leur est accordée.

Nous remercions tous nos clients pour leur soutien !



Contenu

1. Introduction	8
1.1. Fonctions de Dr.Web	9
2. Pré-requis système	10
3. Installation de Dr.Web Security Space pour les appareils mobiles	11
4. Mise à jour et suppression de Dr.Web Security Space pour les appareils mobiles	15
5. Octroi de la licence	18
5.1. Écran Licence	18
5.2. Licence de démonstration	19
5.3. Achat d'une licence	20
5.4. Activation de la licence	22
5.5. Restauration de la licence	26
5.6. Suspension et annulation de l'abonnement	27
5.7. Renouvellement de la licence	28
5.8. Configuration des notifications d'expiration de la licence	30
6. Mise en route	31
6.1. Contrat de licence	31
6.2. Autorisations	31
6.3. Interface	34
6.4. Notifications	36
6.5. Widget	39
6.6. Mon Dr.Web	40
7. Compte Dr.Web	41
8. Composants de Dr.Web	44
8.1. Protection antivirus	44
8.1.1. SpIDer Guard : protection antivirus constante	44
8.1.2. Scanner Dr.Web : scan sur demande de l'utilisateur	47
8.1.3. Résultats du scan	51
8.1.3.1. Menaces dans les applications système	54
8.1.3.2. Modifications dans la zone système	55
8.1.3.3. Menaces utilisant la vulnérabilité Stagefright	56
8.1.4. Applications bloqueurs de l'appareil	56
8.2. Filtre des appels et des SMS	57



8.2.1. Filtre de blocage	58
8.2.2. Filtre d'autorisation	59
8.2.3. Masques	60
8.2.4. Édition des listes	61
8.2.5. Appels et SMS bloqués	62
8.3. Filtre URL	63
8.4. Antivol Dr.Web	66
8.4.1. Activation de l'Antivol Dr.Web	66
8.4.2. Configuration de l'Antivol Dr.Web	67
8.4.3. Commandes de l'Antivol Dr.Web	74
8.4.3.1. Commandes push	75
8.4.3.2. Commandes SMS	77
8.4.4. Désactivation de l'Antivol Dr.Web	79
8.5. Contrôle parental	80
8.5.1. Blocage de l'accès aux applications et aux composants	83
8.5.2. Configuration du Contrôle parental	88
8.5.3. Journal du Contrôle parental	89
8.6. Pare-feu Dr.Web	92
8.6.1. Gestion de l'activité réseau des applications	94
8.6.1.1. Applications actives	94
8.6.1.2. Toutes les applications	97
8.6.1.3. Accès à la transmission de données	100
8.6.1.4. Limitation de l'utilisation du trafic mobile	101
8.6.2. Trafic des applications individuelles	102
8.6.2.1. Statistiques d'utilisation du trafic Internet	103
8.6.2.2. Paramètres de l'application	105
8.6.2.3. Règles de connexions	106
8.6.2.4. Journal de l'application	111
8.6.3. Journal du Pare-feu Dr.Web	112
8.7. Contrôleur de sécurité	114
8.7.1. Vulnérabilités	115
8.7.2. Paramètres système	116
8.7.3. Logiciels en conflit	117
8.7.4. Administrateurs de l'appareil non affichés	117
8.7.5. Applications utilisant la vulnérabilité Fake ID	117
8.7.6. Paramètres d'optimisation	117



8.7.6.1. Asus	119
8.7.6.2. Huawei	119
8.7.6.3. Meizu	121
8.7.6.4. Nokia	122
8.7.6.5. OnePlus	123
8.7.6.6. Oppo	124
8.7.6.7. Samsung	125
8.7.6.8. Sony	126
8.7.6.9. Xiaomi	126
8.8. Statistiques	128
8.9. Quarantaine	129
9. Paramètres	132
9.1. Paramètres généraux	133
9.2. Mise à jour des base virales	134
9.3. Copie de sauvegarde	136
9.4. Réinitialisation des paramètres	136
10. Mode de protection centralisée	138
10.1. Passage en mode de protection centralisée	139
10.2. Gestion	142
10.3. Passage en mode standalone	142
11. Dr.Web sous Android TV	144
11.1. Événements sous Android TV	145
11.2. Protection antivirus sous Android TV	145
11.2.1. Protection permanente SplDer Guard sous Android TV	146
11.2.2. Scanner Dr.Web sous Android TV	146
11.2.3. Résultats du scan sous Android TV	148
11.3. Pare-feu Dr.Web sous Android TV	150
11.3.1. Activité des connexions réseau sous Android TV	151
11.3.2. Traitement du trafic des applications sous Android TV	154
11.3.2.1. Statistiques et paramètres de l'application sous Android TV	155
11.3.2.2. Règles de connexions sous Android TV	158
11.3.2.3. Journal de l'application sous Android TV	162
11.3.3. Journal du Pare-feu Dr.Web sous Android TV	163
11.4. Contrôleur de sécurité sous Android TV	165
11.5. Divers	168
11.5.1. Paramètres de Dr.Web sous Android TV	170



12. Service de support technique

172

13. Mot de passe oublié ?

173



1. Introduction

Dr.Web Security Space pour les appareils mobiles (ci-après — Dr.Web) protège les appareils mobiles fonctionnant sous le système d'exploitation Android™, ainsi que les téléviseurs, les lecteurs média, les consoles de jeux fonctionnant sous Android TV™, contre les menaces créées spécialement pour infecter ces appareils.



Sur les appareils tournant sous Android TV, le mode de protection centralisée n'est pas disponible. Pour vérifier si votre appareil et la version de l'application Dr.Web supportent le mode de protection centralisée, consultez la rubrique [Mode de protection centralisée](#).

L'application utilise les technologies de Doctor Web permettant de détecter et neutraliser les objets malveillants qui représentent une menace pour le fonctionnement de l'appareil et pour sa sécurité informatique.

Dr.Web utilise la technologie Origins Tracing™ for Android qui détecte les programmes malveillants créés spécialement pour la plateforme Android. Cette technologie permet de dépister de nouveaux virus en utilisant la base de connaissances sur les menaces connues. Origins Tracing™ for Android sait reconnaître des virus recompilés, comme Android.SMSSend, Spy, ainsi que les applications infectées par Android.ADRD, Android.Geinimi, Android.DreamExploit. Les noms des menaces détectées à l'aide d'Origins Tracing™ for Android sont basés sur le modèle «Android.VirusName.origin».

À propos du manuel

Ce Manuel est destiné à aider les utilisateurs des appareils fonctionnant sous l'OS Android à installer, à configurer l'application et à découvrir ses fonctions principales.

Les styles utilisés dans ce manuel :

Style	Commentaire
	Avertissement sur des situations potentielles d'erreurs et sur les éléments importants auxquels il faut faire attention.
<i>Réseau antivirus</i>	Un nouveau terme ou l'accent mis sur un terme dans les descriptions.
<IP-address>	Champs destinés à remplacer les noms fonctionnels par leurs valeurs.
Enregistrer	Noms des boutons de l'écran, des fenêtres, des éléments de menu et d'autres éléments de l'interface du logiciel.
CTRL	Touches du clavier.
Internal storage/Android/	Noms de fichiers/dossiers ou fragments de programme.



Style	Commentaire
Annexe A	Liens vers les autres chapitres du manuel ou liens vers des ressources externes.

1.1. Fonctions de Dr.Web

Dr.Web possède les fonctions suivantes :

- Protège le système de fichiers en temps réel (analyse les fichiers enregistrés, installe des applications, etc.).
- Analyse tous les fichiers dans la mémoire ou les fichiers et les dossiers particuliers à la demande de l'utilisateur.
- Analyse des archives.
- Analyse la carte SD ou un autre support amovible.
- Surveille les modifications dans la zone système.
- Supprime ou met en quarantaine des menaces détectées.
- Débloque l'appareil s'il a été bloqué par un ransomware.
- Filtre les appels et les SMS (le filtrage des appels et des SMS n'est pas disponible dans les versions de l'application installées depuis Google Play).
- Effectue des mises à jour régulières des bases virales Dr.Web par Internet.
- Enregistre des statistiques sur les menaces détectées et sur les actions de l'application, écrit le journal d'événements.
- Recherche et bloque l'appareil à distance en cas de perte ou de vol.
- Restreint l'accès aux sites sélectionnés, ainsi qu'aux catégories de sites dans le navigateur standard Android, Google Chrome, Yandex.Browser, Microsoft Edge, Firefox, Firefox Focus, Opera, Adblock Browser, Dolphin Browser, Sputnik, Boat Browser et Atom.
- Détecte et neutralise des problèmes de sécurité et des vulnérabilités.
- Contrôle les connexions Internet, protège l'appareil contre l'accès non autorisé et prévient la fuite des données importantes via le réseau.
- Permet de limiter l'accès aux applications installées sur l'appareil.
- Donne la possibilité d'activer le filtre adulte dans la plupart des moteurs de recherche.



Certaines fonctions susmentionnées ne sont pas disponibles dans l'application installée sur l'appareil fonctionnant sous [Android TV](#).



2. Pré-requis système

Avant l'installation, assurez-vous que votre appareil possède les pré-requis système suivants :

Paramètre	Pré-requis
Système d'exploitation	Android en version 4.4 - 15.0 Android TV (sur les téléviseurs, les lecteurs média et les consoles de jeux)
Processeur	x86/x86-64/ARMv7/ARMv8/ARMv9
Mémoire vive disponible	512 Mo au minimum
Espace disque disponible	45 Mo au minimum (pour le stockage de données)
Résolution de l'écran	800x480 au minimum
Autre	Connexion Internet (pour la mise à jour des bases virales). Le mode de protection centralisée n'est pas disponible sur les appareils tournant sous Android TV

- Pour la compatibilité avec les applications qui bloquent le lancement d'autres applications, il faut que les applications-bloqueurs ne restreignent pas le lancement de Dr.Web.
- Si vous utilisez une tablette, le support des cartes SIM est nécessaire pour un fonctionnement correct du filtrage des appels et des messages, ainsi que de l'Antivol Dr.Web.
- Le filtre URL fonctionne dans le navigateur intégré Android et dans Google Chrome, Yandex.Browser, Microsoft Edge, Firefox, Firefox Focus, Opera, Adblock Browser, Dolphin Browser, Sputnik, Boat Browser et Atom.
- Pour un fonctionnement correct du filtre URL sur les appareils tournant sous Android 5.1 ou une version antérieure, activez la sauvegarde de l'historique dans votre navigateur.



Sur les appareils ayant des firmwares utilisateur et sur les appareils avec l'accès root ouvert (rootés), le fonctionnement correct de Dr.Web n'est pas garanti. De plus, le support technique pour ces appareils n'est pas prévu.

Par défaut, l'application est installée dans la mémoire interne de l'appareil. Pour un fonctionnement correct de Dr.Web ne déplacez pas l'application installée sur des supports amovibles.



3. Installation de Dr.Web Security Space pour les appareils mobiles

Dr.Web peut être installé :

- [Depuis le disque de licence.](#)
- [Depuis le site de la société Doctor Web.](#)
- [Depuis Google Play.](#)
- [Depuis HUAWEI AppGallery.](#)
- [Depuis Xiaomi GetApps.](#)
- [A l'aide du programme de synchronisation avec l'ordinateur.](#)

Installation depuis le disque de licence

Sur certains appareils il faut autoriser la transmission de fichiers en cas de connexion à l'ordinateur avec un câble USB.

Pour installer Dr.Web, activez le paramètre système suivant :

- Sur les appareils tournant sous Android 7.1 ou une version antérieure :
 1. Dans les paramètres de l'appareil, ouvrez l'écran **Sécurité**.
 2. Cochez la case **Sources inconnues**.
- Sur les appareils tournant sous Android 8.0 ou une version supérieure :
 1. Dans les paramètres de l'appareil, ouvrez l'écran **Installation d'applications inconnues**.
 2. Autorisez l'installation d'applications de la source sélectionnée.

Copie du fichier d'installation du disque et lancement sur l'appareil

1. Insérez le disque dans le lecteur.
2. Copiez le fichier d'installation à partir du disque sur l'ordinateur.
3. Connectez l'appareil mobile à l'ordinateur à l'aide d'un câble USB.
4. Faites glisser le fichier d'installation dans la fenêtre qui s'ouvre.
5. Déconnectez l'appareil mobile de l'ordinateur et débranchez le câble.
6. Utilisez le gestionnaire de fichiers pour trouver et lancer le fichier d'installation sur l'appareil mobile.
7. Dans la fenêtre qui s'affiche, appuyez sur **Installer**.
8. Appuyez sur **Ouvrir** pour commencer à utiliser l'application.
Appuyez sur **Terminé** pour fermer la fenêtre et commencer à utiliser l'application plus tard.

Pour la future gestion de l'application, il est nécessaire d'activer la licence [commerciale](#) ou la licence de [démonstration](#).



Après l'installation de l'application :

- Sur les appareils tournant sous Android 7.1 ou une version antérieure, désactivez le paramètre **Sources inconnues** dans les paramètres de l'appareil.
- Sur les appareils tournant sous Android 8.0 ou une version supérieure, ouvrez l'écran **Installation d'applications inconnues** et interdisez l'installation des applications depuis la source sélectionnée.

Installation depuis le site de la société Doctor Web

Pour installer Dr.Web, activez le paramètre système suivant :

- Sur les appareils tournant sous Android 7.1 ou une version antérieure :
 1. Dans les paramètres de l'appareil, ouvrez l'écran **Sécurité**.
 2. Cochez la case **Sources inconnues**.
- Sur les appareils tournant sous Android 8.0 ou une version supérieure :
 1. Dans les paramètres de l'appareil, ouvrez l'écran **Installation d'applications inconnues**.
 2. Autorisez l'installation d'applications de la source sélectionnée.

Vous pouvez télécharger le fichier d'installation Dr.Web sur le site de la société Doctor Web à l'adresse <https://download.drweb.com/android/>.

Pour exécuter le fichier d'installation directement sur l'appareil

1. Copiez le fichier d'installation sur l'appareil.
2. Utilisez le gestionnaire de fichiers pour trouver et lancer le fichier d'installation.
3. Dans la fenêtre qui s'affiche, appuyez sur **Installer**.
4. Appuyez sur **Ouvrir** pour commencer à utiliser l'application.
Appuyez sur **Terminé** pour fermer la fenêtre et commencer à utiliser l'application plus tard.

Pour la future gestion de l'application, il est nécessaire d'activer la licence [commerciale](#) ou la licence de [démonstration](#).



Après l'installation de l'application :

- Sur les appareils tournant sous Android 7.1 ou une version antérieure, désactivez le paramètre **Sources inconnues** dans les paramètres de l'appareil.
- Sur les appareils tournant sous Android 8.0 ou une version supérieure, ouvrez l'écran **Installation d'applications inconnues** et interdisez l'installation des applications depuis la source sélectionnée.



Installation depuis Google Play

Pour installer Dr.Web depuis Google Play, assurez-vous que :

- Vous avez un compte Google.
- Votre appareil est associé au compte Google.
- L'appareil possède une connexion Internet.
- L'appareil satisfait aux [pré-requis système](#).

Pour installer l'application

1. Ouvrez Google Play sur votre appareil, trouvez l'application Dr.Web dans la liste d'applications et appuyez sur **Installer**.



Si vous n'arrivez pas à trouver Dr.Web dans Google Play, il est possible que votre appareil ne satisfait pas aux [pré-requis système](#).

2. Ensuite, un écran va s'ouvrir contenant des informations sur les fonctions de l'appareil, l'accès auxquelles est requis pour le fonctionnement de l'application.

Consultez la liste des autorisations nécessaires et appuyez sur **Accepter**.

3. Pour commencer à gérer l'application, appuyez sur **Ouvrir**.

Pour la future gestion de l'application, il est nécessaire d'activer la licence [commerciale](#) ou la licence de [démonstration](#).

Installation depuis HUAWEI AppGallery

Pour installer Dr.Web depuis HUAWEI AppGallery, assurez-vous que :

- Vous avez un compte Huawei.
- Votre appareil est associé au compte Huawei.
- L'appareil possède une connexion Internet.
- L'appareil satisfait aux [pré-requis système](#).

Pour installer l'application

1. Ouvrez HUAWEI AppGallery sur votre appareil, trouvez l'application Dr.Web dans la liste d'applications et appuyez sur **Installer**.



Si vous n'arrivez pas à trouver Dr.Web dans HUAWEI AppGallery, il est probable que votre appareil ne satisfait pas aux [pré-requis système](#).

2. Ensuite, un écran va s'ouvrir contenant des informations sur les fonctions de l'appareil, l'accès auxquelles est requis pour le fonctionnement de l'application.



Consultez la liste des autorisations nécessaires et appuyez sur **Accepter**.

3. Pour commencer à gérer l'application, appuyez sur **Ouvrir**.

Pour la future gestion de l'application, il est nécessaire d'activer la licence [commerciale](#) ou la licence de [démonstration](#).

Installation depuis Xiaomi GetApps

Pour installer Dr.Web depuis Xiaomi GetApps, assurez-vous que :

- Vous avez un compte Xiaomi.
- Votre appareil est associé au compte Xiaomi.
- L'appareil possède une connexion Internet.
- L'appareil satisfait aux [pré-requis système](#).

Pour installer l'application

1. Ouvrez Xiaomi GetApps sur votre appareil, trouvez l'application Dr.Web dans la liste des applications et appuyez sur **Télécharger**.



Si vous n'arrivez pas à trouver Dr.Web dans Xiaomi GetApps, votre appareil ne satisfait pas aux [pré-requis système](#).

2. Pour commencer à gérer l'application, appuyez sur **Ouvrir**.

Installation à l'aide d'un programme de synchronisation

Installation à l'aide d'un programme de synchronisation avec l'ordinateur (par exemple, HTC Sync™, etc.).

1. Synchronisez votre appareil mobile avec l'ordinateur en utilisant un logiciel approprié.
2. Lancez l'assistant d'installation d'applications inclus dans le programme de synchronisation.
3. Indiquez le chemin d'accès au fichier d'installation sur l'ordinateur, puis suivez les instructions de l'assistant d'installation.
4. L'application sera copiée sur l'appareil mobile, où vous pourrez voir les informations sur les droits d'accès requis et confirmer l'installation. Après la confirmation, l'application sera installée automatiquement.
5. Fermez l'assistant d'installation du programme de synchronisation.

Dr.Web est installé et prêt à l'emploi. Pour le futur travail avec l'application, il est nécessaire d'activer la licence [commerciale](#) ou la licence de [démonstration](#).



4. Mise à jour et suppression de Dr.Web Security Space pour les appareils mobiles

Mise à jour de Dr.Web

Configuration de la mise à jour automatique de la version depuis le site de Doctor Web

Si votre version de Dr.Web est téléchargée du site de Doctor Web, vous pouvez activer les notifications de la disponibilité d'une nouvelle version. Pour ce faire :

1. Appuyez sur **Menu**  sur l'écran d'accueil de Dr.Web et sélectionnez l'élément **Paramètres**.
2. Sur l'écran **Paramètres**, sélectionnez **Mise à jour des bases virales**.
3. Sur l'écran **Mise à jour des bases virales**, cochez la case **Nouvelle version**.

Si cette case est cochée, Dr.Web vérifie la disponibilité d'une nouvelle version à chaque mise à jour des bases virales. Lorsqu'une nouvelle version de l'application apparaît, vous recevrez une notification et vous pourrez la télécharger vite et installer.

Mise à jour manuelle via Google Play

Si la mise à jour automatique n'est pas configurée pour les applications de Google Play, vous pouvez lancer la mise à jour manuellement :

1. Ouvrez l'application **Play Store**.
2. Appuyez sur l'icône de votre profil Google en haut à droite de l'écran.
3. Sélectionnez l'élément **Gérer les applications et l'appareil**.
4. Ouvrez l'onglet **Gérer**.
5. Appuyez sur la liste **Mise à jour disponible** et effectuez l'une des actions suivantes :
 - Sélectionnez **Dr.Web** et appuyez sur **Mettre à jour**.
 - Cochez la case contre **Dr.Web** et appuyez sur l'icône .



L'application figure dans la liste **Mise à jour disponible** si la nouvelle version de l'application est déjà sortie.

6. De nouvelles autorisations peuvent être requises lors de la mise à jour. Dans ce cas, la fenêtre de confirmation va s'ouvrir.

Appuyez sur **Accepter** pour autoriser l'accès aux fonctions de l'appareil nécessaires pour l'application.

Pour commencer à gérer l'application, appuyez sur **Ouvrir**.



Mise à jour via HUAWEI AppGallery

Vous pouvez configurer la mise à jour automatique des applications installées depuis HUAWEI AppGallery, y compris Dr.Web. Pour cela, utilisez l'interrupteur **Mise à jour automatique via le Wi-Fi** dans la section **Gestionnaire** de l'application HUAWEI AppGallery.

Vous pouvez également lancer la mise à jour manuellement :

1. Ouvrez l'application **HUAWEI AppGallery** et appuyez sur **Gestionnaire**.
2. Dans la liste des applications installées, trouvez Dr.Web et appuyez sur **Mettre à jour**.



Le bouton **Mettre à jour** est disponible si la nouvelle version de l'application est déjà sortie.

3. De nouvelles autorisations peuvent être requises lors de la mise à jour. Dans ce cas, la fenêtre de confirmation va s'ouvrir.

Appuyez sur **Accepter** pour autoriser l'accès aux fonctions de l'appareil nécessaires pour l'application.

Pour commencer à gérer l'application, appuyez sur **Ouvrir**.

Suppression de Dr.Web



L'Antivol Dr.Web empêche la suppression de l'application Dr.Web de l'appareil. Si l'Antivol est configuré sur votre appareil, [désactivez-le](#) et excluez Dr.Web des administrateurs de l'appareil avant de supprimer l'application.

Pour supprimer Dr.Web

1. Dans les paramètres de l'appareil, sélectionnez **Applications** ou **Gestionnaire d'applications**.
2. Dans la liste des applications installées, sélectionnez **Dr.Web** et appuyez sur **Supprimer**.

Le dossier de la quarantaine et les fichiers journaux ne sont pas supprimés automatiquement. Vous pouvez les supprimer manuellement du dossier `Android/data/com.drweb/files` de la mémoire interne de l'appareil.



Sur les appareils tournant sous Android 11.0 ou une version supérieure, les journaux sont enregistrés dans le dossier `Download/DrWeb`.

Suppression de Dr.Web via HUAWEI AppGallery

Si vous avez installé Dr.Web depuis HUAWEI AppGallery, vous pouvez supprimer l'application en exécutant les étapes suivantes :



1. Ouvrez l'application Huawei AppGallery.
2. Appuyez sur **Gestionnaire**.
3. Sur l'écran qui s'affiche, appuyez sur **Gestionnaire d'installation**.
4. Dans la liste des applications installées, sélectionnez Dr.Web et appuyez sur **Supprimer**.
5. Confirmez l'action.



5. Octroi de la licence

La licence permet d'utiliser toutes les fonctionnalités du produit pendant toute la durée de la licence. Les droits de l'utilisateur sont définis en fonction du Contrat de licence.

La licence est requise pour le fonctionnement de tous les composants de Dr.Web dans les versions suivantes de l'application :

- Versions téléchargées dans votre espace privé du fournisseur du service Antivirus Dr.Web.
- Versions reçues de l'administrateur du réseau antivirus de votre entreprise.
- Versions pour les appareils tournant sous Android TV.

La licence est requise pour le fonctionnement de tous les composants sauf [SplDer Guard](#), le [Scanner](#) et le [Contrôleur de sécurité](#) dans les versions suivantes de l'application :

- Les versions téléchargées sur le site de la société Doctor Web <https://download.drweb.com/android/>.
- Dans la version Dr.Web installée depuis Google Play.
- Dans la version installée depuis HUAWEI AppGallery.

Si vous souhaitez tester le produit avant de l'acheter, vous pouvez activer la [licence de démonstration](#).

Si vous avez déjà une licence valide pour les produits Dr.Web Security Space ou l'Antivirus Dr.Web (fournis en boîte ou sous forme d'une licence électronique), vous pouvez l'[activer](#).



Quand le [mode de protection centralisée](#) est activé, la licence est téléchargée automatiquement depuis le serveur de protection centralisée.

5.1. Écran Licence

Dans l'écran **Licence** (voir [Figure 1](#)), vous pouvez [acheter](#) ou [activer](#) la licence commerciale ainsi qu'obtenir la [version de démonstration](#).

Pour accéder à l'écran **Licence**, ouvrez l'application et exécutez une des actions suivantes :

- Dans les versions de Dr.Web [nécessitant les licences pour le fonctionnement de tous les composants](#) :
 - Appuyez sur **En savoir plus** dans la notification d'absence de la licence dans la partie supérieure de l'écran d'accueil de Dr.Web.
 - Appuyez sur **Menu**  sur l'écran d'accueil de Dr.Web et sélectionnez l'élément **Licence**.
- Dans les versions de Dr.Web [nécessitant les licences pour le fonctionnement de certains composants](#) :



- Sur l'écran d'accueil de Dr.Web, sélectionnez l'un des composants nécessitant l'achat d'une licence.
- Appuyez sur **Menu**  sur l'écran d'accueil de Dr.Web et sélectionnez l'élément **Licence**.

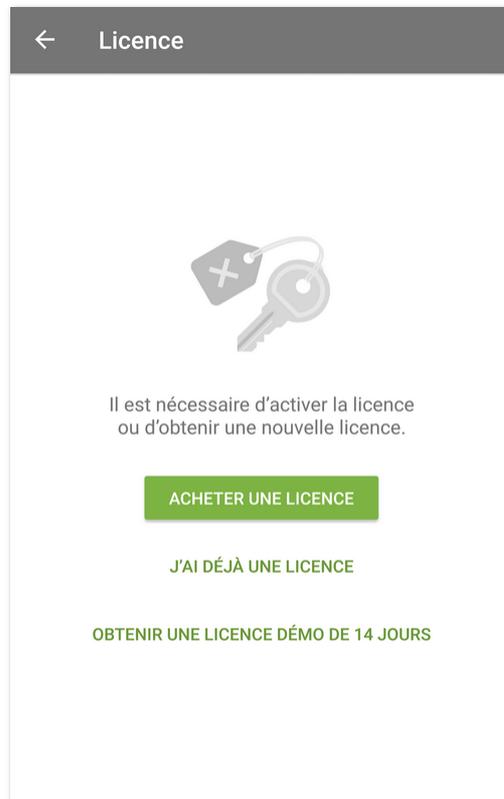


Figure 1. Écran Licence

5.2. Licence de démonstration

Si vous voulez tester les fonctions de l'application avant de l'acheter, vous pouvez activer une licence de démonstration pour 14 jours.

Pour activer la licence de démonstration

1. Ouvrez l'application.
2. Passez à l'écran [Licence](#).
3. Sélectionnez **Obtenir une licence démo de 14 jours**.
4. Indiquez vos données personnelles (voir [Figure 2](#)) :
 - Le nom et le prénom.
 - L'adresse e-mail valide.
 - Le pays.
5. Cochez la case **Recevoir des informations par e-mail** (optionnel).



À cette étape, l'application vous demande l'accès aux contacts. Si vous autorisez l'accès, les champs **Adresse e-mail** et **Pays** seront remplis automatiquement. Si vous déclinez la demande, vous devez remplir les champs manuellement.

- Appuyez sur **Obtenir une version démo**. La licence de démonstration sera activée.

← Version démo

Pour obtenir une démo, indiquez le nom et l'adresse e-mail.

Nom et prénom
Adele Blanc

Adresse e-mail
username@example.com

Pays
France

Recevoir des informations par e-mail

OBTENIR UNE VERSION DÉMO

Figure 2. Réception de la licence de démonstration

5.3. Achat d'une licence

Si l'application est installée depuis Google Play

- Ouvrez l'application.
- Passez à l'écran [Licence](#).
- Sélectionnez **Acheter une licence**.

Si vous n'avez pas de compte Google, indiquez l'adresse e-mail sur laquelle la licence sera enregistrée. En cas de réinstallation de l'application ou l'installation sur un autre appareil, vous pourrez restaurer la licence en utilisant cette adresse.

À cette étape, l'application vous demande l'accès aux contacts. Si vous autorisez l'accès, l'adresse e-mail sera saisie automatiquement. Si vous déclinez la demande, vous devez saisir l'adresse manuellement.

- Sur l'écran **Acheter une licence** (voir [Figure 3](#)), sélectionnez une des options suivantes :



- **Abonnement pour un mois.** L'abonnement pour un mois permet d'utiliser la licence pendant un mois à compter de la date de paiement. Ensuite, l'abonnement se renouvelle automatiquement et il est facturé une fois par mois.
- **Licence pour 1 an.** La licence est valable pendant un an à compter de la date d'achat.
- **Licence pour 2 ans.** La licence est valable pendant deux ans à compter de la date d'achat.

Une fois une option sélectionnée, l'écran d'achat de licence s'ouvre. Quelque temps après le paiement, la licence sera activée automatiquement.

Le fichier clé de licence sera envoyé à votre adresse e-mail pour confirmer l'achat de la licence pour 1 an ou pour 2 ans. Si la licence n'est pas activée à cause d'une erreur technique, contactez le support technique : <https://support.drweb.com/>.

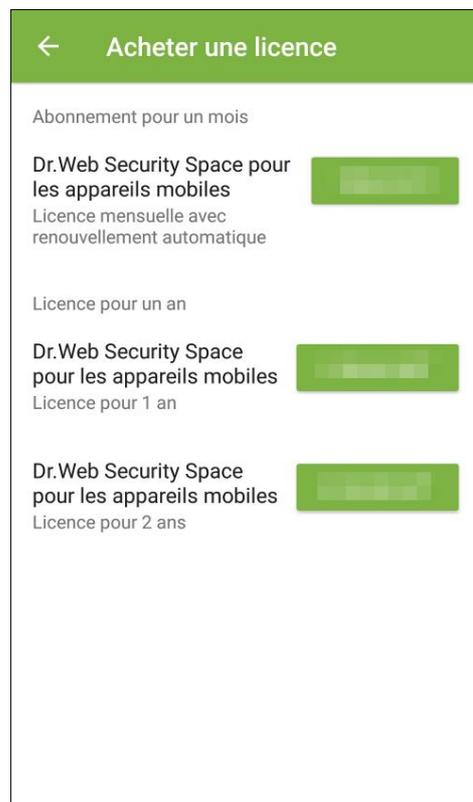


Figure 3. Achat d'une licence

Si l'application a été installée depuis le site de la société Doctor Web ou depuis Xiaomi GetApps

1. Ouvrez l'application.
2. Passez à l'écran [Licence](#).
3. Sélectionnez l'option **Acheter une licence**. Une page de la boutique en ligne de Doctor Web va s'ouvrir.

Vous pouvez également ouvrir la page de la boutique en ligne en suivant le lien <https://estore.drweb.com/mobile/>.

4. Sélectionnez la durée de licence et le nombre d'appareils protégés.



5. Appuyez sur **Acheter**.
6. Remplissez le formulaire d'achat et appuyez sur **Passer la commande**.
Après la commande, le numéro de série vous sera envoyé sur l'adresse e-mail indiquée. De plus, vous pouvez choisir de recevoir le numéro de série par SMS sur le numéro de téléphone indiqué.
7. [Enregistrez le numéro de série obtenue](#).

Si l'application est installée depuis HUAWEI AppGallery

1. Ouvrez l'application.
2. Passez à l'écran [Licence](#).
3. Sélectionnez **Acheter une licence**.

Créez un compte Huawei ou connectez-vous au compte existant. Après la connexion, accordez les autorisations nécessaires à l'application.

À cette étape, l'application peut vous demander l'accès aux données de votre compte Huawei. Si vous autorisez l'accès, l'adresse e-mail sera saisie automatiquement. Si vous bloquez l'accès, il vous sera proposé de sélectionner l'adresse dans la liste de la fenêtre pop-up.

4. Sur l'écran **Acheter une licence**, sélectionnez une des options suivantes :

- **Licence pour 1 an**
- **Licence pour 2 ans**

Une fois une des variantes sélectionnée, l'écran d'achat de licence s'ouvre. Quelque temps après le paiement, la licence sera activée automatiquement. Le fichier clé de licence sera envoyé à votre adresse e-mail pour confirmer l'achat. Si la licence n'est pas activée à cause d'une erreur technique, contactez le support technique : <https://support.drweb.com/>.

5.4. Activation de la licence

L'activation de la licence est requise si vous avez installé l'application depuis le site de la société Doctor Web. L'activation peut aussi être nécessaire si vous avez la licence valide pour les produits Dr.Web qui inclut Dr.Web Security Space pour les appareils mobiles.



À partir du 01/09/2024 Dr.Web Security Space pour les appareils mobiles n'est pas inclus dans la licence pour les produits Dr.Web pour ordinateurs. Si vous avez acheté une telle licence après le 31/08/2024 et que vous souhaitez utiliser Dr.Web Security Space pour les appareils mobiles, il vous faudra [acheter une licence supplémentaire](#).

Pour activer la licence

- Enregistrez le numéro de série :
 - [Dans l'application](#), si l'appareil avec l'application installée a une connexion Internet active.



- [Sur le site de Doctor Web](#), s'il n'y a pas de connexion Internet sur l'appareil avec l'application installée.
- [Utilisez le fichier clé](#) (uniquement pour l'application installée depuis le site de Doctor Web).

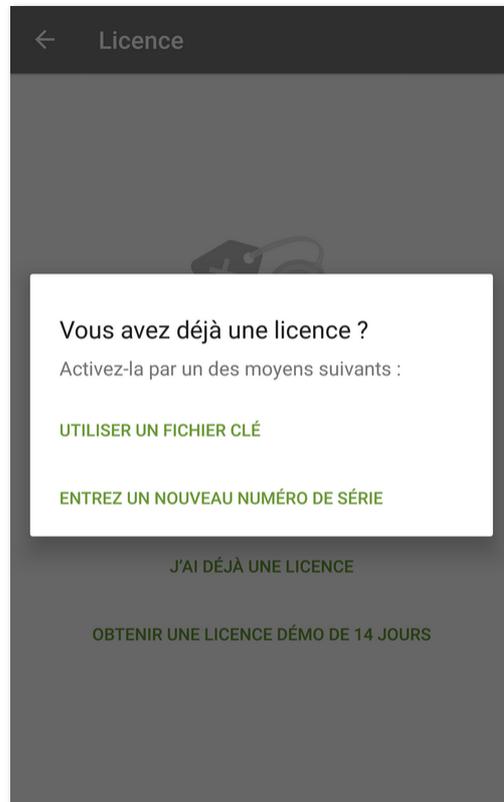


Figure 4. Activation de la licence

Enregistrement d'un numéro de série dans l'application

Pour enregistrer le numéro de série et activer la licence dans l'application

1. Ouvrez l'application.
2. Passez à l'écran [Licence](#).
3. Sélectionnez l'élément **J'ai déjà une licence**.
4. Dans la fenêtre suivante (voir [Figure 4](#)), appuyez sur **Entrez un nouveau numéro de série**.
5. Sur l'écran **Activation d'une licence** (voir [Figure 5](#)), entrez le numéro de série que vous avez reçu après l'achat.
6. Appuyez sur **Activer**.



← Activation de la licence

Pour activer la licence, indiquez le numéro de série.

Numéro de série

XXXX-XXXX-XXXX-XXXX

ACTIVER

Figure 5. Enregistrement d'un numéro de série

7. Indiquez vos données personnelles :
 - Le nom et le prénom.
 - L'adresse e-mail valide.
 - Le pays.
8. Cochez la case **Recevoir des informations par e-mail** (optionnel).
9. Appuyez sur **Activer**.

L'écran d'accueil de Dr.Web va s'ouvrir. Le message vous informant de l'activation de la licence va apparaître en bas de l'écran.

Enregistrement d'un numéro de série sur le site

S'il n'y a pas de connexion Internet sur l'appareil avec l'application installée, vous pouvez enregistrer le numéro de série à l'aide d'un ordinateur ou d'un autre appareil ayant une connexion Internet active. Dans ce cas, vous recevrez un fichier clé de licence qu'il faudra copier sur l'appareil pour activer la licence.

Pour enregistrer le numéro de série sur le site

1. Visitez le site <https://products.drweb.com/register/>.



2. Entrez le numéro de série reçu lors de l'achat de Dr.Web.
3. Remplissez le formulaire contenant les données de l'acheteur.
4. Le fichier clé de licence sera envoyé à l'adresse e-mail indiquée sous forme d'une archive ZIP.

Fichier clé de licence

Le fichier clé de licence contient les droits d'utilisateur d'utilisation de produits Dr.Web.

Le fichier clé de licence possède l'extension .key et contient les informations suivantes :

- Période pendant laquelle vous pouvez utiliser l'application.
- Liste des composants autorisés pour l'utilisation.
- Autres restrictions.

Un fichier clé de licence est valide s'il satisfait aux critères suivants :

- La licence n'a pas expiré.
- Tous les composants antivirus utilisés par l'application sont soumis à licence.
- L'intégrité du fichier clé de licence n'est pas violée.

Si l'une de ces conditions est violée, le fichier clé de licence devient invalide et l'antivirus arrête de détecter et de neutraliser les logiciels malveillants.



Toute modification rend le fichier clé de licence non valide. Par conséquent, il n'est pas recommandé d'ouvrir le fichier clé de licence dans des éditeurs de texte pour ne pas l'endommager.

Utilisation du fichier clé

Vous pouvez utiliser le fichier clé uniquement avec l'application installée depuis le site de Doctor Web.

Pour utiliser un fichier clé

1. Copiez le fichier clé dans le dossier situé dans la mémoire interne de votre appareil.
Vous pouvez décompresser l'archive et copier uniquement le fichier avec l'extension .key ou bien, copier sur l'appareil l'archive ZIP entière.
2. Sur l'écran [Licence](#), sélectionnez l'élément **J'ai déjà une licence**.
3. Sélectionnez l'élément **Utiliser un fichier clé** (voir [Figure 4](#)).
4. Trouvez le dossier contenant le fichier clé ou l'archive ZIP avec le fichier et sélectionnez-le.

Le fichier clé sera installé et prêt à l'emploi. L'écran d'accueil de Dr.Web va s'ouvrir. Le message vous informant de l'activation de la licence va apparaître en bas de l'écran.



Le fichier clé de Dr.Web Security Space ou de l'Antivirus Dr.Web peut être utilisé pour Dr.Web, s'il supporte les composants DrWebGUI et Update.

Pour vérifier la possibilité d'utiliser le fichier clé :

1. Ouvrez le fichier clé dans un éditeur de texte (par exemple, dans le Bloc-notes).
2. Vérifiez si les composants DrWebGUI et Update sont inclus dans la liste des valeurs du paramètre Applications, dans le groupe [Key] : s'ils sont indiqués dans la liste, le fichier clé peut être utilisé pour le fonctionnement de Dr.Web.

Toute modification rend le fichier clé invalide. Pour éviter l'endommagement du fichier, n'enregistrez pas le fichier quand vous fermez l'éditeur de texte.

5.5. Restauration de la licence

La restauration de la licence peut être nécessaire si vous avez réinstallé l'application ou que vous voulez utiliser Dr.Web sur un autre appareil.

Si l'application est installée depuis Google Play

1. Ouvrez l'application.
2. Passez à l'écran [Licence](#).
3. Sur l'écran **Licence**, sélectionnez **J'ai déjà une licence**.
4. Appuyez sur **Restaurer l'achat sur Google Play**.
5. Indiquez vos données personnelles et l'adresse e-mail que vous avez spécifiée pour l'enregistrement de la licence.

La licence enregistrée à l'adresse e-mail spécifiée sera activée automatiquement.

Si l'application a été installée depuis le site de Doctor Web ou depuis Xiaomi GetApps

Vous pouvez restaurer la licence de deux façons :

- [Enregistrer le numéro de série](#).
- [Utiliser le fichier clé](#).

Si l'application est installée depuis HUAWEI AppGallery

1. Ouvrez l'application.
2. Passez à l'écran [Licence](#).
3. Sur l'écran **Licence**, sélectionnez **J'ai déjà une licence**.
4. Appuyez sur **Restaurer l'achat sur HUAWEI AppGallery**.
5. Indiquez vos données personnelles et l'adresse e-mail que vous avez spécifiée pour l'enregistrement de la licence.

La licence enregistrée à l'adresse e-mail spécifiée sera activée automatiquement.



Restauration de la licence de démonstration

1. Ouvrez l'application.
2. Passez à l'écran [Licence](#).
3. Sur l'écran **Licence**, sélectionnez **Obtenir une licence démo de 14 jours**.
4. Indiquez l'adresse e-mail, que vous avez spécifié lors de l'activation de la licence de démonstration, et vos données personnelles.
5. Appuyez sur **Obtenir une version démo**.

5.6. Suspension et annulation de l'abonnement

Si vous utilisez une licence d'abonnement, vous pouvez suspendre l'abonnement pour un délai déterminé ou annuler l'abonnement dans l'application Play Market.

Suspension de l'abonnement



L'abonnement sera suspendu à la fin de la période de facturation en cours. La licence sera valable jusqu'à la suspension de l'abonnement.

Pour suspendre l'abonnement

1. Ouvrez l'application **Play Store**.
2. Appuyez sur l'icône de votre profil Google en haut à droite de l'écran.
3. Sélectionnez **Payments & subscriptions > Subscriptions**.
4. Sélectionnez l'application Dr.Web dans la liste d'abonnements.
5. Sur l'écran **Manage subscription**, sélectionnez **Suspendre les paiements**.
6. Indiquez le délai de suspension de paiements.
7. Confirmez la suspension.

Vous pouvez reprendre l'abonnement suspendu à tout moment avant la fin du délai de suspension de paiements.

Pour reprendre l'abonnement

1. Ouvrez l'application **Play Store**.
2. Appuyez sur l'icône de votre profil Google en haut à droite de l'écran.
3. Sélectionnez **Payments & subscriptions > Subscriptions**.
4. Sélectionnez l'application Dr.Web dans la liste d'abonnements.
5. Sur l'écran **Manage subscription**, sélectionnez **Reprendre**.
6. Confirmez la reprise de paiements.



Annulation de l'abonnement



Si vous désinstallez l'application Dr.Web, votre abonnement ne sera pas résilié.

Après l'annulation de l'abonnement, la licence restera valable jusqu'à la fin de la période de facturation en cours.

Pour résilier l'abonnement

1. Ouvrez l'application **Play Store**.
2. Appuyez sur l'icône de votre profil Google en haut à droite de l'écran.
3. Sélectionnez **Payments & subscriptions** > **Subscriptions**.
4. Sélectionnez l'application Dr.Web dans la liste d'abonnements.
5. Sur l'écran **Manage subscription**, sélectionnez **Annuler l'abonnement**.
6. Sur l'écran **Souhaitez-vous suspendre votre abonnement ?**, appuyez sur **Non**.
7. Sur l'écran **Pour quelle raison annulez-vous votre abonnement ?** sélectionnez l'une des options et appuyez sur **Suivant**.
8. Sur l'écran **Annuler l'abonnement ?**, appuyez sur **Annuler l'abonnement**.

5.7. Renouvellement de la licence

Pour voir les informations sur la licence utilisée :

- **Sous Android**. Appuyez sur **Menu**  et sélectionnez l'élément **Licence** sur l'écran d'accueil de Dr.Web (voir [Figure 8](#)).
- **Sous Android TV**. Allez dans la section **Divers** > **Licence** sur l'[écran d'accueil](#) de Dr.Web.

Sur l'écran **Licence**, vous pouvez regarder le numéro de série, le nom du propriétaire de la licence et les dates d'enregistrement et d'expiration de la licence.

Si vous êtes abonné au service Antivirus Dr.Web, en [mode de protection centralisée](#), l'écran **Licence** affiche aussi la date d'expiration de votre abonnement.

Renouvellement de la licence



La licence d'abonnement achetée via Google Play ne requiert pas le renouvellement manuel. L'abonnement est renouvelé et facturé automatiquement une fois par mois.

Pour renouveler la licence Dr.Web, vous n'avez pas besoin de réinstaller ou d'arrêter l'application.



Vous pouvez renouveler votre licence par un des moyens suivants :

- Si vous avez déjà un nouveau numéro de licence, [enregistrez-le](#).
- Si vous avez acheté votre licence actuelle sur le site de Doctor Web ou dans Xiaomi GetApps, vous pouvez :
 - [Acheter une licence](#).
 - [Utiliser le fichier clé](#).
 - Renouveler la licence dans votre [espace personnel](#) sur le site de Doctor Web.

Pour vous rendre sur cette page, appuyez sur **Menu** , sélectionnez l'élément **A propos**, puis suivez le lien **Mon Dr.Web**.

- Si vous avez acheté votre licence actuelle sur Google Play :
 1. Appuyez sur **Menu**  sur l'écran d'accueil de Dr.Web et sélectionnez l'élément **Licence**.
 2. Sur l'écran **Licence** (voir [Figure 6](#)), appuyez sur **Renouveler la licence de Google Play**.

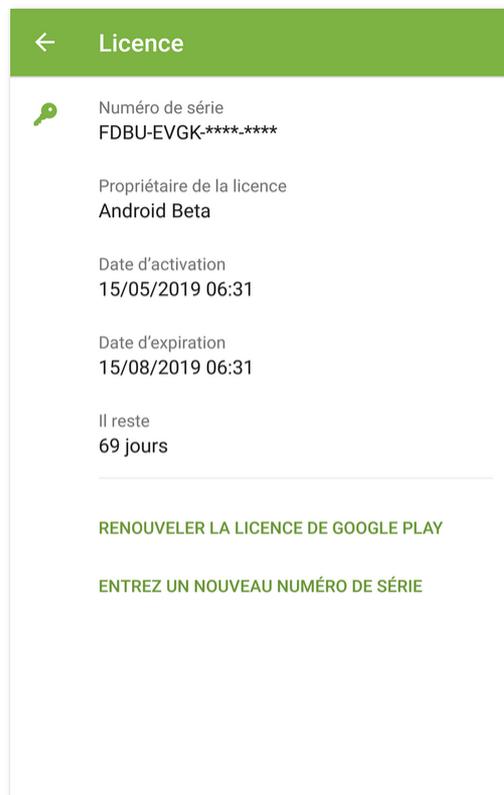


Figure 6. Renouvellement de la licence

3. Sur l'écran **Renouvellement de la licence**, sélectionnez une des options suivantes :
 - **Licence pour 1 an**
 - **Licence pour 2 ans**

Une fois une des variantes sélectionnée, l'écran d'achat de licence s'ouvre. Quelque temps après le paiement, la licence sera activée automatiquement. Le fichier clé de licence sera envoyé à votre adresse e-mail pour confirmer l'achat. Si la licence n'est pas activée à



cause d'une erreur technique, contactez le support technique :

<https://support.drweb.com/>.

- Si vous avez acheté votre licence actuelle sur HUAWEI AppGallery :
 1. Appuyez sur **Menu**  sur l'écran d'accueil de Dr.Web et sélectionnez l'élément **Licence**.
 2. Sur l'écran **Licence**, appuyez sur **Renouveler la licence sur HUAWEI AppGallery**.
 3. Sur l'écran **Renouvellement de la licence**, sélectionnez une des options suivantes :
 - **Licence pour 1 an**
 - **Licence pour 2 ans**

Une fois une des variantes sélectionnée, l'écran d'achat de licence s'ouvre. Quelque temps après le paiement, la licence sera activée automatiquement. Le fichier clé de licence sera envoyé à votre adresse e-mail pour confirmer l'achat. Si la licence n'est pas activée à cause d'une erreur technique, contactez le support technique :

<https://support.drweb.com/>.

5.8. Configuration des notifications d'expiration de la licence

Sur les appareils mobiles, vous pouvez activer les notifications informant de la proche expiration de la licence (sauf l'utilisation de la licence sur abonnement de Google Play).

Pour activer les notifications

1. Appuyez sur **Menu**  et sélectionnez l'élément **Paramètres** (voir [Paramètres](#)) sur l'écran d'accueil Dr.Web.
2. Sélectionnez l'élément **Licence**.
3. Cochez la case **Notifications**.



6. Mise en route

Après l'installation de Dr.Web et l'activation de la licence, vous pourrez prendre connaissance de l'interface et du menu principal de l'application, configurer le panneau de notifications et ajouter le widget Dr.Web sur l'écran d'accueil de l'appareil.

6.1. Contrat de licence

Au premier démarrage de l'application, vous serez invité à lire le Contrat de Licence. Vous devez l'accepter pour continuer à utiliser l'application.

Dans la même fenêtre, vous serez invité à accepter l'accord sur l'envoi des statistiques de fonctionnement de l'application et des menaces détectées sur les serveurs de Doctor Web, Google et Yandex.

A tout moment, vous pouvez refuser d'envoyer les statistiques en décochant la case **Envoi des statistiques** dans la section **Paramètres généraux** des [paramètres](#) de l'application.



Si votre version de Dr.Web est fournie par l'administrateur du [réseau antivirus](#) de l'entreprise, le Contrat de licence ne sera pas affiché.

6.2. Autorisations

A partir de la version 6.0, dans l'OS Android, il existe une option permettant d'autoriser ou d'interdire aux applications l'accès aux fonctions de l'appareil ainsi qu'aux données personnelles.

Une fois Dr.Web installé et le Contrat de licence accepté, accordez les autorisations nécessaires à l'application. Les autorisations peuvent être requises au premier appui sur un des [composants](#) ou au moment du lancement.

- au premier lancement, Dr.Web vous demande d'accorder les autorisations suivantes :
 - L'accès aux photos, médias et fichiers sur l'appareil.
 - Accès à tous les fichiers (sur les appareils tournant sous Android 11.0 ou une version supérieure).

Ces autorisations sont nécessaires pour le fonctionnement de l'application.

- Autorisation d'envoyer les [notifications](#) (sur les appareils tournant sous Android 13.0 ou une version supérieure).

L'autorisation est nécessaire pour que Dr.Web puisse utiliser le panneau de notifications pour afficher les messages sur le statut de protection de l'appareil et le fonctionnement des composants de Dr.Web. Si vous n'accordez pas l'autorisation, Dr.Web ne pourra pas vous



signaler la détection de menaces et les événements des composants avant que vous ouvriez l'application.

- [Filtre des appels et des SMS](#) demande les autorisations suivantes :
 - D'effectuer les appels et de gérer les appels.
 - D'envoyer et de consulter les messages SMS.
 - L'accès aux contacts.
 - L'accès aux notifications.
 - L'accès à la liste d'appels (sur les appareils tournant sous Android 9.0 ou une version supérieure).
 - La permission de définir Dr.Web comme application par défaut pour la détection automatique des numéros de téléphone et la protection contre le spam (sur les appareils tournant sous Android 10.0 ou une version supérieure).
- [Filtre URL](#) demande l'accès aux fonctionnalités spéciales Android pour le fonctionnement dans les navigateurs installés.
- [Antivol Dr.Web](#) demande les autorisations suivantes :
 - L'accès aux appels et à la gestion des appels.
 - La possibilité d'envoyer et de consulter les messages SMS.
 - L'accès aux contacts.
 - L'accès aux notifications.
 - L'accès à la localisation de l'appareil.
 - L'accès aux fonctions spéciales de Android.
 - L'autorisation de désigner Dr.Web l'administrateur de l'appareil.
- [Pare-feu Dr.Web](#) demande les autorisations suivantes :
 - Connexion au réseau VPN pour surveiller le trafic.
 - Superposition au-dessus des autres fenêtres.
- [Dr.Web sous Android TV](#) demande les autorisations suivantes :
 - L'accès aux contacts.
 - L'accès aux photos, médias et fichiers sur l'appareil.
 - Accès à tous les fichiers (sur les appareils tournant sous Android 11.0 ou une version supérieure).



En [mode de protection centralisée](#), les autorisations suivantes sont requises :

- Autorisations principales (l'accès aux photos, médias, fichiers, contacts, etc) : pour le fonctionnement de la plupart des fonctions de l'application.
- Autorisation d'envoyer les notifications (sur les appareils tournant sous Android 13.0 ou une version supérieure) : pour afficher les messages sur le statut de la protection et le fonctionnement des composants.
- Accès à tous les fichiers (sur les appareils tournant sous Android 11.0 ou une version supérieure) - pour l'analyse de l'appareil.



- Filtre des appels et des SMS (en fonction de la version de l'OS Android, voir [ci-dessus](#)) — pour le filtrage d'appels et de SMS.
- Administration de l'appareil : pour la protection de l'application contre la suppression et le fonctionnement complet de l'Antivol.
- Accès aux fonctionnalités spéciales : pour le filtrage des applications et le fonctionnement complet du Filtre URL, de l'Antivol et du Contrôle parental.
- Superposition au-dessus des autres fenêtres : pour le filtrage des applications et le fonctionnement du Pare-feu.

Si vous n'accordez pas les autorisations obligatoires, l'écran **Les permissions sont requises** s'affichera (voir [Figure 7](#)). Vous pouvez accorder toutes les autorisations ou les autorisations obligatoires uniquement. Les autorisations obligatoires pour le fonctionnement des composants sont marquées par l'icône jaune. Les autorisations non obligatoires sont marquées par l'icône grise. Une fois l'autorisation accordée, l'icône devient verte.

Si vous accordez toutes les autorisations requises par le composant, l'activité de l'application se poursuivra automatiquement. Si vous n'accordez que les autorisations obligatoires, vous pourrez continuer à utiliser l'application en appuyant sur le bouton **Continuer**. Vous pourrez accorder les autorisations non obligatoires une autre fois, au moment de l'ouverture de ce composant depuis l'écran d'accueil de Dr.Web ou sur l'écran de paramètres.

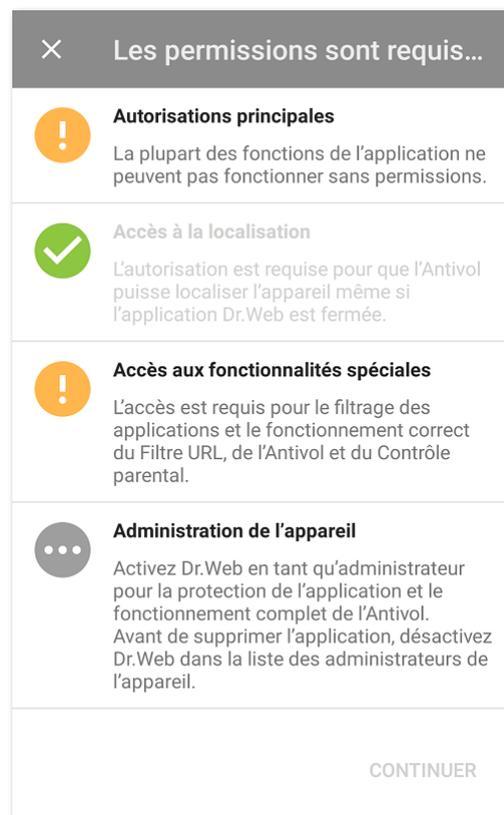


Figure 7. Les permissions sont requises



Si vous refusez une ou plusieurs demandes d'accorder les autorisations obligatoires, vous serez invité à passer sur l'écran de paramètres :

- Sur les appareils tournant sous Android 9.0 ou une version antérieure :
 1. Appuyez sur **Aller aux Paramètres** et sélectionnez la section **Autorisations**.
 2. Sélectionnez l'élément **Mémoire** ou **Stockage** et accordez l'autorisation à l'aide de l'interrupteur.
- Sur les appareils fonctionnant sous Android 10.0 :
 1. Appuyez sur **Aller aux Paramètres** et sélectionnez la section **Autorisations**.
 2. Sélectionnez l'élément **Mémoire** ou **Stockage** dans la catégorie **Accès refusé**, puis sélectionnez l'option **Autoriser**.
- Sur les appareils tournant sous Android 11.0 ou une version supérieure :
 1. Appuyez sur **Aller aux Paramètres** et sélectionnez la section **Autorisations**.
 2. Sélectionnez l'élément **Fichiers et contenus multimédias** ou bien **Stockage** dans la catégorie **Accès refusé** et puis sélectionnez l'option **Autoriser la gestion de tous les fichiers**. En utilisant cette option, vous accordez un accès aux photos et fichiers multimédia ainsi qu'à tous les fichiers.

Pour consulter la liste de toutes les autorisations pour Dr.Web

1. Ouvrez les paramètres de l'appareil .
2. Appuyez sur **Applications** ou **Gestionnaire d'applications**.
3. Trouvez Dr.Web dans la liste des applications installées et appuyez dessus.
4. Sur l'écran **À propos de l'application**, sélectionnez l'élément **Autorisations**.
5. Dans le menu se trouvant en haut à droite, sélectionnez **Toutes les autorisations**.

6.3. Interface

Écran d'accueil

Sur l'écran d'accueil (voir [Figure 8](#)) se trouve la liste des composants principaux de Dr.Web.

Le **Menu**  en haut à droite de l'écran d'accueil permet :

- D'ouvrir l'écran contenant les informations sur la licence.
- D'ouvrir les statistiques.
- D'ouvrir la liste des fichiers mis en quarantaine.
- De lancer manuellement la mise à jour des bases virales.
- D'accéder aux paramètres de l'application.
- D'ouvrir l'aide.
- D'accéder à la gestion du compte.

- D'ouvrir l'écran contenant les informations sur l'application.

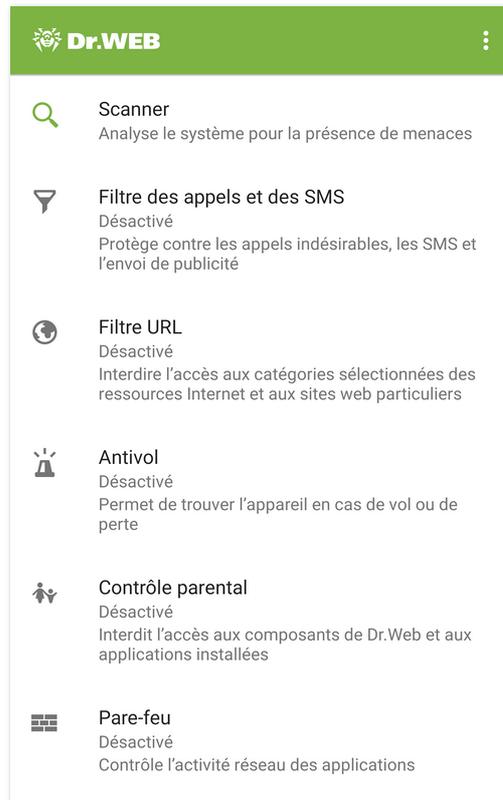


Figure 8. Écran d'accueil de Dr.Web

Barre d'état

Dans la partie supérieure de l'écran d'accueil de Dr.Web se trouve la barre d'état avec l'identificateur qui représente l'état actuel de la protection de l'appareil (voir [Figure 9](#)).

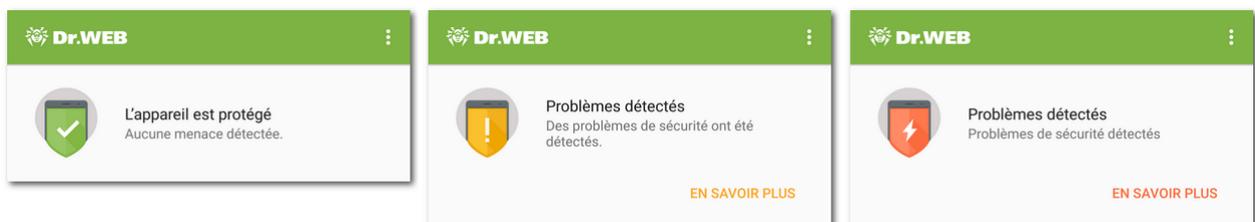


Figure 9. Barre d'état

- L'indicateur vert signifie que l'appareil est protégé. Aucune intervention n'est requise.
- L'indicateur jaune signifie que Dr.Web a détecté des problèmes de sécurité, par exemple, l'absence de la licence ou une vulnérabilité. Pour en savoir plus sur les problèmes détectés et les résoudre, appuyez sur **En savoir plus**.



- L'indicateur rouge signifie que Dr.Web a détecté des modifications suspectes dans la zone système ou des menaces. Pour ouvrir les [résultats du scan](#) et neutraliser les menaces, cliquez sur **En savoir plus**.

Si Dr.Web a détecté plusieurs événements nécessitant l'attention de l'utilisateur, le bouton **En savoir plus** ouvrira la section **Événement** où tous les messages importants seront affichés.

6.4. Notifications

Sur les appareils tournant sous Android 7.0 ou une version supérieure, toutes les notifications Dr.Web sont groupées dans une seule notification déroulante.

Sur les appareils tournant sous Android 8.0 ou une version supérieure, les notifications de Dr.Web sont divisées en catégories ou en chaînes. Vous pouvez gérer chaque catégorie de notifications dans les paramètres de l'appareil. Si vous désactivez une catégorie, vous ne recevrez plus les notifications de cette catégorie. Toutes les catégories sont activées par défaut.

Catégories de notifications

Catégorie	Notifications
Détection d'une menace	<ul style="list-style-type: none">• Notifications des menaces détectées par le composant SpIDer Guard.• Notifications de menaces détectées par le Scanner Dr.Web.
Applications sécurisées	Notifications d'absence des menaces dans les applications et les mises à jour récemment installées. Sur les appareils tournant sous Android 7.1 ou une version antérieure, vous pouvez activer ou désactiver les notifications de cette catégorie dans les paramètres généraux de Dr.Web .
Statut de la protection antivirus	<p>Si le panneau de notifications est désactivé, cette catégorie contient les notifications suivantes :</p> <ul style="list-style-type: none">• Le système est protégé. Elle s'affiche si le composant SpIDer Guard est activé et que l'analyse du Scanner Dr.Web n'est pas lancée.• Notification sur le type de scan du Scanner Dr.Web. Elle s'affiche si un scan rapide, complet ou personnalisé est lancé.• Notification d'analyse du support amovible. Elle s'affiche en cas d'analyse de la carte SD et des supports amovibles par le composant SpIDer Guard. <p>Si le panneau de notifications est activé, une notification s'affiche vous informant de l'analyse en cours, si une des analyses du Scanner Dr.Web est lancée.</p>
Statut des composants supplémentaires	<ul style="list-style-type: none">• Les composants supplémentaires sont activés. Elle s'affiche si le Filtre des appels et des SMS, le Filtre URL, l'Antivol Dr.Web ou le Pare-feu Dr.Web est activé.• L'Agent est activé. Elle s'affiche en mode de protection centralisée si le Filtre des appels et des SMS (tous les appels et les SMS entrants sont autorisés), le Filtre URL, l'Antivol Dr.Web et le Pare-feu Dr.Web sont désactivés.



Catégorie	Notifications
	<ul style="list-style-type: none">• L'Agent et les composants supplémentaires sont activés. Elle s'affiche en mode de protection centralisée si le Filtre des appels et des SMS, le Filtre URL, l'Antivol Dr.Web, ou le Pare-feu Dr.Web est activé.
Notifications des amis	Notifications reçues des amis.
Configuration des composants de protection	Configuration des composants en cours... s'affiche lors de la localisation de l'appareil à la demande de l'ami, si l'Antivol Dr.Web est activé dans la version téléchargée depuis Google Play.
Autres	<ul style="list-style-type: none">• Les permissions sont requises. Elle s'affiche lors de l'ouverture de l'application si l'accès aux photos, multimédias et fichiers a été refusé. Dans la version de l'application obtenue de l'administrateur du réseau antivirus de votre entreprise ou du fournisseur du service Antivirus Dr.Web, la notification s'affiche lors de l'ouverture de l'application si une des autorisations a été refusée.• Notifications de la licence :<ul style="list-style-type: none">▫ Une erreur s'est produite lors de la vérification de la licence. Elle s'affiche si une erreur est survenue lors du scan. Il se peut que la licence soit introuvable ou non approuvée par le Serveur.▫ Jours restants : <nombre de jours>. Elle s'affiche si la licence a expiré et que la case Notifications est cochée dans les paramètres de l'application.▫ La licence a expiré. Elle s'affiche si vous utilisez le service Antivirus Dr.Web et que la licence a expiré.▫ Contactez l'administrateur du réseau antivirus. Elle s'affiche si vous utilisez le service Antivirus Dr.Web et que la licence a été bloquée.• Une nouvelle version de Dr.Web est disponible. Elle s'affiche dans la version téléchargée du site Doctor Web si une nouvelle version est disponible et que la case Nouvelle version est cochée dans les paramètres de l'application.• Notifications de l'Antivol Dr.Web :<ul style="list-style-type: none">▫ Aucune carte SIM trouvée ;▫ Nouvelle carte SIM trouvée.• Notification du Filtre des appels et des SMS Tous les appels et les SMS sont bloqués. Elle s'affiche en cas d'activation du profil Bloquer tous.• Notifications du Pare-feu Dr.Web :<ul style="list-style-type: none">▫ Le Pare-feu Dr.Web est désactivé. Elle s'affiche si la connexion VPN de l'application Dr.Web est interrompue.▫ Limite du trafic mobile est atteinte. Elle s'affiche si la limite spécifiée du trafic mobile est dépassée et que la case Notifications est cochée dans les paramètres du Pare-feu.• Nouveau message. Elle s'affiche en cas de réception d'un message de l'antivirus du réseau antivirus.
Grouper les notifications	Cette catégorie ne contient pas de notifications particulières, mais elle permet de grouper toutes les notifications Dr.Web dans une seule

Catégorie	Notifications
	notification déroulante.

Panneau de notifications

Le panneau de notifications Dr.Web (voir [Figure 10](#)) est utilisé pour un accès rapide aux fonctions principales de l'application. De plus, il affiche rapidement les notifications sur les modifications suspectes dans la zone système et les menaces détectées.

Si Dr.Web détecte des modifications suspectes dans la zone système ou des menaces sur les appareils tournant sous Android 11.0 ou une version antérieure, l'icône de l'application dans le panneau de notifications changera en . Sur les appareils tournant sous Android 12.0 ou une version supérieure, l'icône de l'application changera en  et l'indicateur de statut deviendra rouge .



Figure 10. Panneau de notifications sous Android 11.0 (à gauche) et Android 12.0 (à droite)



Sous [Android TV](#), le panneau de notifications n'est pas disponible.

Pour activer le panneau de notifications Dr.Web

1. Sur l'écran d'accueil Dr.Web, sélectionnez l'élément **Menu**  > **Paramètres**.
2. Sélectionnez **Paramètres généraux**.
3. Activez l'option **Panneau de notifications**.



Sous Android 5.0 ou 5.1, si Dr.Web détecte une modification suspecte dans la zone système ou une menace, le panneau de notifications s'affiche par-dessus toutes les applications jusqu'à ce qu'une action ne soit appliquée à l'objet détecté ou que vous fassiez défiler la notification de menace du panneau de notifications.

Si votre appareil ne supporte pas les cartes SIM, au lieu de l'option **Filtre**, le panneau de notifications contiendra l'option **Téléchargement** permettant de lancer le scan des objets téléchargés.

Si Dr.Web fonctionne en [mode de protection centralisée](#) et que vous n'avez pas les droits de modifier les paramètres du Filtre des appels et des SMS ou du Filtre URL, les options **Filtre** et **Filtre URL** seront indisponibles dans le panneau de notifications.



Avec le panneau de notifications, vous pouvez effectuer les actions suivantes :

- Sur les appareils tournant sous Android 11.0 ou une version antérieure :
 - Ouvrir l'application. Pour ce faire, appuyez sur l'icône .
 - Lancer le scan rapide, complet ou personnalisé. Appuyez sur  **Scanner**.
 - Sélectionner le filtre des appels et des SMS entrants. Appuyez sur  **Filtre**.
 - Sélectionner les catégories des sites auxquels vous voulez limiter l'accès. Appuyez sur  **Filtre URL**.
- Sur les appareils tournant sous Android 12.0 ou une version supérieure :
 - Ouvrir l'application (si l'indicateur de protection est vert). Pour ce faire, appuyez sur .
 - Accordez les autorisations nécessaires pour le fonctionnement de l'application (si l'indicateur est jaune). Appuyez sur .
 - Ouvrir les résultats du scan (si l'indicateur est rouge). Appuyez sur .
 - Lancer le scan rapide, complet ou personnalisé. Appuyez sur .
 - Sélectionner le filtre des appels et des SMS entrants. Appuyez sur .
 - Sélectionner les catégories des sites auxquels vous voulez limiter l'accès. Appuyez sur .
 - Voir l'état de la protection, les actions actuelles et recommandées. Appuyez sur .

6.5. Widget

Pour rendre la gestion de Dr.Web plus facile, vous pouvez ajouter sur l'écran d'accueil de votre appareil un widget spécial permettant d'activer et de désactiver la protection antivirus permanente de SpIDer Guard.



Le widget n'est pas disponible sous [Android TV](#).

Pour ajouter un widget Dr.Web

1. Ouvrez la liste des widgets disponibles sur votre appareil mobile.
2. Dans la liste, sélectionnez le widget Dr.Web.

Le widget sans indicateur signifie que l'appareil est protégé par le composant SpIDer Guard. Le widget à l'indicateur jaune signifie que le composant SpIDer Guard est désactivé (voir [Figure 11](#)). Appuyez sur le widget pour que SpIDer Guard reprenne son fonctionnement.

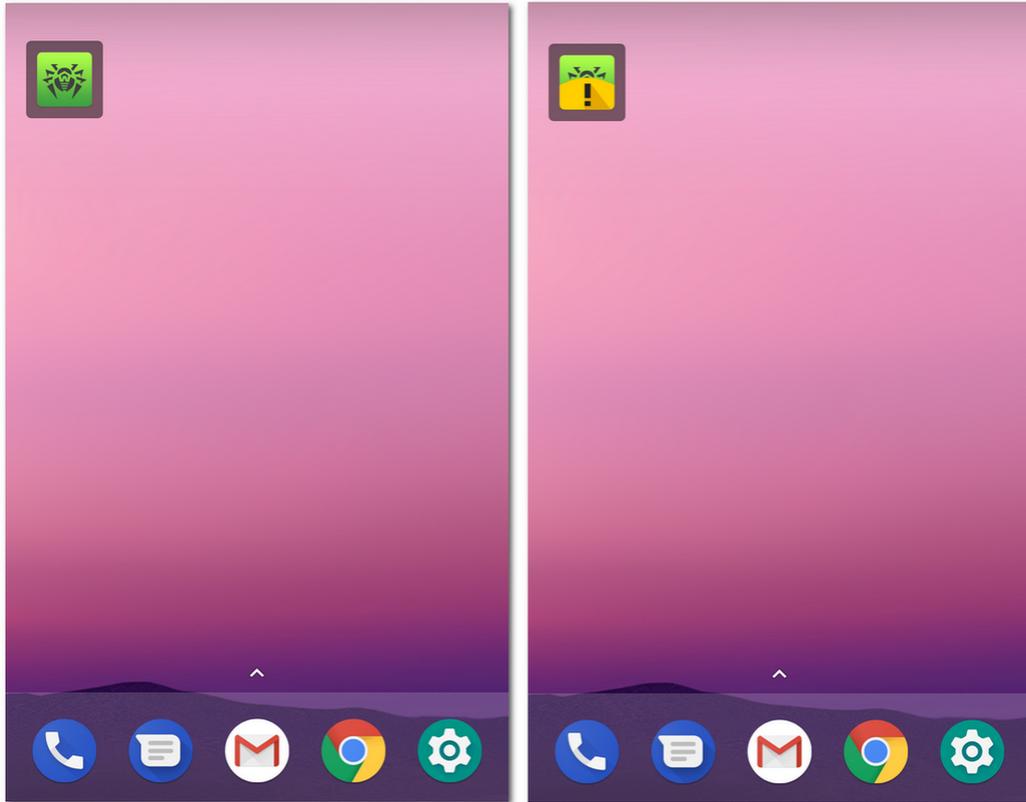


Figure 11. Widget Dr.Web

6.6. Mon Dr.Web

Le service en ligne Mon Dr.Web est votre espace personnel sur le site web officiel de Doctor Web. Cette page fournit des informations sur votre licence (la durée et le numéro de série), l'heure et la date de la dernière mise à jour, le nombre d'entrées dans les bases virales, les actualités et les promotions, et vous permet de renouveler la licence, de contacter le support technique, etc.

Pour ouvrir le service en ligne Mon Dr.Web

1. Dans l'[écran d'accueil](#) Dr.Web, appuyez sur **Menu**  et sélectionnez l'élément **A propos**.
2. Appuyez sur **Mon Dr.Web**.



7. Compte Dr.Web

Le compte Dr.Web permet de protéger par mot de passe ou par empreinte digitale l'accès aux composants de Dr.Web et aux paramètres de l'appareil.

Par défaut, le mot de passe du compte ou l'empreinte digitale est requis :

- Pour accéder aux composants de Dr.Web :
 - Antivol Dr.Web.
 - Contrôle parental.
- Si l'Antivol Dr.Web est activé, pour accéder aux options de l'application :
 - **Réinitialisation des paramètres.**
 - **Copie de sauvegarde.**
 - **Gestion.**
- Si l'Antivol Dr.Web est activé, pour accéder aux paramètres sur votre appareil :
 - **Paramètres**  > **Applications** ou **Gestionnaire d'applications** >  **Dr.Web Security Space** (sous Android 6.0 ou une version supérieure).
 - **Paramètres**  > **Accessibilité.**
 - **Paramètres**  > **Sécurité** > **Localisation** (sous Android 6.0 ou une version supérieure).
 - **Paramètres**  > **Sécurité** > **Administrateurs de l'appareil** >  **Dr.Web Security Space.**
 - **Paramètres**  > **Paramètres avancés** > **Réinitialisation des paramètres** (le nom et le placement du paramètre varient sur des appareils différents).



Sur les appareils Xiaomi, l'accès au paramètre **Économiseur de batterie** est également protégé.

Si le Contrôle parental est activé sur l'appareil, l'empreinte digitale vous permettra d'obtenir l'accès aux sections et aux paramètres listés ci-dessus uniquement si l'option **Déverrouillage par empreinte digitale** est activée dans les paramètres du Contrôle parental.

Vous pouvez protéger par mot de passe ou par empreinte digitale l'accès au Filtre des appels et des SMS et au Filtre URL, ainsi que l'accès aux paramètres de l'application (voir la section [Blocage de l'accès aux applications et aux composants](#)).

Création du compte

1. Sur l'écran d'accueil de Dr.Web, appuyez sur **Menu**  en haut à droite.
2. Sélectionnez l'élément **Compte**.
3. Sur l'écran **Compte**, appuyez sur le bouton **Créer**.
4. Entrez l'adresse e-mail.



Vous pourrez en avoir besoin plus tard si vous oubliez le mot de passe. C'est pourquoi il faut indiquer l'adresse e-mail à laquelle vous avez accès.

Notez qu'une fois le compte enregistré, il est impossible de modifier l'adresse e-mail. Si vous voulez utiliser une nouvelle adresse, il vous faudra supprimer le compte et le créer de nouveau avec la nouvelle adresse e-mail.



Une connexion Internet active est requise pour l'enregistrement de l'adresse e-mail.

5. Appuyez sur **Suivant**.
6. Créez un mot de passe. Le mot de passe doit contenir au moins 4 caractères.
7. Entrez le mot de passe de nouveau et appuyez sur **Suivant**.
Sur l'écran suivant, vous verrez la confirmation de la création réussie du compte.
8. Appuyez sur **Terminer**.

Gestion du compte

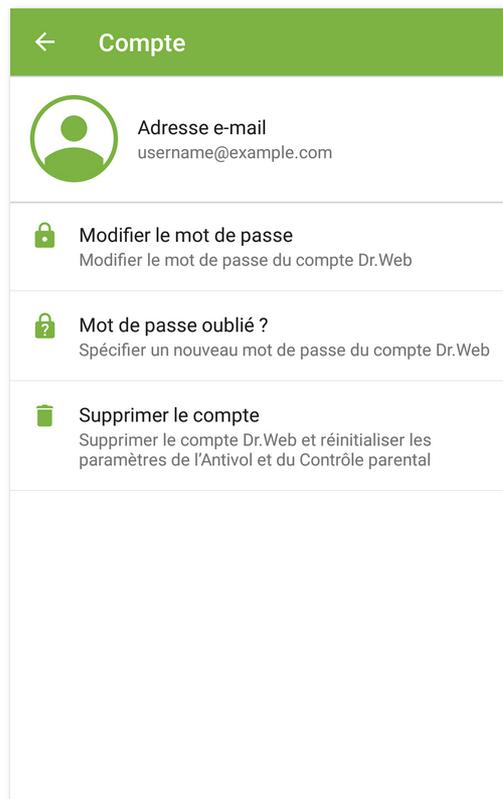


Figure 12. Compte

Sur l'écran **Compte** (voir [Figure 12](#)), vous pouvez effectuer les actions suivantes :

- Modifier le mot de passe.
- Si vous avez oublié le mot de passe, vous pouvez [créer un nouveau mot de passe](#).



- Supprimer le compte.



En cas de suppression du compte, les composants Antivol et Contrôle parental seront désactivés et leurs paramètres seront réinitialisés.

Pour modifier le mot de passe ou supprimer le compte, entrez le mot de passe actuel du compte ou scannez l'empreinte digitale.



8. Composants de Dr.Web

Sur l'écran d'accueil de Dr.Web, vous trouverez la liste des composants et leur état actuel (activé ou désactivé) :

- [Scanner](#) analyse le système à la demande de l'utilisateur. Trois types de scan sont possibles : scan rapide, scan complet et scan personnalisé.
- [Filtre des appels et des SMS](#) bloque les appels et les SMS indésirables.
- [Filtre URL](#) limite l'accès de l'utilisateur aux ressources Internet.
- [Antivol](#) permet de trouver et de bloquer l'appareil en cas de vol ou de perte.
- [Contrôle parental](#) spécifie les restrictions d'utilisation de l'appareil.
- [Pare-feu](#) contrôle les connexions Internet et le transfert de données via réseau.
- [Contrôleur de sécurité](#) effectue l'analyse du système et résout les problèmes de sécurité et les vulnérabilités détectées.



Si l'utilisation de la carte SIM n'est pas prévue pour votre appareil (il n'y a pas de logement de la carte SIM), le **Filtre des appels et des SMS** et l'**Antivol Dr.Web** ne sont pas disponibles.

8.1. Protection antivirus

- [SpIDer Guard](#) analyse le système de fichiers en temps réel.
- Le [Scanner Dr.Web](#) permet de lancer l'analyse manuellement.
- Sur l'écran [Résultats du scan](#), vous pouvez sélectionner des actions pour neutraliser les menaces détectées.

8.1.1. SpIDer Guard : protection antivirus constante

SpIDer Guard s'active automatiquement, une fois le Contrat de licence accepté. Le composant fonctionne indépendamment du fait que l'application soit lancée ou non. Si SpIDer Guard est activé, l'icône Dr.Web  s'affiche dans la barre d'état Android.

Sur certains appareils, l'icône Dr.Web peut ne pas s'afficher quand l'application fonctionne en arrière-plan. Cela peut arriver car le firmware de l'appareil optimise les processus en arrière-plan pour économiser la batterie et augmenter les performances. Pour épingler l'icône Dr.Web dans la barre d'état Android, enlevez les limitations de l'application en arrière-plan : vérifiez les paramètres de l'appareil et du gestionnaire d'applications intégré. Les paramètres dépendent du modèle de l'appareil. Souvent, il suffit d'appuyer sur l'icône de cadenas de l'application Dr.Web dans les applications récentes.

SpIDer Guard protège le système même si l'icône Dr.Web ne s'affiche pas dans la barre d'état. Si une application malveillante est installée, le composant réagira tout de suite et affichera une



notification de menace. Vous pouvez [vérifier le fonctionnement de SplDer Guard](#) à l'aide du fichier de test EICAR.

Si SplDer Guard détecte une modification suspecte dans la zone système ou une menace, l'écran affichera :

- L'icône dans la barre d'état d'Android en haut à gauche de l'écran :
 -  — sous Android 4.4,
 -  — sous Android 5.0–11.0,
 -  — sous Android 12.0 ou une version supérieure.
- Notification pop-up de détection de menace (voir [Figure 13](#)).
- Icône  (sous Android 11.0 ou une version antérieure) ou  (sous Android 12.0 ou une version supérieure) dans la [barre d'état](#).
- Le message avec l'indicateur rouge dans la [barre d'état](#).

Pour ouvrir les résultats du scan, appuyez sur l'icône  () ou sur le message dans la barre d'état.



SplDer Guard s'arrête si vous nettoyez la mémoire interne de votre appareil avec le Gestionnaire des tâches intégré. Dans ce cas, il faut rouvrir Dr.Web pour réactiver la protection antivirus permanente.

Pour désactiver et activer SplDer Guard de nouveau

1. Appuyez sur **Menu**  sur l'écran d'accueil de Dr.Web et sélectionnez l'élément **Paramètres**.
2. Sur l'écran **Paramètres**, sélectionnez **SplDer Guard**.

Paramètres de SplDer Guard



En [mode de protection centralisée](#), les paramètres du composant SplDer Guard peuvent être modifiés ou bloqués conformément à la politique de sécurité de l'entreprise ou à la liste des services payés.

Pour ouvrir les paramètres de SplDer Guard

1. Appuyez sur **Menu**  sur l'écran d'accueil de Dr.Web et sélectionnez l'élément **Paramètres**.
2. Sur l'écran **Paramètres**, sélectionnez **SplDer Guard**.

Fichiers archivés

Pour activer le scan des fichiers dans les archives, cochez la case **Fichiers archivés**.



Par défaut, l'analyse des archives est désactivée. L'activation de l'analyse des archives peut affecter les performances du système et augmenter la consommation de la batterie. Dans ce cas, même si l'analyse des archives est désactivée, la protection reste fiable, parce que SpIDer Guard analyse les fichiers d'installation APK indépendamment de la valeur spécifiée pour **Fichiers archivés**.

Carte SD intégrée et supports amovibles

Pour activer le scan de la carte SD intégrée ou des supports amovibles lors de chaque montage, cochez la case **Carte SD intégrée et supports amovibles**. Si ce paramètre est activé, l'analyse est lancée à chaque activation de SpIDer Guard. De plus, une [notification](#) correspondante s'affiche.

Zone système

Pour suivre les [modifications dans la zone système](#), cochez la case **Zone système**. Si ce paramètre est activé, SpIDer Guard suit les modifications (ajout, modification et suppression des fichiers) et vous informe de la suppression de tous les fichiers, ainsi que de l'ajout ou de la modification des fichiers exécutables : `.jar`, `.odex`, `.so`, fichiers aux formats APK, ELF, etc.

Nouvelle analyse de la zone système

Pour relancer l'analyse de la zone système, appuyez sur **Nouvelle analyse de la zone système**. SpIDer Guard analysera de nouveau toutes les modifications dans la zone système qui ont été ignorées auparavant.

Notifications de la zone système

Pour activer la notification de la modification de tous les fichiers dans la zone système (non seulement des fichiers exécutables), cochez la case **Notifications de la zone système**.

Options supplémentaires

Pour activer l'analyse du système pour la présence des adwares et des riskwares (y compris les hacktools et les canulars), sélectionnez l'élément **Options supplémentaires**, et cochez les cases **Adwares** et **Riskwares**.

Statistiques

L'application enregistre les événements liés au fonctionnement de SpIDer Guard : activation/désactivation, détection des menaces de sécurité et résultats du scan de la mémoire de l'appareil et des applications installées. Les statistiques de SpIDer Guard sont affichées dans

la section **Événement** de l'onglet **Statistiques**. Les statistiques sont triées par date (voir la rubrique [Statistiques](#)).

Vérification du fonctionnement de SpIDer Guard

Vous pouvez vérifier le fonctionnement de SpIDer Guard à l'aide du fichier de test EICAR. D'habitude, ce fichier est utilisé pour :

- Vérifier si l'Antivirus est installé correctement.
- Démontrer le comportement de l'antivirus face à une menace détectée.
- Vérifier le règlement de l'entreprise en cas de détection d'une menace.

Le fichier n'est pas un virus et il ne contient pas de fragments de code de virus, c'est pourquoi il est inoffensif pour votre appareil. Le fichier est considéré par Dr.Web comme « EICAR Test File (NOT a Virus!) ».

Vous pouvez télécharger le fichier sur Internet ou créer le fichier vous-même :

1. Dans un éditeur de texte, créez un nouveau fichier contenant une seule ligne :

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

2. Enregistrez le fichier avec l'extension `.com`.

Une fois le fichier EICAR sauvegardé sur votre appareil, une notification pop-up de SpIDer Guard s'affiche (voir [Figure 13](#)).



Figure 13. Détection du fichier de test EICAR sous Android 10.0 (à gauche) et Android 12.0 (à droite)

8.1.2. Scanner Dr.Web : scan sur demande de l'utilisateur

Le composant Scanner Dr.Web effectue le scan du système sur demande de l'utilisateur. Il permet d'effectuer le scan rapide ou complet du système de fichiers, ainsi que de scanner des dossiers et des fichiers particuliers.

Il est fortement recommandé de scanner périodiquement le système de fichiers, notamment si le composant SpIDer Guard n'a pas été actif pendant quelque temps. D'habitude, il suffit d'effectuer un scan rapide.



En [mode de protection centralisée](#), les paramètres du Scanner Dr.Web peuvent être modifiés ou bloqués conformément à la politique de sécurité de votre entreprise ou à la liste des services payés. Le scan peut être lancé selon la planification spécifiée sur le serveur de protection centralisée.

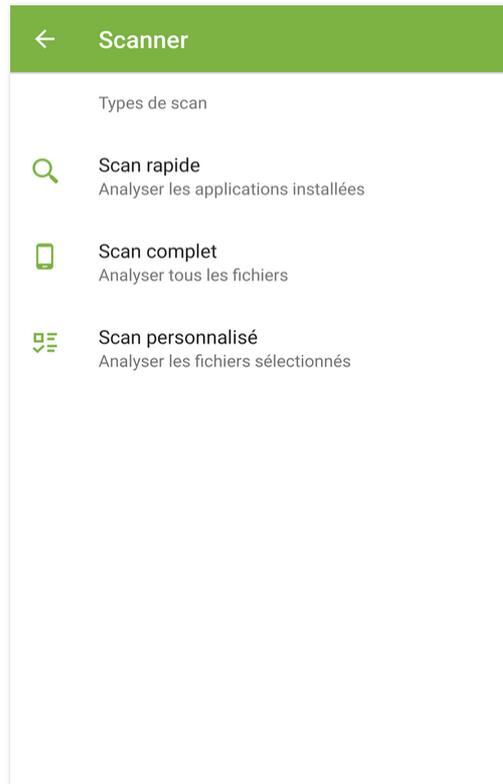


Figure 14. Scanner Dr.Web

Analyse

Pour analyser le système, sélectionnez l'élément **Scanner** sur l'écran d'accueil de Dr.Web. Ensuite, effectuez l'une des actions suivantes sur l'écran **Scanner** (voir [Figure 14](#)) :

- Pour scanner seulement les applications installées, sélectionnez l'élément **Scan rapide**.
- Pour scanner tous les fichiers, sélectionnez l'élément **Scan complet**.
- Pour analyser certains dossiers et fichiers, appuyez sur **Scan personnalisé**, puis sélectionnez les objets à scanner dans la liste des objets du système de fichiers (voir [Figure 15](#)). Pour sélectionner tous les objets, cochez la case en haut à droite de l'écran. Ensuite, appuyez sur **Scan**.

Si votre appareil est rooté, vous pouvez sélectionner pour l'analyse les dossiers `/sbin` et `/data` situés dans le dossier racine.

Sur les appareils tournant sous Android 11.0 ou 12.0, il faut accorder à Dr.Web l'autorisation d'accéder aux dossiers `/Android/data` et `/Android/obb` pour pouvoir les analyser.

Pour autoriser l'accès au dossier `/Android/data` ou `/Android/obb`

1. Sélectionnez l'élément **Scan personnalisé**.

2. Sélectionnez le dossier `/Android/data` ou `/Android/obb` dans la liste d'objets du système de fichiers.
3. Dans la boîte de dialogue, appuyez sur **Autoriser**.
4. Appuyez sur **Utiliser ce dossier**.

Sur les appareils tournant sous Android 13.0 ou une version supérieure, les dossiers `/Android/data` et `/Android/obb` sont protégés par le système et ne sont pas disponibles pour l'analyse.

Si lors d'une analyse, le Scanner Dr.Web détecte des menaces, l'icône  apparaîtra en bas de l'écran de scan. Appuyez sur cette icône pour ouvrir les résultats du scan (voir [Figure 16](#)) et [neutraliser les menaces](#). Si vous avez fermé l'écran de scan ou que vous avez fermé l'application, vous pouvez ouvrir les résultats de l'analyse en appuyant sur l'icône dans le [panneau de notifications](#).

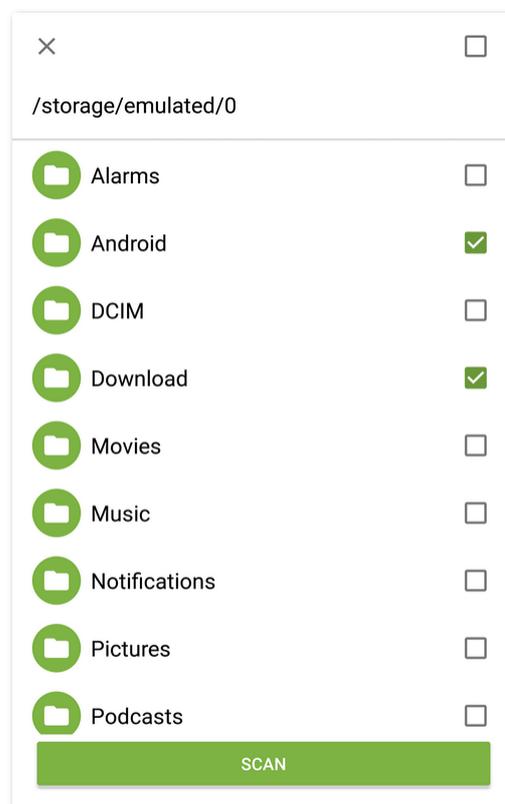


Figure 15. Analyse personnalisée

Envoi des fichiers suspects au laboratoire antivirus de Doctor Web

Vous pouvez envoyer au laboratoire antivirus de Doctor Web des archives ZIP suspectes (des fichiers ayant l'extension `.jar`, `.apk`) probablement contenant des virus, des fichiers ayant l'extension `.odex`, `.dex`, `.so` ou des archives ZIP saines provoquant un faux positif.



Pour envoyer un fichier au laboratoire

1. Appuyez et maintenez le fichier dans la liste des objets du système de fichiers (voir [Figure 15](#)), puis appuyez sur le bouton **Envoyer au Laboratoire**.
2. Sur l'écran suivant, entrez votre adresse e-mail, si vous voulez recevoir les résultats de l'analyse du fichier envoyé.
3. Sélectionnez une catégorie de votre requête :
 - **Fichier suspect**, si vous croyez que le fichier représente une menace.
 - **Faux positif**, si vous croyez que le fichier est considéré comme menace par erreur.
4. Appuyez sur **Envoyer**.



Vous pouvez envoyer au laboratoire antivirus de Doctor Web des fichiers dont la taille ne dépasse pas 250 Mo.

Paramètres du Scanner Dr.Web

Pour accéder aux paramètres du Scanner Dr.Web, ouvrez l'écran [Paramètres](#) et sélectionnez l'élément **Scanner**.

- Pour activer le scan des fichiers dans les archives, cochez la case **Fichiers archivés**.



Par défaut, l'analyse des archives est désactivée. L'activation de l'analyse des archives peut affecter les performances du système et augmenter la consommation de la batterie. Dans ce cas, même si l'analyse des archives est désactivée, la protection reste fiable, car le Scanner Dr.Web analyse les fichiers d'installation APK indépendamment de la valeur spécifiée pour **Fichiers archivés**.

- Pour activer/désactiver le scan pour la présence des adwares et des riskwares (y compris les hacktools et les canulars), sélectionnez l'élément **Options supplémentaires**, puis cochez/décochez les cases **Adwares** et **Riskwares**.

Statistiques

L'application enregistre les événements liés au fonctionnement du Scanner Dr.Web (le mode et les résultats du scan, la détection des menaces de sécurité). Les actions de l'application sont affichées dans la section **Événement** de l'onglet **Statistiques**. Les actions sont triées par date (voir la rubrique [Statistiques](#)).

8.1.3. Résultats du scan

Comment ouvrir les résultats du scan

- Si le Scanner Dr.Web détecte des menaces, l'icône  apparaîtra sur l'écran de scan. Pour ouvrir les résultats du scan, appuyez sur cette icône.
 - Si SpIDer Guard détecte une modification suspecte dans la zone système ou une menace, l'écran affichera :
 - L'icône dans la barre d'état d'Android en haut à gauche de l'écran :
 -  — sous Android 4.4,
 -  — sous Android 5.0–11.0,
 -  — sous Android 12.0 ou une version supérieure.
 - Notification pop-up de détection de menace (voir [Figure 13](#)).
 - Icône  (sous Android 11.0 ou une version antérieure) ou  (sous Android 12.0 ou une version supérieure) dans la barre d'état.
 - Le message avec l'indicateur rouge dans la barre d'état.
- Pour ouvrir les résultats du scan, appuyez sur l'icône  () ou sur le message dans la barre d'état.



Sous Android 5.0 ou une version supérieure, une notification de menace s'affiche sur l'écran de verrouillage de l'appareil. Depuis cet écran vous pouvez accéder aux résultats du scan.

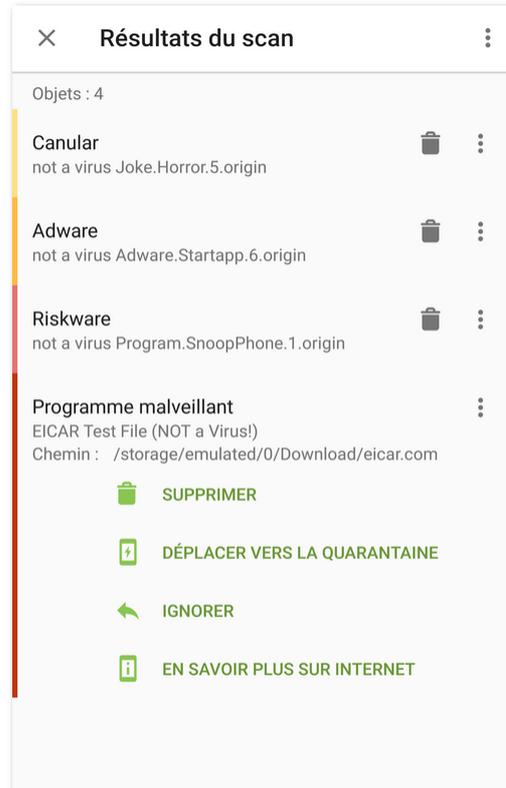


Figure 16. Résultats du scan

Neutralisation des menaces

Sur l'écran **Résultats du scan**, vous pouvez consulter la liste de menaces ou de modifications suspectes dans la zone système. Le type et le nom sont indiqués pour chaque objet, ainsi que l'icône de l'option recommandée pour cet objet.

Les objets sont marqués de couleurs différentes en fonction du niveau de danger. Types d'objets classés dans l'ordre décroissant de danger :

1. Programme malveillant.
2. Riskware.
3. Hacktool.
4. Adware.
5. Modifications dans la zone système :
 - Nouveaux fichiers dans la zone système.
 - Modification de fichiers système.
 - Suppression de fichiers système.
6. Canular.



Pour voir le chemin d'accès au fichier, sélectionnez l'objet correspondant. Le nom de package de l'application est également indiqué pour les menaces détectées dans les applications.

Neutralisation de toutes les menaces

Pour supprimer toutes les menaces en même temps

- Sélectionnez **Menu**  > **Supprimer tout** en haut à droite de l'écran **Résultats du scan**.

Pour déplacer toutes les menaces en quarantaine en même temps

- Sélectionnez **Menu**  > **Mettre tout en quarantaine** en haut à droite de l'écran **Résultats du scan**.

Neutralisation de menaces une par une

Un ensemble d'options est disponible pour chaque objet. Pour ouvrir une liste d'options, sélectionnez un objet. Les options recommandées sont les premières dans la liste. Sélectionnez l'une des options suivantes :

 **Désinfecter** : pour désinfecter une application infectée.

L'option est disponible pour certaines [menaces se trouvant dans les applications système](#), si l'accès root est autorisé.

 **Supprimer** : pour supprimer définitivement la menace de l'appareil.

Dans certains cas, Dr.Web ne peut pas supprimer les applications qui utilisent les fonctionnalités spéciales d'Android. Si vous sélectionnez l'option **Supprimer**, mais Dr.Web ne supprime pas l'application, passez en mode sécurisé et supprimez l'application manuellement. Si Dr.Web a l'accès aux fonctionnalités spéciales, la suppression se fera automatiquement une fois l'option **Supprimer** sélectionnée.

L'option n'est pas disponible pour les [menaces se trouvant dans les applications système](#) dans les cas suivants :

- Si l'accès root n'est pas autorisé sur l'appareil.
- Si la suppression de l'application peut provoquer la perte d'efficacité de l'appareil.
- Si une modification de menace est détectée. Pour déterminer si l'application présente une menace, signalez un faux positif.

 **Déplacer vers la Quarantaine** : pour déplacer une menace dans le dossier isolé (voir la rubrique [Quarantaine](#)).

Si la menace est détectée dans une application installée, il n'est pas possible de la placer en quarantaine. Dans ce cas, l'option **Déplacer vers la Quarantaine** n'est pas disponible.

 **Ignorer** : pour laisser intacte pour le moment la modification de la zone système ou la menace.



 **Bloquer**, pour bloquer l'accès de l'application aux connexions Internet.

L'option est disponible pour les [menaces se trouvant dans les applications système](#).

 **Envoyer au Laboratoire** ou **Faux positif** : pour envoyer le fichier pour l'analyse au laboratoire antivirus de Doctor Web. L'analyse montrera si le fichier présente un danger ou qu'il s'agit d'un faux positif. Si c'est un faux positif, il sera corrigé. Pour obtenir les résultats de l'analyse, indiquez l'adresse e-mail.

Si le fichier est envoyé avec succès au laboratoire, l'action **Ignorer** s'applique automatiquement à l'objet.

L'option **Envoyer au Laboratoire** est disponible uniquement pour les fichiers ajoutés ou les fichiers exécutables modifiés dans la zone système : .jar, .odex, .so, fichiers aux formats APK, ELF, etc.

L'option **Faux positif** est disponible uniquement pour les modifications des menaces et pour les menaces détectées dans la zone système.

 **En savoir plus sur Internet** pour ouvrir la page contenant la description de l'objet détecté sur le site de Doctor Web.

8.1.3.1. Menaces dans les applications système

Les applications installées dans la zone système peuvent, dans certains cas, réaliser les fonctions typiques pour les programmes malveillants. C'est pour cette raison, Dr.Web peut considérer ces applications comme des menaces.

L'option **Bloquer** est disponible pour les applications système. Sélectionnez-la pour que le Pare-feu Dr.Web bloque toutes les connexions Internet pour l'application considérée comme une menace.

L'option **Déplacer vers la Quarantaine** n'est pas disponible pour les applications système et pour toutes les applications installées.

Si l'application système peut être désinfectée ou supprimée sans perte d'efficacité de l'appareil, l'option correspondante sera disponible. Pour cela, l'accès root doit être autorisé.

Si l'application système ne peut pas être supprimée sans perte d'efficacité de l'appareil, l'option **Supprimer** ne sera pas disponible, mais vous pouvez suivre les recommandations suivantes :

- Arrêtez l'application dans les paramètres de l'appareil. Sélectionnez l'application considérée comme une menace dans la liste de l'écran **Paramètres > Applications**, puis sur l'écran contenant les informations sur cette application, appuyez sur **Arrêter**.



Il est nécessaire de répéter cette action à chaque fois que l'appareil est redémarré.



- Désactivez l'application dans les paramètres de l'appareil. Sélectionnez l'application considérée comme une menace dans la liste de l'écran **Paramètres** > **Applications**, puis sur l'écran contenant les informations sur cette application, appuyez sur **Désactiver**.
- Si un firmware personnalisé est installé sur votre appareil, vous pouvez restaurer les paramètres par défaut et revenir au système officiel du fabricant de votre appareil vous-même ou en s'adressant au centre de services.
- Si vous utilisez le système d'exploitation officiel, veuillez contacter le fabricant de votre appareil pour en savoir plus sur cette application.
- Si votre appareil est rooté, vous pouvez supprimer cette application à l'aide d'outils spéciaux.

Pour désactiver la notification de détection des menace dans les applications système qui ne peuvent pas être supprimées sans perte d'efficacité de l'appareil, cochez la case **Applications systèmes** dans la section **Paramètres** > **Paramètres généraux** > **Options supplémentaires**.



Sous Android TV, cochez la case **Applications systèmes** dans la section **Divers** > **Paramètres** > **Paramètres généraux** > **Options supplémentaires**.

8.1.3.2. Modifications dans la zone système

Zone système : une zone de mémoire qui est utilisée par les applications système et contient des données critiques pour le fonctionnement de l'appareil et des données sensibles des utilisateurs. Si votre appareil n'est pas rooté, vous ne pouvez pas accéder à la zone système.

Des applications malveillantes peuvent obtenir un accès root et modifier la zone système : supprimer, ajouter ou modifier les fichiers et les dossiers.

Le composant SplDer Guard peut suivre les modifications dans la zone système. Vous pouvez activer l'analyse de la zone système dans les [paramètres de SplDer Guard](#). Si le composant détecte des modifications suspectes, il vous en informera.

Modification	Nom	Type
Suppression d'un dossier avec des fichiers	read-only.area.dir.deleted.threat	Suppression de fichiers système
Suppression d'un fichier	read-only.area.deleted.threat	Suppression de fichiers système
Ajout d'un dossier avec des fichiers	read-only.area.dir.added.threat	Nouveaux fichiers dans la zone système
Ajout d'un fichier	read-only.area.added.threat	Nouveaux fichiers dans la zone système
Modification d'un fichier	read-only.area.changed.threat	Modification de fichiers système



Si SplDer Guard détecte l'une des modifications ci-dessus, sachez que les fichiers ou dossiers ne sont pas forcément malveillants mais la modification peut être effectuée par une application malveillante.

Les options suivantes sont disponibles pour les modifications détectées :

- [Ignorer](#).
- [Envoyer au Laboratoire](#) : disponible uniquement en cas d'ajout ou de modification de fichiers exécutables : .jar, .odex, .so, fichiers aux formats APK, ELF, etc.
- [En savoir plus sur Internet](#).

SplDer Guard vous informe simplement des modifications ci-dessus. Pour détecter une application malveillante qui aurait pu apporter des modifications dans la zone système, effectuez un [scan complet](#) de l'appareil.

8.1.3.3. Menaces utilisant la vulnérabilité Stagefright

La vulnérabilité Stagefright permet de pirater un appareil à l'aide d'un fichier média contenant un code malveillant.

Les menaces utilisant la vulnérabilité Stagefright sont détectées et neutralisées par le [Pare-feu Dr.Web](#). Activez-le pour assurer la protection contre les exploits Stagefright.

Le Pare-feu Dr.Web analyse en temps réel le contenu des fichiers média que vous téléchargez sur l'appareil. Si Dr.Web détecte un code malveillant dans le fichier que vous téléchargez sur votre appareil :

- Le téléchargement du fichier sera interrompu.
- En bas de l'écran, vous verrez une notification avec l'icône . Le nom de la menace détectée aura l'extension <nom.de.la.menace>. Stagefright.
- Une entrée sur la menace détectée sera inscrite dans les [statistiques](#) de fonctionnement de l'application.

8.1.4. Applications bloqueurs de l'appareil

Dr.Web permet de protéger l'appareil mobile contre les ransomwares. Ces logiciels représentent un danger important. Ils chiffrent les fichiers stockés dans la mémoire interne de l'appareil et sur les supports amovibles (comme, par exemple, la carte SD). Ces programmes peuvent verrouiller l'écran et afficher des messages exigeant une rançon pour le décryptage des fichiers et le déverrouillage de l'appareil.

Les ransomwares peuvent endommager vos photos, vos vidéos et vos documents. De plus, ils volent et envoient sur le serveur de malfaiteurs des données sur l'appareil infecté (y compris l'identifiant IMEI), les contacts (noms, numéros de téléphone et e-mails), ils surveillent les appels sortants et entrants et ils peuvent les bloquer. Toutes les données recueillies, y compris les informations sur les appels, sont envoyées sur un serveur de gestion.



Dr.Web détecte et supprime les ransomwares lors de leur tentative de pénétrer dans l'appareil protégé. Pourtant ces programmes malveillants se caractérisent par une évolution et une modification rapides, c'est pourquoi un bloqueur peut être installé sur l'appareil mobile, surtout si les bases virales Dr.Web ne sont pas mises à jour depuis un moment et elles ne contiennent pas d'informations sur de nouveaux exemplaires.

Si votre appareil est bloqué par un ransomware et que SpIDer Guard est activé, vous pouvez débloquer l'appareil.

Pour débloquer l'appareil

1. Dans les 5 secondes, branchez et débranchez un chargeur.
2. Dans les 10 secondes suivantes, branchez des écouteurs.
3. Dans les 5 secondes suivantes, débranchez les écouteurs.
4. Dans les 10 secondes suivantes, secouez vivement votre appareil.
5. Dr.Web termine tous les processus actifs sur l'appareil, y compris le processus lancé par le bloqueur, puis un court signal de vibration s'active (sur les appareils ayant cette fonction). Ensuite, l'écran Dr.Web s'ouvre.



Attention ! L'arrêt des processus actifs peut causer la perte des données non sauvegardées des applications qui étaient actives au moment du blocage de l'appareil.

6. Après le déblocage de l'appareil, il est recommandé de [mettre à jour](#) les bases virales Dr.Web et de lancer le [scan rapide](#) du système, ou bien de supprimer le logiciel malveillant.

8.2. Filtre des appels et des SMS

Le Filtre des appels et des SMS bloque les appels et les messages SMS non-sollicités, par exemple, la publicité ou les appels et les messages provenant de numéros inconnus et privés.

Vous pouvez activer le filtre de blocage ou le filtre d'autorisation.

- Le filtre de blocage bloque les contacts, les mots-clés ou les [masques](#) ajoutés.
- Le filtre d'autorisation autorise seulement les appels et les SMS provenant de certains contacts ou des [masques](#) ajoutés.

Si un filtre est activé, l'autre se désactive.

Vous pouvez choisir un profil des listes standard ou créer votre propre profil pour le filtrage.



Le filtre SMS ne marche pas dans les versions de l'application installées depuis Google Play.

Sur les appareils ayant deux cartes SIM le fonctionnement correct du Filtre n'est pas garanti.

Le filtre SMS peut ne pas fonctionner correctement à cause des limitations techniques d'Android. Les messages bloqués peuvent s'afficher dans le journal de SMS.

En [mode de protection centralisée](#), les paramètres de filtrage, peuvent être modifiés ou bloqués conformément à la politique de sécurité de votre entreprise ou à la liste des services payés.

Autorisations

Au premier démarrage, le Filtre des appels et des SMS peut demander les autorisations suivantes :

- D'accéder aux contacts.
- D'effectuer les appels et de gérer les appels.
- D'envoyer et de consulter les messages SMS.

Appuyez sur **Autoriser** dans chaque fenêtre.

Sur les appareils tournant sous Android 9.0 ou une version supérieure, le Filtre des appels et des SMS demande également l'accès à la liste d'appels.

Sur les appareils tournant sous Android 10.0 ou une version supérieure, le Filtre des appels et des SMS demande également l'autorisation d'utiliser Dr.Web comme application par défaut pour la détection automatique des numéros de téléphone et la protection contre le spam.

Le composant ne fonctionnera pas sans autorisations nécessaires.



Si vous utilisez un téléphone Xiaomi avec l'application **Sécurité** installée, autorisez Dr.Web à gérer les SMS dans cette application.

8.2.1. Filtre de blocage

Le filtre de blocage bloque les appels et les SMS de certains contacts ajoutés.

Comment utiliser le filtre de blocage

- Activer l'option **Bloquer tous** pour bloquer tous les appels et les SMS entrants.
- Ajouter les contacts à **Liste noire**.
- Créer ses propres listes.



Pour créer une liste

1. Ouvrez le filtre de blocage.
2. Appuyez sur l'icône .
3. Indiquez le nom de la liste.
4. Ajoutez les contacts ou les mots-clés. Vous ne pourrez pas enregistrer une liste vide.

Pour ajoutez les contacts dans la liste

1. Sur l'écran de la liste nécessaire, appuyez sur l'icône . Sélectionnez une des options suivantes :

 **Contacts** : ajouter un contact depuis vos contacts sur l'appareil.

 **Journal des appels** : ajouter un contact depuis la liste des appels récents. Disponible seulement dans la version téléchargée du site.

 **Journal des SMS** : ajouter un contact depuis les SMS récents. Disponible seulement dans la version téléchargée du site.

 **Mot-clé** : ajouter un mot-clé pour le blocage des SMS. Disponible seulement dans la version téléchargée du site.

Dr.Web cherchera dans les messages le mot ou le groupe de mots que vous aurez ajoutée. Si vous voulez que l'application bloque les messages contenant plusieurs mots détachés, ajoutez-les un par un.

 **Numéro privé** : bloquer les appels de tous les numéros privés. Disponible seulement dans la version téléchargée depuis Google Play. Dans la version de site ou dans la version téléchargée depuis HUAWEI AppGallery, vous pouvez ajouter un numéro privé depuis le journal d'appels ou de SMS.

 **Nouveau contact** : créer un nouveau contact ou un [masque](#).

 **Importation des contacts** : importer la liste des contacts enregistrée précédemment.

2. Si nécessaire, éditez le nom et le numéro de téléphone de chaque contact, sélectionnez ce que vous voulez bloquer : **Appels** ou **SMS**. Il est impossible d'éditer un numéro privé et un numéro ajouté depuis vos contacts.

Pour enregistrer les contacts de la liste sur l'appareil

1. Sélectionnez la liste nécessaire.
2. Appuyez sur l'icône  en haut à droite.

8.2.2. Filtre d'autorisation

Le filtre d'autorisation autorise les appels et les SMS uniquement de certains contacts ajoutés.



Comment utiliser le filtre d'autorisation

- Activer l'option **Contacts** pour n'accepter que les appels et les SMS provenant des numéros inclus dans la liste de vos contacts.
- Créer ses propres listes.

Pour créer une liste

1. Ouvrez le filtre d'autorisation.
2. Appuyez sur l'icône .
3. Indiquez le nom de la liste.
4. Ajoutez les contacts. Vous ne pourrez pas enregistrer une liste vide.

Pour ajoutez les contacts dans la liste

1. Sur l'écran de la liste nécessaire, appuyez sur l'icône . Sélectionnez une des options suivantes :
 -  **Contacts** : ajouter un contact depuis vos contacts sur l'appareil.
 -  **Journal des appels** : ajouter un contact depuis la liste des appels récents. Disponible seulement dans la version téléchargée du site.
 -  **Journal des SMS** : ajouter un contact depuis les SMS récents. Disponible seulement dans la version téléchargée du site.
 -  **Nouveau contact** : créer un nouveau contact ou un [masque](#).
 -  **Importation des contacts** : importer la liste des contacts enregistrée précédemment.
2. Si nécessaire, éditez le nom et le numéro de téléphone de chaque contact. Il est impossible d'éditer le numéro ajouté depuis vos contacts.

Pour enregistrer les contacts de la liste sur l'appareil

1. Sélectionnez la liste nécessaire.
2. Appuyez sur l'icône  en haut à droite.

8.2.3. Masques

Les masques permettent d'ajouter des numéros similaires dans les listes du filtre de [blocage](#) et du filtre [d'autorisation](#) :

- Numéros de téléphone commençant par une séquence particulière de chiffres (ou d'autres caractères).
- Numéros de téléphone terminant par une séquence particulière de chiffres (ou d'autres caractères).



- Numéros de téléphone contenant une séquence particulière de chiffres (ou d'autres caractères).

Pour ajouter un masque

1. Sur l'écran de la liste nécessaire, appuyez sur l'icône  et sélectionnez  **Nouveau contact**.
2. Si nécessaire, modifiez le nom.
3. Lors de la saisie du numéro de téléphone, utilisez l'astérisque * au début, à la fin ou des deux côtés.

L'astérisque remplace toute séquence de caractères. N'utilisez pas l'astérisque au milieu du numéro de téléphone ou deux astérisques consécutifs : un tel masque ne marchera pas.

4. Si vous ajoutez un masque à la liste du filtre de blocage, sélectionnez ce que vous voulez bloquer : **Appels** ou **SMS**.

Exemples de masques

Exemple	Commentaire
+7*	Numéros commençant par +7
0	Tous les numéros de téléphone contenant 0 au début, au milieu ou à la fin du numéro
*0	Numéros terminant par 0
* +7*0 *0*0 **0 +7**	Exemples de masques incorrects

8.2.4. Édition des listes

Pour éditer une liste

1. Appuyez sur la liste à éditer.
2. Apportez les modifications.
3. Appuyez sur **Enregistrer**.

Pour supprimer une liste

- Faites défiler le nom de la liste à gauche.

Si vous avez supprimé la mauvaise liste par erreur, appuyez sur **Annuler**. Vous ne pouvez pas supprimer les listes standards.



Pour supprimer plusieurs listes

1. Appuyez et maintenez une liste.
2. Après un signal de vibration, sélectionnez les autres listes à supprimer.
3. Appuyez sur l'icône  en haut à droite.

Pour supprimer un contact de la liste

- Faites-le défiler à gauche.

Pour supprimer plusieurs contacts de la liste

1. Appuyez et maintenez un contact.
2. Après un signal de vibration, sélectionnez les autres contacts à supprimer.
3. Appuyez sur l'icône  en haut à droite.

Pour annuler une suppression accidentelle d'un contact, appuyez sur **Annuler**.



Quand vous supprimez un contact de la liste, il n'est pas supprimé de vos contacts sur l'appareil.

8.2.5. Appels et SMS bloqués

Pour ouvrir la liste des appels et des SMS bloqués

1. Sélectionnez **Filtre des appels et des SMS** sur l'écran d'accueil de Dr.Web.
2. Appuyez sur **Menu**  et sélectionnez **Appels bloqués** ou **SMS bloqués**.

S'il y a des appels ou des SMS bloqués, vous en serez informé par un message apparu dans la [barre d'état](#). Appuyez sur **En savoir plus** dans la barre d'état pour voir les informations sur un appel ou un message bloqué.

Les informations suivantes sont disponibles pour chaque appel ou SMS bloqué :

- La date et l'heure de l'appel ou du message.
- Le numéro de téléphone et le nom du contact.
- Texte du message SMS.

Actions appliquées aux appels et aux SMS bloqués

Pour appeler

1. Appuyez sur le numéro dans la liste des appels ou des messages bloqués.



2. Appuyez sur **Appeler**.

Pour envoyer un message SMS

1. Appuyez sur le numéro dans la liste des appels ou des messages bloqués.
2. Appuyez sur **Envoyer un SMS**.

Pour supprimer un appel ou un message SMS

- Faites-le défiler à gauche.

Pour supprimer tous les appels ou les messages SMS

1. Appuyez sur **Menu**  en haut à droite de l'écran.
2. Appuyez sur **Effacer la liste**.

8.3. Filtre URL

L'accès aux sites est contrôlé par le filtre URL. Il permet de protéger l'utilisateur contre les sites Internet indésirables. Pour configurer le filtre URL, vous pouvez sélectionner des sites particuliers ou des catégories des sites.

En cas de tentative d'ouverture d'un site de la liste des sites interdits, vous verrez la page de blocage.



Le Filtre URL prend en charge le navigateur intégré Android et les navigateurs Google Chrome, Yandex.Browser, Microsoft Edge, Firefox, Firefox Focus, Opera, Adblock Browser, Dolphin Browser, Sputnik, Boat Browser et Atom.

Activation du filtre URL

Sur l'[écran d'accueil de Dr.Web](#), sélectionnez l'option **Filtre URL** (voir [Figure 17](#)).

Le Filtre URL peut demander l'accès aux fonctionnalités spéciales de Android. L'accès est requis pour un fonctionnement correct du Filtre URL dans des navigateurs installés. Sans accès, le Filtre URL ne pourra pas fonctionner.

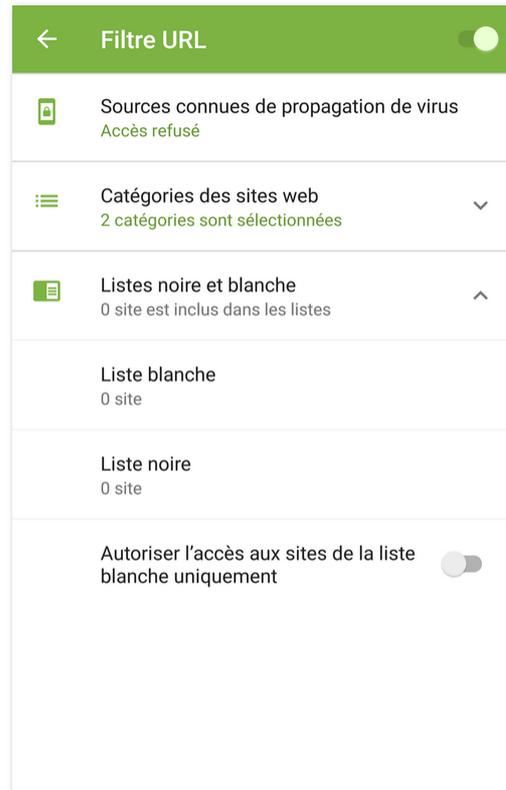


Figure 17. Filtre URL

Catégories des sites web

Dr.Web permet de sélectionner des catégories particulières des sites Web auxquels l'accès doit être interdit. Ouvrez la liste **Catégories des sites web** et sélectionnez les catégories nécessaires :

- Sites non recommandés ;
- Sites pour adultes ;

Quand vous sélectionnez cette catégorie, vous activez le *filtre adulte* dans les moteurs de recherche Google, Yandex, Bing, Yahoo et Rambler. Cela veut dire que le contenu pour adulte sera complètement exclu des résultats de recherche.

- Violence ;
- Armes ;
- Jeux d'argent ;
- Drogues ;
- Langage obscène ;
- Jeux en ligne ;
- Terrorisme ;
- E-mail ;



- Réseaux sociaux ;
- Tchats ;
- URL ajoutées sur demande du détenteur des droits ;
- Anonymiseurs ;
- Pools de minage de cryptomonnaies.



Par défaut, le filtre URL bloque l'accès aux sites connus comme sources de propagation des virus.

Listes noire et blanche

Vous pouvez créer des listes des sites auxquels vous voulez autoriser ou bloquer l'accès indépendamment des autres paramètres du filtre URL. Les listes sont vides par défaut.

Pour ajouter un site à la liste blanche ou noire

1. Dans la fenêtre du filtre URL, ouvrez la section **Listes noire et blanche**.
2. Sélectionnez la liste dans laquelle vous voulez ajouter l'adresse.
3. Appuyez sur l'icône  en bas à droite de la fenêtre.
4. Spécifiez l'adresse du site dans un des formats suivants :
 - example.com
 - http://example.com
 - https://www.example.com
 - www.example.com



Vous pouvez ajouter uniquement les adresses de sites particuliers. L'ajout des masques ou des mots-clés n'est pas pris en charge.

5. Appuyez sur **Ajouter l'URL**.

Si vous tentez d'ajouter une adresse qui existe déjà dans l'autre liste, on vous proposera de la déplacer.

Autoriser l'accès aux sites de la liste blanche uniquement

Activez cette option pour voir uniquement les sites inclus dans la **Liste blanche**. L'accès à d'autres sites sera interdit.



En [mode de protection centralisée](#), certains paramètres du filtre URL peuvent être modifiés ou bloqués conformément à la politique de sécurité de votre entreprise ou à la liste des services payés.



8.4. Antivol Dr.Web

L'Antivol Dr.Web permet de gérer l'appareil en cas de perte ou de vol. Par exemple, vous pouvez supprimer les données à distance, localiser l'appareil ou le bloquer. Pour débloquer l'appareil, il faut entrer le mot de passe :

- du [compte Dr.Web](#) s'il est configuré
- de l'Antivol si le compte n'est pas configuré.

Comment gérer l'appareil avec l'Antivol

- [Configurez l'Antivol](#) d'avance. Par exemple, activez le blocage de l'appareil en cas de changement de la carte SIM.
- Envoyer une [commande](#) à l'Antivol, par exemple, pour localiser l'appareil.

8.4.1. Activation de l'Antivol Dr.Web

1. Sélectionnez **Antivol** sur l'écran d'accueil de Dr.Web.
2. Sur l'écran **Antivol**, appuyez sur **Activer**.
3. Si vous lancez l'Antivol pour la première fois, autorisez l'application à accéder aux fonctions spéciales d'Android et aux données de votre appareil.



Si vous utilisez la version de l'application téléchargée depuis le [site de Doctor Web](#) sur un téléphone Xiaomi avec l'application **Sécurité** installée, autorisez Dr.Web à gérer les SMS dans cette application.

L'Antivol fonctionne uniquement si toutes les autorisations sont accordées.

4. Si le compte Dr.Web n'est pas créé sur votre appareil, [créez-le](#).
Si le compte est déjà créé, entrez le mot de passe du compte. Après dix tentatives échouées d'entrer le mot de passe, le champ de saisie sera temporairement bloqué. Vous verrez le temps restant jusqu'à la prochaine tentative.
5. Si Dr.Web n'est pas l'administrateur de l'appareil, lancez l'application en tant qu'administrateur :
 - Pour prévenir une suppression accidentelle de l'application.
 - Pour autoriser l'Antivol Dr.Web à réinitialiser les paramètres de l'appareil par défaut. Cela protégera vos données en cas de perte ou de vol.
6. Pour [ajouter des amis](#), appuyez sur l'icône . Les [amis](#) vous aideront à gérer à distance votre appareil en cas de perte ou de vol ou si vous oubliez le mot de passe du compte Dr.Web. Appuyez sur **Suivant**.
7. Éditez le texte qui sera affiché sur l'écran de l'appareil mobile en cas de blocage. Ici vous pouvez indiquer vos coordonnées pour qu'on puisse vous contacter et rendre l'appareil perdu. Appuyez sur **Suivant**.



8. Éditez le texte de la notification que vous pouvez envoyer aux amis si l'Antivol bloque votre appareil et que vous oubliez le mot de passe. Appuyez sur **Suivant**.
9. Activez tous les paramètres nécessaires et appuyez sur **Terminer**.

8.4.2. Configuration de l'Antivol Dr.Web



En [mode de protection centralisée](#), certains paramètres de l'Antivol Dr.Web peuvent être modifiés ou bloqués conformément à la politique de sécurité de votre entreprise ou à la liste des services payés.

Pour ouvrir l'Antivol

1. Sélectionnez **Antivol** sur l'écran d'accueil de Dr.Web.
2. Si l'icône  se trouve à côté du champ de saisie de mot de passe, appuyez sur l'icône et touchez le scanner d'empreintes digitales.

Si l'authentification par empreinte digitale n'est pas disponible, entrez le mot de passe du compte Dr.Web. Après dix tentatives échouées d'entrer le mot de passe, le champ de saisie sera temporairement bloqué. Vous verrez le temps restant jusqu'à la prochaine tentative.



Si vous migrez vers la version 12, votre mot de passe de l'Antivol Dr.Web devient automatiquement le mot de passe du compte Dr.Web.

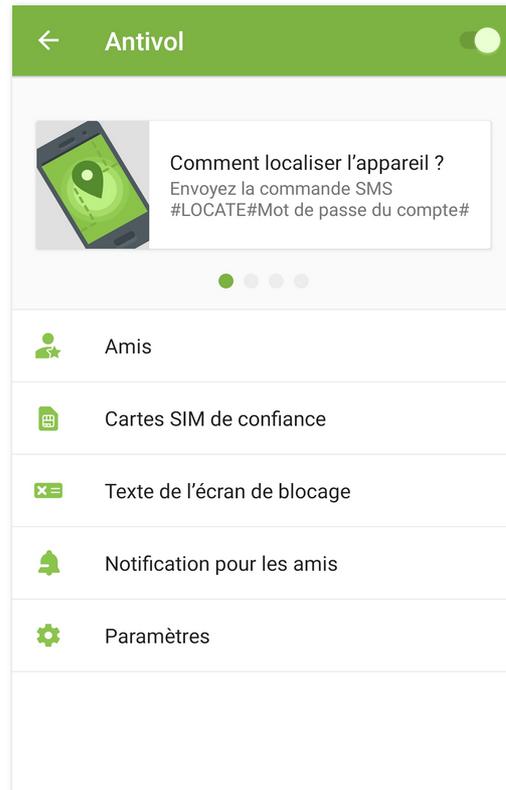


Figure 18. Antivol Dr.Web

Fiches avec les commandes SMS



Disponible uniquement dans la version de l'application téléchargée depuis le [site de Doctor Web](#).

Les fiches avec les [commandes SMS](#) se trouvent en haut de l'écran **Antivol** (voir [Figure 18](#)).

- Pour voir toutes les commandes SMS, faites défiler les fiches à droite.
- Pour ouvrir une description détaillée d'une commande SMS ou [envoyer une commande SMS](#), appuyez sur la fiche portant cette commande.

Amis

Amis : ce sont les contacts auxquels vous autorisez la gestion de votre appareil via les [commandes](#) ou les contacts qui vous font confiance. Dans l'application, les amis sont divisés en deux onglets : [Je leur fais confiance](#) et [Ils me font confiance](#).



Je leur fais confiance

Cet onglet contient la liste des amis à qui vous autorisez la gestion de votre appareil via les commandes. Vous avez ajouté ces contacts à la liste d'amis ayant indiqué leurs numéros de téléphone et leurs adresses e-mail.

Icône	Version de l'application	Commentaire
	Seule la version du site de Doctor Web	Vous avez ajouté un numéro de téléphone. Votre ami peut envoyer des commandes SMS sans mot de passe sur votre appareil.
	Toute	Vous avez ajouté une adresse e-mail. Votre ami n'a pas encore accepté votre demande d'ami et ne peut pas envoyer des commandes push à l'Antivol. Pour confirmer la demande, l'ami ajouté doit avoir l'application Dr.Web Security Space ou la version gratuite de Dr.Web Light installée sur son appareil. Il se peut que votre demande ait été ignorée. S'il est nécessaire, envoyez a demande encore une fois.
	Toute	Vous avez ajouté une adresse e-mail. L'ami a accepté votre demande d'ami et peut envoyer des commandes push à l'Antivol. <ul style="list-style-type: none">• Si l'application Dr.Web Security Space est installée sur l'appareil de votre ami, il peut vous envoyer toutes les commandes.• Si l'application Dr.Web Light est installée sur l'appareil de votre ami. l'ami peut vous aider à débloquer votre appareil s'il a été bloqué par l'Antivol et que vous avez oublié le mot de passe.
	Toute	Vous avez ajouté une adresse e-mail, mais l'ami a rejeté votre demande d'ami. L'ami ne peut pas envoyer des commandes push à l'Antivol. Dans ce cas, vous pouvez supprimer le contact de la liste d'amis.

Pour ajouter un ami

- Dans l'onglet **Je leur fais confiance**, appuyez sur l'icône .
- **Pour la version de l'application téléchargée du site Doctor Web.** Ajoutez un numéro de téléphone. Depuis ce numéro, on pourra envoyer des commandes SMS sans mot de passe sur votre appareil. Pour ce faire, choisissez l'une des options suivantes :
 -  **Contacts** : sélectionner un numéro de téléphone dans vos contacts sur l'appareil.
 -  **Journal des appels** : sélectionner un numéro de téléphone dans la liste des appels récents.
 -  **Journal des SMS** : sélectionner un numéro de téléphone dans la liste des SMS récents.
 -  **Nouveau contact** : entrer un nouveau numéro de téléphone.
- **Pour toutes les versions de l'application** Ajoutez l'adresse e-mail. Un message sera envoyé à l'adresse indiquée. La demande peut être acceptée dans l'application Dr.Web



Security Space ou dans la version gratuite Dr.Web Light. Une fois la demande acceptée, votre ami pourra envoyer des commandes à l'Antivol à l'aide des notifications. Depuis Dr.Web Light, on peut envoyer la commande de déblocage de l'appareil et de réinitialisation du mot de passe si votre appareil est bloqué. Depuis Dr.Web Security Space, on peut envoyer toutes les commandes.

Vous pouvez ajouter cinq adresses e-mail au maximum (ou cinq numéros de téléphone dans la version de l'application téléchargée depuis le site de Doctor Web).

Pour modifier un contact d'ami

1. Sélectionnez le contact nécessaire dans l'onglet **Je leur fais confiance**.
2. Appuyez sur l'icône .
3. Apportez les modifications.
4. Appuyez sur l'icône  pour enregistrer les modifications.



Vous ne pouvez pas modifier l'entrée si ce contact a rejeté votre demande d'amis.

Pour supprimer un ami

- Faites défiler le contact correspondant à gauche.

Si vous supprimez par erreur un contact important de la liste d'amis, vous pouvez annuler la suppression en appuyant sur **Annuler**.

Ils me font confiance

L'onglet **Ils me font confiance** contient la liste des amis qui vous confient la gestion de leurs appareils. Ils vous ont ajouté à la liste d'amis dans l'Antivol Dr.Web, en indiquant votre e-mail. Pour pouvoir gérer l'appareil de l'ami à distance, il faut accepter la demande d'ami.

Statuts de demandes d'ami

Icône	Commentaire
	Vous n'avez pas encore accepté la demande d'ami. Pour pouvoir envoyer des commandes push sur l'appareil de l'ami, acceptez la demande d'ami.
	Vous avez accepté la demande d'ami et vous pouvez gérer l'appareil de l'ami à distance avec les commandes push .
	Vous êtes supprimé de la liste d'amis. Votre ami doit vous envoyer une nouvelle demande pour que vous puissiez envoyer des commandes push .



Pour accepter une demande d'ami

Effectuez l'une des actions suivantes :

- Appuyez sur la notification portant la demande que vous avez reçue après être ajouté à la liste d'amis et appuyez sur **Confirmer**.
- Sélectionnez le contact nécessaire dans l'onglet **Ils me font confiance** et appuyez sur **Confirmer**.

Pour rejeter une demande d'ami

Effectuez l'une des actions suivantes :

- Appuyez sur la notification portant la demande que vous avez reçue après être ajouté à la liste d'amis et appuyez sur **Rejeter**.
- Sélectionnez le contact nécessaire dans l'onglet **Ils me font confiance** et appuyez sur **Rejeter**.
- Supprimez le contact de la liste d'amis.

Pour modifier un contact d'ami

1. Sélectionnez le contact nécessaire dans l'onglet **Ils me font confiance**.
2. Appuyez sur l'icône .
3. Modifiez l'entrée.
4. Appuyez sur l'icône  pour enregistrer les modifications.



Vous ne pouvez pas modifier l'entrée si ce contact vous a supprimé de la liste d'amis.

Pour supprimer un ami

- Faites défiler le contact correspondant à gauche.
Si vous supprimez par erreur un contact d'ami ou une demande d'ami que vous n'avez pas encore confirmée, vous pouvez annuler la suppression en appuyant sur **Annuler**.

Pour débloquent l'appareil de l'ami

1. Appuyez sur la notification reçue de votre ami.
2. Contactez votre ami pour obtenir le code de confirmation. Méfiez-vous des messages reçus contenant le code de confirmation. Ils peuvent être envoyés par des malfaiteurs.
3. Entrez le code de confirmation.
4. Appuyez sur **Débloquer**.



Cartes SIM de confiance

Les cartes SIM de confiance est une liste des cartes SIM que vous utilisez sur votre appareil. Par défaut, l'Antivol bloque l'appareil s'il ne détecte pas de carte SIM de la liste de confiance. Même si votre appareil est volé et que la carte SIM est remplacée, il sera impossible de l'utiliser. En cas de remplacement d'une carte SIM de confiance par une autre carte SIM de cette liste, l'Antivol ne bloque pas l'appareil.

Si vous utilisez deux cartes SIM sur un appareil tournant sous Android 5.1 ou une version supérieure, les deux cartes SIM seront automatiquement ajoutées à la liste de confiance. Si votre appareil tourne sous Android 5.0 ou une version antérieure, vous ne pouvez ajouter à la liste de confiance qu'une seule carte SIM (il est impossible d'ajouter deux cartes SIM en même temps).

Chaque carte SIM dans la liste porte le nom et l'identificateur (sur les appareils tournant sous Android 5.0 ou une version antérieure) ou l'indication de l'opérateur mobile (sur les appareils tournant sous Android 5.1 ou une version supérieure).

Les nouvelles cartes SIM de confiance sont ajoutées lors du redémarrage de l'appareil ou quand vous lancez Dr.Web.

Appuyez sur **Cartes SIM de confiance** pour ouvrir ou modifier la liste :

- Pour voir les informations détaillées sur une carte SIM, appuyez sur cette carte dans la liste. En fonction de la version de l'OS, les champs suivant peuvent être disponibles : nom, opérateur mobile, identificateur.
- Pour renommer une carte SIM, appuyez sur cette carte dans la liste. Sur l'écran qui s'affiche, indiquez un nouveau nom dans le champ **Nom** et appuyez sur **Enregistrer**.
- Pour supprimer la carte SIM de la liste de confiance, faites-la défiler à gauche.



La carte SIM utilisée en ce moment ne peut pas être supprimée de la liste de confiance.

Texte de l'écran de blocage

Ici vous pouvez modifier le texte à afficher sur l'écran de l'appareil bloqué en cas de perte ou de vol. Par exemple, vous pouvez spécifier votre deuxième numéro de téléphone ou l'adresse e-mail pour vous contacter.

Pour modifier le texte sur l'écran de blocage

- Appuyez sur **Texte de l'écran de blocage**, entrez le nouveau texte et appuyez sur **Enregistrer**.



Notification pour les amis

Notification pour les amis : c'est une notification que vous pouvez envoyer aux amis si l'Antivol bloque votre appareil et que vous oubliez le mot de passe. Après avoir reçu la notification, les amis doivent vous demander le code de confirmation pour réinitialiser votre mot de passe. Ensuite vous pouvez spécifier un nouveau mot de passe.

Pour changer le texte de notification

- Appuyez sur **Notification pour les amis**, entrez le nouveau texte et appuyez sur **Enregistrer**.

Paramètres

Verrouiller lors du redémarrage

Cette option est désactivée par défaut.

Si cette option est activée, l'Antivol Dr.Web bloquera l'appareil après chaque redémarrage. Pour débloquer l'appareil, il faut entrer le mot de passe du compte Dr.Web. Il est impossible de débloquer l'appareil sans mot de passe.

Verrouiller lors du remplacement de la carte SIM

Cette option est activée par défaut.

Si l'Antivol Dr.Web détecte sur l'appareil une carte SIM non incluse dans la liste de confiance, il bloquera l'appareil. Pour débloquer l'appareil, il faut entrer le mot de passe du compte Dr.Web. Il est impossible de débloquer l'appareil sans mot de passe.

Envoyer un SMS pour informer les amis du changement de la carte SIM



Disponible uniquement dans la version de l'application téléchargée depuis le [site](#) de Doctor Web.

Cette option est désactivée par défaut.

Si cette option est activée, l'Antivol Dr.Web enverra les messages SMS à tous les contacts de la liste d'amis dès qu'il aura détecté sur l'appareil une carte SIM non incluse dans la liste de confiance. De plus, l'Antivol Dr.Web déterminera le numéro de téléphone lié à cette carte SIM.

Au redémarrage de l'appareil avec la carte SIM remplacée, l'Antivol enverra de nouveau les messages SMS aux contacts de la liste d'amis. L'Antivol peut envoyer de tels messages SMS cinq fois par jour au maximum.



Supprimer les données

Cette option est désactivée par défaut.

Si votre appareil est volé et bloqué, un étranger peut essayer de le débloquer par force brute. Pour que personne ne puisse accéder à vos données, activez l'option **Supprimer les données**.

Après 10 tentatives de saisie de mot de passe sur l'appareil bloqué :

- Si Dr.Web est activé en tant qu'administrateur de l'appareil, les paramètres de l'appareil seront réinitialisés par défaut (toutes les applications installées, vos données personnelles, les photos, les messages SMS, les contacts seront supprimés ainsi que toutes les informations de la carte mémoire). Notez que la réinitialisation des paramètres par défaut supprimera Dr.Web.
- Si Dr.Web n'est pas activé en tant qu'administrateur de l'appareil, vos données personnelles seront supprimées (sauf les SMS car Dr.Web n'est pas une application d'envoi et de réception de SMS par défaut). Dr.Web ne sera pas supprimé et continuera de bloquer l'appareil.

Mode de fonctionnement sans carte SIM

Le mode de fonctionnement sans carte SIM est activé non seulement en cas d'absence de la carte SIM mais aussi lorsque votre appareil interdit l'accès aux informations sur la carte SIM aux applications installées. Cela concerne les appareils pour lesquels l'utilisation des cartes SIM est prévue.

Dès que l'Antivol Dr.Web aura révélé l'absence de l'accès à la carte SIM, un écran s'affichera vous invitant à entrer le mot de passe du compte Dr.Web. Un message s'affichera dans le panneau de notifications, vous indiquant que la carte SIM n'est pas détectée. Entrez le mot de passe pour approuver le mode sans carte SIM. L'envoi des commandes SMS sera indisponible, mais vous pourrez utiliser les autres fonctions de l'Antivol Dr.Web.

8.4.3. Commandes de l'Antivol Dr.Web

Utilisez les commandes de l'Antivol Dr.Web pour gérer votre appareil à distance.

- Les [commandes push](#) sont envoyées via les notifications push et ne sont pas affichées sur l'appareil du destinataire.
- Les [commandes SMS](#) sont envoyées via les messages SMS et elles sont affichées sur l'appareil du destinataire.



Configuration requise pour l'envoi des commandes de l'Antivol

Appareil	Commandes push	Commandes SMS
Expéditeur	Appareil avec toute version de l'application. L'antivol est activé, la demande d'ami du destinataire est confirmée.	L'installation de l'application Dr.Web n'est pas requise. <ul style="list-style-type: none">• Tout appareil, si le mot de passe est indiqué dans la commande SMS.• Appareil avec le numéro de téléphone ajouté dans la liste d'amis du destinataire si le mot de passe n'est pas indiqué dans la commande SMS.
Destinataire	Appareil avec toute version de l'application. L'antivol est activé.	Appareil avec la version de l'application téléchargée depuis le site ou depuis HUAWEI AppGallery. L'antivol est activé.



Le paramètre système **Afficher sur l'Écran de verrouillage** présent sur certains appareils peut empêcher la saisie du mot de passe du compte Dr.Web sur un appareil bloqué par une commande. Par défaut, ce paramètre est désactivé. Si vous l'avez activé, ouvrez **Applis > Dr.Web > Autres autorisations** et désactivez le paramètre **Afficher sur l'Écran de verrouillage**.

8.4.3.1. Commandes push

Qu'est-ce que les commandes push ?

Les commandes push sont des commandes de gestion de l'Antivol Dr.Web qui sont envoyées via les notifications push Android. Les notifications push contenant des commandes push ne sont pas affichées sur l'appareil du destinataire et ne sont pas traitées par l'application.



Le fonctionnement correct des notifications push n'est pas garanti dans la version téléchargée depuis HUAWEI AppGallery, installée sur un appareil autre que Huawei car les services mobiles non mis à niveau peuvent être utilisés.

Qu'est-ce qu'il faut pour utiliser les commandes push

1. Pour envoyer et recevoir des commandes push, il faut que les appareils soient connectés à Internet.
2. L'application Dr.Web Security Space doit être installée sur l'appareil du destinataire. Dr.Web Security Space ou Dr.Web Light doit être installé sur l'appareil de l'expéditeur.
3. L'Antivol doit être activé sur l'appareil du destinataire.
4. La commande push peut être envoyée uniquement depuis l'appareil sur lequel la demande d'amis du destinataire a été confirmée.



- L'ami peut envoyer toutes les commandes push depuis l'application Dr.Web Security Space.
- L'ami peut débloquer l'appareil du destinataire depuis l'application Dr.Web Light en utilisant le composant Aide à l'ami.

Pour envoyer une commande push

1. Sur l'écran **Antivol**, appuyez sur **Amis**.
2. Sélectionnez l'onglet **Ils me font confiance**.
3. Sélectionnez l'ami sur l'appareil de qui il faut envoyer la commande.
4. Sélectionnez la commande.



La transmission de commandes push peut prendre jusqu'à 15 minutes.

Commandes



Le paramètre système **Afficher sur l'Écran de verrouillage** présent sur certains appareils peut empêcher de débloquer l'appareil bloqué par une commande. Assurez-vous d'avance que le paramètre est [désactivé](#).

Commande	Action
Localiser	<p>Obtenir les coordonnées de l'appareil mobile.</p> <p>En réponse à votre commande, vous allez recevoir un lien avec les coordonnées de l'appareil sur la carte.</p> <p>La localisation de l'appareil est utilisée par un service spécialisée de Doctor Web Dr.Web Anti-theft Locator affichant dans la fenêtre du navigateur la carte et les coordonnées de l'appareil. L'exactitude de localisation dépend de la disponibilité du récepteur GPS, de la visibilité des réseaux Wi-Fi et des stations GSM. De ce fait, selon les données reçues, les coordonnées seront exactes (sous forme d'une position sur la carte) ou approximatives (sous forme d'un cercle d'un certain rayon).</p> <p>En-haut de l'écran avec la carte, vous pouvez sélectionner le service de cartographie approprié.</p>
Bloquer l'appareil	Bloquer l'appareil. Pour débloquer l'appareil, il faut entrer le mot de passe du compte Dr.Web.
Bloquer l'appareil et activer une signal sonore	Bloquer l'appareil et activer l'alarme sonore qui continuera à sonner même après le redémarrage de l'appareil. Pour débloquer l'appareil, il faut entrer le mot de passe du compte Dr.Web.



Commande	Action
Supprimer les données	Supprimer toutes les données de l'appareil. Si Dr.Web est activé en tant qu'administrateur sur l'appareil de l'ami, cette commande réinitialisera les paramètres par défaut de l'appareil. Cette commande s'applique aussi en cas de blocage de l'appareil, si l'option Supprimer les données est activée dans les paramètres de l'Antivol Dr.Web.
Réinitialiser le mot de passe	Débloquer l'appareil et réinitialiser le mot de passe du compte Dr.Web. Pour l'envoi de la commande, le code de confirmation est requis. Le code s'affiche sur l' appareil de l'ami .

8.4.3.2. Commandes SMS



Vous pouvez envoyer les commandes SMS uniquement sur les appareils sur lesquels est installée la version de l'application téléchargée depuis le [site Doctor Web](#).

Pour que les commandes SMS fonctionne sur un téléphone Xiaomi avec l'application **Sécurité** installée, autorisez Dr.Web à gérer les SMS dans cette application.

Les commandes SMS sont des commandes de gestion distante de l'Antivol Dr.Web envoyées via les messages SMS. Les commandes SMS permettent de localiser votre appareil mobile, ainsi que de verrouiller ses fonctions ou de supprimer les données personnelles.

Vous pouvez envoyer une commande SMS de la façon suivante :

- Avec l'indication du mot de passe — depuis tout appareil.
- Sans indication du mot de passe — de l'appareil de l'[ami](#).

Il n'est pas recommandé d'envoyer des commandes SMS avec le mot de passe sur l'appareil perdu ou volé : les criminels peuvent voir le SMS avec le mot de passe et débloquer l'appareil. Pour pouvoir envoyer une commande SMS sans mot de passe, [ajoutez d'avance les numéros de téléphone](#) dans la liste d'amis.

Commandes SMS



Le paramètre système **Afficher sur l'Écran de verrouillage** présent sur certains appareils peut empêcher de débloquer l'appareil bloqué par une commande. Assurez-vous d'avance que le paramètre est [désactivé](#).

Commande	Action
#LOCK#Mot de passe#	Verrouiller l'appareil mobile. En réponse à votre commande, vous allez recevoir le message SMS suivant : « Antivol Dr.Web – L'appareil <nom de l'appareil> est bloqué ».



Commande	Action
#SIGNAL#Mot de passe#	<p>Bloquer l'appareil et activer l'alarme sonore qui continuera à sonner même après le redémarrage de l'appareil.</p> <p>En réponse à votre commande, vous allez recevoir le message SMS suivant : « Antivol Dr.Web – L'appareil <nom de l'appareil> est bloqué ».</p>
#LOCATE#Mot de passe#	<p>Obtenir les coordonnées de l'appareil mobile par SMS.</p> <p>En réponse à votre commande, vous allez recevoir un lien avec les coordonnées de l'appareil sur la carte.</p> <p>La localisation de l'appareil est utilisée par un service spécialisée de Doctor Web Dr.Web Anti-theft Locator affichant dans la fenêtre du navigateur la carte et les coordonnées de l'appareil. L'exactitude de localisation dépend de la disponibilité du récepteur GPS, de la visibilité des réseaux Wi-Fi et des stations GSM. De ce fait, selon les données reçues, les coordonnées seront exactes (sous forme d'une position sur la carte) ou approximatives (sous forme d'un cercle d'un certain rayon).</p> <p>En-haut de l'écran avec la carte, vous pouvez sélectionner le service de cartographie approprié.</p>
#UNLOCK#Mot de passe#	Débloquer l'appareil sans réinitialiser le mot de passe du compte Dr.Web.
#WIPE#Mot de passe#	<p>Rétablir les paramètres initiaux de l'appareil mobile et supprimer toutes les données depuis la mémoire de l'appareil.</p> <p>En réponse à votre commande, vous allez recevoir le message SMS suivant : « Antivol Dr.Web - Suppression des données sur l'appareil <nom de l'appareil> ».</p> <p>Cette commande s'applique aussi en cas de blocage de l'appareil, si l'option Supprimer les données est activée dans les paramètres de l'Antivol Dr.Web.</p>
#RESETPASSWORD#	Débloquer l'appareil et créer un nouveau mot de passe. Cette commande peut être exécutée uniquement si elle est envoyée depuis un numéro inclus dans la liste d'amis.



Les commandes SMS sont insensibles à la casse. Par exemple, pour bloquer l'appareil, vous pouvez envoyer la commande **#LOCK#Mot de passe#** écrite comme **#Lock#Mot de passe#**, **#lock#Mot de passe#**, **#lOck#Mot de passe#**, etc.

Pour obtenir les résultats plus précis après avoir envoyé la commande SMS **#LOCATE#**, activez l'option de localisation via les réseaux sans fil dans les paramètres de l'appareil.



Envoi des commandes SMS via l'Antivol Dr.Web

Depuis l'Antivol Dr.Web, vous pouvez envoyer des commandes SMS aux appareils sur lesquels l'Antivol Dr.Web est aussi activé.

Pour envoyer une commande SMS

1. Sur l'écran **Antivol** (voir [Figure 18](#)), appuyez sur une [fiche portant une commande SMS](#).
2. Appuyez sur **Envoyer une commande SMS**.
3. Sur l'écran **Envoi d'une commande SMS** :
 1. Dans la liste **Commande**, sélectionnez la commande nécessaire :
 - **Verrouiller** : correspond à la commande [#LOCK#](#).
 - **Verrouiller et activer une alarme** : correspond à la commande [#SIGNAL#](#).
 - **Détecter les coordonnées** : correspond à la commande [#LOCATE#](#).
 - **Déverrouiller** : correspond à la commande [#UNLOCK#](#).
 - **Supprimer toutes les données** : correspond à la commande [#WIPE#](#).
 - **Déverrouiller et spécifier un nouveau mot de passe** : correspond à la commande [#RESETPASSWORD#](#).
 2. Dans le champ **A qui**, indiquez le numéro de téléphone du destinataire.
 3. Dans le champ **Mot de passe de destinataire**, indiquez le mot de passe du compte du destinataire.

Si votre numéro figure dans la [liste d'amis](#) du destinataire, vous pouvez laisser le champ vide.
 4. Dans la liste **De qui**, sélectionnez la carte SIM depuis laquelle la commande sera envoyée.

Cette option est disponible sur les appareils à deux cartes SIM tournant sous Android 5.1 ou une version supérieure.
 5. Appuyez sur **Envoyer**.

8.4.4. Désactivation de l'Antivol Dr.Web

Pour désactiver l'Antivol Dr.Web

1. Sélectionnez l'**Antivol** sur l'écran d'accueil de Dr.Web.
2. Entrez le mot de passe du compte Dr.Web ou de l'Antivol.
3. Désactivez l'Antivol sur l'écran **Antivol** (voir [Figure 18](#)) en utilisant l'interrupteur en haut à droite de l'écran.
4. Dans la fenêtre qui s'affiche, appuyez sur **OK**.



La désactivation de l'Antivol Dr.Web peut affaiblir considérablement la protection de votre appareil mobile.

8.5. Contrôle parental

Avec le Contrôle parental, l'utilisateur du compte Dr.Web peut bloquer l'accès à toute application installée, à un groupe d'applications et aux paramètres des composants de Dr.Web.

Comment fonctionne le Contrôle parental ?

Si vous voulez bloquer l'accès aux applications et aux paramètres des composants de Dr.Web pour un utilisateur de l'appareil, assurez-vous que l'application Dr.Web est installée sur cet appareil. Vous activez le composant Contrôle parental sur l'appareil de l'utilisateur et indiquez les paramètres de votre compte Dr.Web. Après l'activation du composant, vous spécifiez les limites d'accès de l'utilisateur de l'appareil aux applications, aux groupes d'applications et aux paramètres des composants de Dr.Web. En cas de tentative de lancement d'une application bloquée ou d'ouverture des paramètres d'un composant, l'utilisateur de l'appareil voit l'[écran de blocage](#) ou l'écran de saisie de mot de passe. L'accès à l'application ou au composant bloqué est possible uniquement après la saisie du mot de passe de votre compte Dr.Web ou l'authentification par votre empreinte digitale.

Fonctions principales du Contrôle parental

Le Contrôle parental permet de :

- bloquer l'accès à une application ou à un groupe d'applications ;
- bloquer l'accès aux paramètres des composants de Dr.Web ;
- limiter l'accès à une application ou à un groupe d'applications pendant un intervalle de temps spécifié ;
- créer des groupes utilisateur d'applications bloquées ;
- suivre les événements liés aux applications et aux composants bloqués.

Activation du Contrôle parental

Pour activer le Contrôle parental

1. Sélectionnez **Contrôle parental** sur l'écran d'accueil de Dr.Web.
2. Si le compte Dr.Web n'est pas créé sur votre appareil, [créez-le](#).

Si le compte est créé, entrez le mot de passe du compte. Après dix tentatives échouées d'entrer le mot de passe, le champ de saisie sera temporairement bloqué. Vous verrez le temps restant jusqu'à la prochaine tentative.



3. Sur l'écran **Contrôle parental**, appuyez sur **Activer**.
4. Si Dr.Web n'est pas l'administrateur de l'appareil, activez l'application en tant qu'administrateur. Cela permettra de prévenir une suppression involontaire de l'application. De plus, en cas de perte ou de vol de l'appareil vous pouvez protéger vos données en réinitialisant les paramètres par défaut avec l'[Antivol Dr.Web](#).

Désactivation du Contrôle parental

Pour désactiver le Contrôle parental

1. Sélectionnez **Contrôle parental** sur l'écran d'accueil de Dr.Web.
2. Entrez le mot de passe du compte Dr.Web.
3. Désactivez le Contrôle parental en utilisant l'interrupteur en haut à droite de l'écran et appuyez sur **OK**.

Mode d'apprentissage

Dans la partie supérieure de l'écran d'accueil du composant Contrôle parental (voir [Figure 19](#)) les mini-diapositives sont disponibles permettant de lancer le mode d'apprentissage. Le mode d'apprentissage aide à apprendre vite les fonctions essentielles du Contrôle parental.

Le mode d'apprentissage comporte quatre sections :

- [Applications](#) : bloquer l'accès aux applications et aux groupes d'applications.
- [Accès par heure](#) : limiter l'accès aux applications et aux groupes d'applications dans le temps.
- [Composants](#) : bloquer l'accès aux paramètres des composants de Dr.Web.
- [Paramètres](#) : paramètres et journal du Contrôle parental.

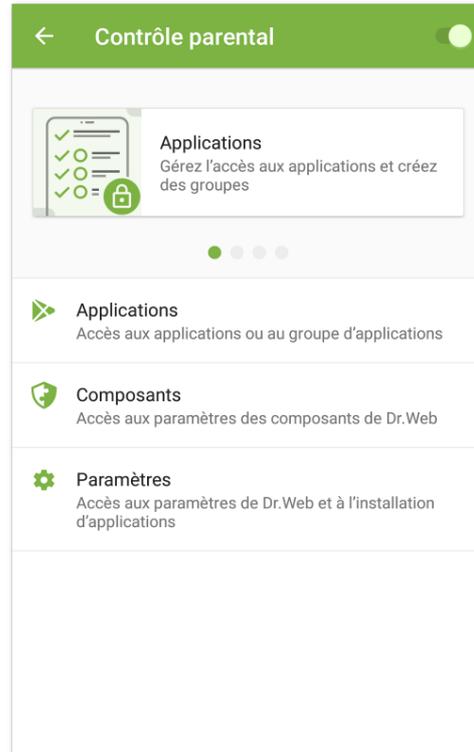


Figure 19. Contrôle parental

Les mini-diapositives permettent d'ouvrir une des sections du mode d'apprentissage. Faites-glisser la mini-diapositive vers la gauche ou la droite pour aller à la mini-diapositive précédente ou suivante. Appuyez sur la mini-diapositive pour ouvrir la section correspondante du mode d'apprentissage.

Les diapositives plein écran sont également disponibles dans le mode d'apprentissage. Elles expliquent comment utiliser les fonctions du Contrôle parental (voir [Figure 20](#)). Faites glisser la diapositive courante vers la gauche pour aller à la diapositive suivante.

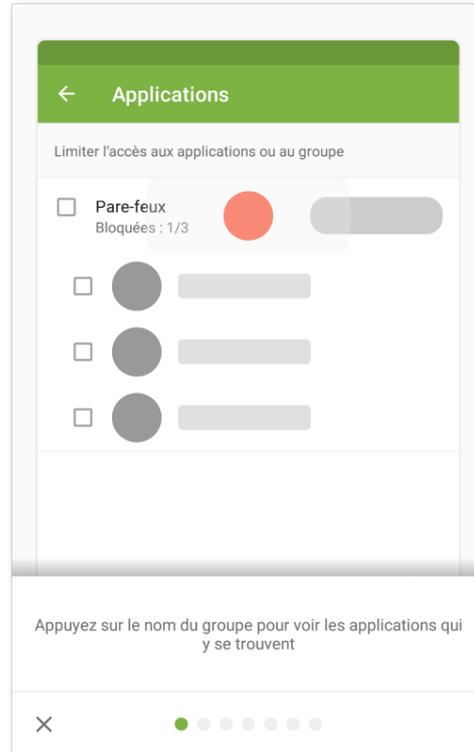


Figure 20. Diapositive du mode d'apprentissage

Pour quitter le mode d'apprentissage, appuyez sur **X** en bas à gauche de l'écran.

8.5.1. Blocage de l'accès aux applications et aux composants

Applications

La section **Applications** contient la liste de toutes les applications installées sur l'appareil.

Bloquer l'accès aux applications et aux groupes d'applications

Le composant Contrôle parental permet de bloquer l'accès à certaines applications ou aux groupes d'applications entiers. Si vous essayez d'ouvrir une application à laquelle l'accès est bloqué ou limité, un [écran de blocage de l'application](#) s'affichera vous empêchant d'accéder à l'application. Vous pouvez obtenir l'accès à l'application avec le mot de passe du compte Dr.Web ou [l'empreinte digitale enregistrée](#).

Pour bloquer l'accès à une application ou à toutes les applications du groupe, cochez la case contre l'application ou le groupe en question. Pour autoriser l'accès de nouveau, décochez la case.



Groupes d'applications

Par défaut, les applications sont divisées en groupes système par catégories. Pour voir les applications dans un groupe, appuyez sur le nom du groupe.



Sur les appareils tournant sous Android 8.0 ou une version antérieure, toutes les applications font partie du groupe système **Autres**.

Vous pouvez également créer des groupes d'applications utilisateur.

Pour créer un groupe utilisateur

1. Appuyez sur l'icône  en bas à droite de l'écran.
2. Dans le menu qui s'affiche, sélectionnez **Nouveau groupe**.
3. Entrez le nom du nouveau groupe.
4. Appuyez sur  contre les applications à ajouter dans le nouveau groupe.
5. Appuyez sur  pour enregistrer le nouveau groupe.

Les groupes utilisateur s'affichent en haut de la liste de groupes d'applications.

Pour modifier un groupe utilisateur

1. Faites défiler le nom du groupe vers la gauche.
2. Appuyez sur l'icône .
3. Apportez les modifications nécessaires.
4. Appuyez sur l'icône  en haut à droite de l'écran.

Pour supprimer un groupe utilisateur

1. Faites défiler le nom du groupe vers la gauche.
2. Appuyez sur l'icône .

Pour supprimer plusieurs groupes utilisateur

1. Appuyez et maintenez le nom d'un groupe à supprimer.
2. Sélectionnez les autres groupes à supprimer.
3. Supprimez les groupes en appuyant sur l'icône  en haut à droite de l'écran.



Il est interdit de modifier ou supprimer les groupes système.



Si l'option **Bloquer les navigateurs sans Filtre URL** ou **Bloquer le lancement de nouvelles applications** est activée dans les [paramètres du Contrôle parental](#), le groupe système **Navigateurs sans Filtre URL** ou **Nouvelles applications** apparaît respectivement dans la liste d'applications. Pour autoriser l'accès aux applications de ces groupes, désactivez les options correspondantes dans les paramètres du Contrôle parental.

Recherche dans la liste d'applications

Pour faciliter la navigation dans la liste d'applications, vous pouvez utiliser la recherche.

Pour rechercher par nom d'une application ou d'un groupe

1. Appuyez sur l'icône  en bas à droite de l'écran.
2. Dans le menu qui s'affiche, sélectionnez **Recherche**.
3. Saisissez un mot clé dans le champ de recherche en bas de l'écran.

Limitation de l'accès dans le temps

Vous pouvez bloquer l'accès aux groupes d'applications en permanence ou pendant des intervalles de temps spécifiés.

Le type de blocage s'affiche à droite du nom de groupe. Deux types de blocage sont possibles :

- **Toujours** : l'accès au groupe est toujours bloqué.
- **Plage horaire** : l'accès au groupe est bloqué pendant une période de temps spécifiée.

Par défaut, quand vous bloquez un groupe d'applications, l'accès est toujours bloqué.

Pour spécifier une période de blocage

1. Cliquez sur le type de blocage à droite du groupe d'applications.
2. Appuyez sur  en bas à droite de l'écran.
3. Sélectionnez les jours de semaine auxquels la limite s'appliquera.
4. Appuyez sur **Début** et spécifiez l'heure de début de la limite.
5. Appuyez sur **OK**, pour confirmer l'heure de début choisie.
6. Appuyez sur **Fin** et spécifiez l'heure de fin de la limite.
7. Appuyez sur **OK**, pour confirmer l'heure de fin choisie.
8. Appuyez sur  en haut à droite de l'écran pour enregistrer la limite.

Vous pouvez spécifier une seule période de temps pour une limite. Pour bloquer un groupe d'applications un autre jour de la semaine ou à une autre heure, créez des limites supplémentaires.



Vous pouvez modifier et supprimer les limites.

Pour modifier une limite

1. Cliquez sur le type de blocage à droite du groupe d'applications.
2. Faites défiler la limite nécessaire vers la gauche.
3. Appuyez sur l'icône .
4. Apportez les modifications nécessaires.
5. Enregistrez les modifications en appuyant sur l'icône  en haut à droite de l'écran.

Pour supprimer une limite

1. Cliquez sur le type de blocage à droite du groupe d'applications.
2. Faites défiler la limite nécessaire vers la gauche.
3. Appuyez sur l'icône .

Composants

Outre l'accès aux applications ou aux groupes d'applications, vous pouvez bloquer l'accès aux paramètres des composants de Dr.Web : Filtre des appels et des SMS, Pare-feu et paramètres de l'application Dr.Web.

Pour bloquer l'accès aux paramètres des composants

1. Sur l'écran d'accueil du Contrôle parental, sélectionnez la section **Composants**.
2. Cochez les cases contre les composants Dr.Web, auxquels vous voulez bloquer l'accès :
 - [Filtre des appels et des SMS](#). Permet à l'utilisateur du compte de créer les listes des numéros depuis lesquels l'utilisateur peut recevoir les appels et les messages. Par exemple, on peut autoriser les appels entrants et les messages SMS provenant seulement des numéros particuliers ou des numéros de la liste des contacts. L'utilisateur de l'appareil ne pourra pas modifier la liste des numéros autorisés ou bloqués.
 - [Filtre URL](#). Permet à l'utilisateur du compte de limiter l'accès de l'utilisateur de l'appareil à des sites spécifiques, des pages web et des catégories des sites (par exemple, « Drogues », « Armes », « Terrorisme », « Sites pour adultes », etc.). L'utilisateur de l'appareil ne pourra pas modifier la liste des sites et des catégories de sites auxquels il a l'accès.
 - [Pare-feu](#). Permet à l'utilisateur du compte de limiter l'utilisation du trafic mobile, de contrôler la transmission de données et de gérer les connexions Internet des applications installées sur l'appareil de l'utilisateur. L'utilisateur ne pourra pas modifier les règles et les limites prédéfinies.
 - [Paramètres de Dr.Web](#). Permet au titulaire du compte d'interdire à l'utilisateur de l'appareil d'accéder aux paramètres de Dr.Web et de les modifier. Par exemple, l'utilisateur ne pourra pas réinitialiser les paramètres par défaut.



Il est impossible de spécifier une limite de temps d'accès pour les composants de Dr.Web. L'accès sera toujours bloqué.

Pour accéder à un composant bloqué, il faudra entrer le mot de passe du compte Dr.Web ou scanner l'empreinte digitale (si le [paramètre correspondant](#) est spécifié).

Écran de blocage

Si vous essayez de lancer une application bloquée, l'écran de blocage s'affiche (voir [Figure 21](#)). Pour accéder à l'application il faut saisir le mot de passe du compte et appuyer sur le bouton **Débloquer**. Vous pouvez également accéder à l'application avec l'empreinte digitale si l'option **Déverrouillage par empreinte digitale** est activée dans les [paramètres du Contrôle parental](#).

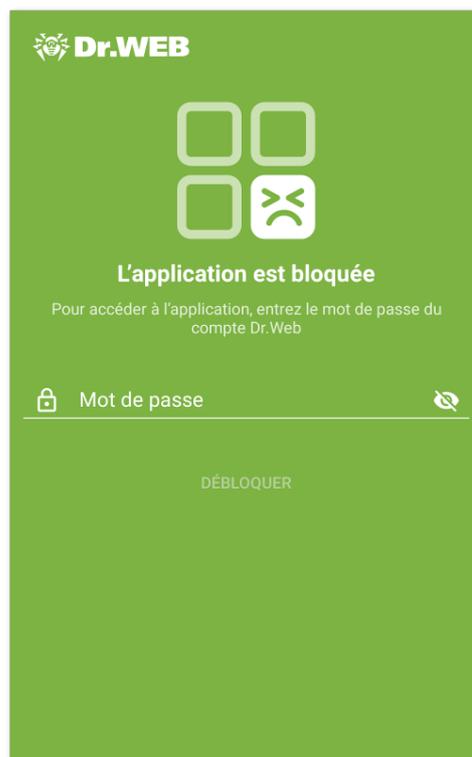


Figure 21. Écran de blocage de l'application

Nouvelles applications

Si l'option **Bloquer le lancement de nouvelles applications** est activée dans les paramètres du Contrôle parental, toutes les applications installées après l'activation de l'option feront partie du groupe système bloqué **Nouvelles applications**. Au lancement de l'application du groupe **Nouvelles applications**, l'option permettant d'autoriser l'accès permanent à l'application devient disponible sur l'écran de blocage.



Pour autoriser l'accès à la nouvelle application

1. Lancez l'application nécessaire.
2. Entrez le mot de passe du compte Dr.Web sur l'écran de blocage.
3. Cochez la case contre l'option **Exclure du groupe « Nouvelles applications »**.
4. Appuyez sur **Débloquer**.

8.5.2. Configuration du Contrôle parental

Vous pouvez ouvrir la section **Paramètres** (voir [Figure 22](#)) depuis l'écran d'accueil du composant. La section permet de gérer les paramètres du Contrôle parental et d'accéder au journal du Contrôle parental.

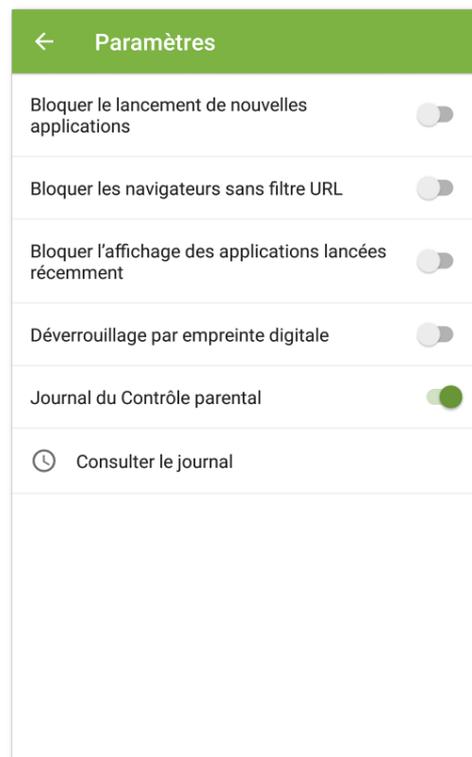


Figure 22. Configuration du Contrôle parental

Dans la section **Paramètres**, les options suivantes sont disponibles :

- **Bloquer le lancement de nouvelles applications.** Permet de bloquer l'accès aux applications installées sur l'appareil après l'activation de l'option. De nouvelles applications intègrent le groupe système **Nouvelles applications**. L'accès aux applications du groupe est toujours bloqué.



Vous pouvez autoriser l'accès à une application particulière avec l'option **Exclure du groupe « Nouvelles applications »** sur l'écran de blocage de cette application.



- **Bloquer les navigateurs sans Filtre URL.** Permet de bloquer l'accès aux [navigateurs non pris en charge par le Filtre URL](#). Les navigateurs intègrent le groupe système **Navigateurs sans Filtre URL**. L'accès aux applications de ce groupe est toujours bloqué.



L'activation de cette option requiert que le Filtre URL soit activé sur l'appareil.

- **Bloquer l'affichage des applications lancées récemment.** Permet de bloquer l'écran d'applications récemment lancées. En cas de tentative d'ouvrir l'écran d'applications récemment lancées, l'écran de blocage s'affiche.



L'option peut fonctionner incorrectement en cas d'utilisation d'interpréteur de commande du système de tierce partie.

- **Déverrouillage par empreinte digitale.** Permet d'utiliser l'empreinte digitale au lieu du mot de passe du compte Dr.Web pour débloquer les applications et les composants.



Avant d'activer l'option, assurez-vous que l'empreinte du propriétaire du compte Dr.Web est la seule qui est enregistrée sur l'appareil.

Le Scanner d'empreintes digitales sera désactivé après plusieurs erreurs de reconnaissance d'empreintes. Pour réactiver le scanner il faut déverrouiller l'appareil d'une autre manière spécifiée (mot de passe image, code PIN ou mot de passe).

- **Journal du Contrôle parental.** Active la [journalisation du Contrôle parental](#). Une fois l'option activée, l'option **Consulter le journal** devient disponible.

8.5.3. Journal du Contrôle parental

Le journal du Contrôle parental enregistre les événements liés aux applications et aux composants auxquels l'accès est bloqué ou limité.

Par défaut, les événements du journal du Contrôle parental sont représentés sous forme d'une liste d'événements regroupés par date. Le journal enregistre les événements suivants :

- Événements des applications :
 - tentative de lancement ;
 - déblocage.
- Événements des composants et du Contrôle parental:
 - activation ;
 - désactivation.

L'heure est indiquée pour chaque événement.



Affichage d'événements dans le journal

Pour faciliter la consultation, vous pouvez gérer l'affichage d'événements dans le journal du Contrôle parental : trier, filtrer ou regrouper les événements. Vous pouvez aussi rechercher par les événements.

Filtre d'événements

Pour trier ou filtrer les événements par un paramètre spécifié, appuyez sur l'icône  en bas à droite de l'écran et sélectionnez **Filtre**.

Les options suivantes de tri sont disponibles :

- par ordre chronologique croissant,
- par ordre chronologique décroissant,
- alphabétique (A-Z),
- alphabétique (Z-A).

Vous pouvez également spécifier un filtre par type d'événements: déblocage, tentative de lancement d'applications; activation, désactivation des composants.

Pour trier ou filtrer la liste d'événements, sélectionnez les valeurs nécessaires et retournez à la liste d'événements.

Vous pouvez revenir à l'affichage d'événements par défaut, en appuyant sur  en haut à droite de l'écran **Filtre d'événements**.

Recherche

Pour chercher dans le journal d'événements du Contrôle parental

1. Appuyez sur l'icône  en bas à droite de l'écran.
2. Dans le menu qui s'affiche, sélectionnez **Recherche**.
3. Saisissez un mot clé dans le champ de recherche en bas de l'écran.

Regroupement

Vous pouvez regrouper les événements par application ou par composant. Dans ce type de groupement, le journal du Contrôle parental est une liste d'applications et de composants, dont les événements ont été enregistrés dans le journal (voir [Figure 23](#)).

Pour regrouper les événements du journal du Contrôle parental, appuyez sur **Menu**  en haut à droite de l'écran du journal et cochez la case **Regrouper**. Appuyez sur le nom d'application ou de composant pour ouvrir la liste des événements relatifs.

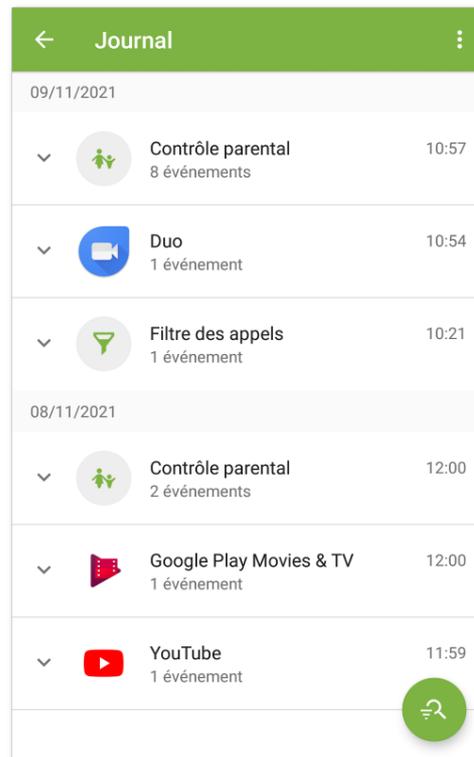


Figure 23. Regroupement d'événements

Filtre de groupes

Si nécessaire, vous pouvez trier les groupes d'événements selon un paramètre spécifié.

Pour trier les événements groupés

1. Appuyez sur l'icône  en bas à droite de l'écran.
2. Sélectionnez l'option **Filtre**.
3. Sur l'écran **Filtre de groupes**, sélectionnez un type de tri.
4. Retournez à la liste d'événements.

Vous pouvez revenir à l'affichage d'événements par défaut, en appuyant sur  en haut à droite de l'écran **Filtre de groupes**.



Sauvegarder le journal

Pour enregistrer le journal d'événements dans un fichier, appuyez sur **Menu**  en haut à droite de l'écran et sélectionnez **Sauvegarder le journal**.

Le journal est enregistré dans le fichier `DrWeb_Parental_Log.txt` situé dans le dossier `Android/data/com.drweb/files` dans la mémoire interne de l'appareil.



Sur les appareils tournant sous Android 11.0 ou une version supérieure, le journal est enregistré dans le dossier `Download/DrWeb`.

Vider le journal

Pour supprimer tous les événements du journal du Contrôle parental, appuyez sur **Menu**  sur l'écran du journal et sélectionnez l'élément **Vider le journal**.

8.6. Pare-feu Dr.Web

Le Pare-feu Dr.Web protège votre appareil mobile contre l'accès non autorisé et prévient la fuite de données importantes via le réseau. Il permet de contrôler les connexions et les transferts de données via le réseau, ainsi que de bloquer les connexions suspectes.

Technologie

Le Pare-feu Dr.Web se base sur la technologie VPN pour Android, ce qui lui permet de fonctionner sans obtenir les droits du super-utilisateur (root) de l'appareil. La réalisation de la technologie VPN sur Android est liée aux limitations particulières :

- À chaque instant, une seule application installée sur l'appareil peut utiliser le VPN. Quand l'application active le VPN sur l'appareil, une fenêtre demandant l'autorisation d'utiliser le VPN pour cette application s'ouvre. Si l'utilisateur permet à l'application d'utiliser le VPN, elle commence à l'utiliser, mais une autre application qui avait utilisé le VPN auparavant, ne peut plus y accéder. Une demande pareille s'affiche au premier démarrage du Pare-feu Dr.Web. On peut aussi la voir apparaître lors du redémarrage de l'appareil ou quand les autres applications demandent l'accès au VPN. Le VPN est partagé par les applications dans le temps, et le Pare-feu ne peut fonctionner que s'il possède les droits exclusifs d'utiliser le VPN.
- L'activation du Pare-feu Dr.Web peut provoquer l'impossibilité de connecter l'appareil sur lequel il est lancé aux autres appareils via Wi-Fi ou via le réseau local. Cela dépend du modèle de l'appareil et des applications utilisées pour la connexion.
- Si le Pare-feu Dr.Web est activé, l'appareil ne peut pas être utilisé comme un point d'accès Wi-Fi.



Le Pare-feu Dr.Web n'utilise la technologie VPN pour Android que pour exécuter ses fonctionnalités, il n'établit pas de tunnel VPN et le trafic n'est pas chiffré.

Pour activer le Pare-feu Dr.Web

1. Sélectionnez l'option **Pare-feu** sur l'[écran d'accueil](#) de Dr.Web.
2. Appuyez sur **Activer** ou utilisez l'interrupteur en haut à droite de l'écran.
Dr.Web demande l'autorisation de se connecter au VPN. Il faut accorder cette autorisation pour le fonctionnement correct du Pare-feu.

Pour activer le Pare-feu après le chargement de l'appareil, ouvrez l'application Dr.Web.

Sur les appareils tournant sous Android 7.0 ou une version supérieure, vous pouvez configurer l'activation automatique du Pare-feu Dr.Web après le chargement de l'appareil. Pour ce faire :

1. Dans les paramètres de l'appareil, sélectionnez **VPN**.
2. Ouvrez les paramètres du réseau **Dr.Web**.
3. Sur l'écran **Dr.Web** activez le paramètre **VPN permanent**.

Sur les appareils tournant sous Android 8.0 ou une version supérieure, vous pouvez bloquer l'accès à Internet après le chargement de l'appareil, avant que la connexion au VPN apparaisse. Pour ce faire, activez le paramètre **Se connecter uniquement via VPN**.



Si le droit d'utiliser le VPN est transmis à une autre application, le Pare-feu Dr.Web sera désactivé et une alerte correspondante s'affichera. Pour redémarrer le Pare-feu Dr.Web, il suffit d'appuyer sur cette alerte.

Si vous gérez l'appareil en mode d'accès limité (en mode d'invité), les paramètres du Pare-feu Dr.Web ne sont pas disponibles pour vous.

Écran d'accueil

L'écran d'accueil du Pare-feu contient les fiches d'informations de ses sections :

- [Limitation de trafic](#) (s'il y a une limitation active) : affiche les informations sur la limite courante du trafic.
- [Applications actives](#) : affiche le diagramme du volume du trafic entrant et sortant utilisé par les connexions réseau actives des applications.
- [Toutes les applications](#) : affiche le volume total du trafic entrant et sortant utilisé par les applications installées sur l'appareil.

Appuyez sur **En savoir plus** sur les fiches du trafic des applications et de la limitation du trafic pour accéder à la section correspondante.



Le menu en haut à droite de l'écran d'accueil permet :

- d'accéder au paramètre de [limitation du trafic mobile](#) ;
- d'ouvrir le [journal du Pare-feu](#).

8.6.1. Gestion de l'activité réseau des applications

Le Pare-feu Dr.Web permet de contrôler l'utilisation du trafic sur l'appareil et de configurer les paramètres généraux de l'accès des applications à Internet. La gestion générale comporte les fonctionnalités suivantes :

- suivi du [trafic actif](#) des applications en temps réel ;
- consultation de la [liste des applications utilisant le trafic Internet](#) et du volume du trafic qu'elles ont consommé ;
- gestion de l'accès à la [transmission de données](#) des applications par Wi-Fi, Internet mobile et en itinérance ;
- [limitation de la consommation totale du trafic](#) pendant une période spécifiée.

8.6.1.1. Applications actives

Dans la section **Applications actives**, vous pouvez voir en temps réel la liste des connexions actives initiées par les applications installées sur l'appareil. La section vous fournit un accès rapide à la gestion du trafic Internet actuel des applications.

Les applications au trafic actif maximal s'affichent sur la fiche de la section sur l'écran d'accueil du Pare-feu. Appuyez sur **En savoir plus** pour ouvrir la liste complète des applications aux connexions actives.

Les informations suivantes s'affichent pour chaque application sur l'écran **Applications actives** (voir [Figure 24](#)) :

- Volume total du trafic entrant et sortant par les connexions établies.
- [Accès à la transmission de données](#) par Wi-Fi, Internet mobile et en itinérance.
- Présence des paramètres utilisateur. Les applications dont l'accès à la transmission de données a été modifié sont marquées par l'icône .
- Présence des menaces système avec la connexion Internet bloquée. Les applications système dont l'accès à la transmission de données a été modifié sont marquées par l'icône .

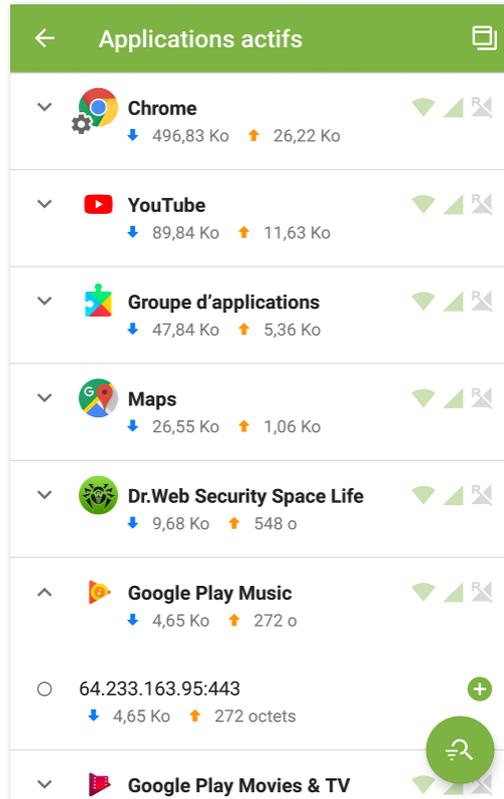


Figure 24. Applications actives

Connexion des applications

Pour voir les informations détaillées sur les connexions établies par une application, appuyez sur l'icône ▼ à gauche du nom de l'application sur l'écran **Applications actives** :

- liste des connexions établies ;
- volume du trafic entrant et sortant par chaque connexion établie ;
- présence d'une règle pour la connexion :
 - ● règle d'autorisation,
 - ● règle de blocage,
 - ● règle de redirection,
 - ○ aucune règle spécifiée.

Pour copier l'adresse d'une connexion, appuyez et maintenez la ligne contenant l'adresse de la connexion. L'adresse sera copiée dans le presse-papiers.

Appuyez sur la ligne de connexion pour accéder à l'écran [Connexion](#).



Règles de connexions

Vous pouvez gérer les connexions établies par les applications avec des règles d'autorisation, de blocage et de redirection (voir la section [Règles de connexions](#)). Pour créer ou éditer les règles, appuyez sur l'icône  ou  à droite de la connexion.

Tri d'applications

Pour trier la liste d'applications, appuyez sur l'icône  en bas à droite de l'écran. Ensuite, appuyez sur **Filtre** et choisissez les paramètres de tri nécessaires :

- tri décroissant du trafic - les applications au trafic maximal sont en haut de la liste ;
- tri croissant du trafic - les applications au trafic minimal sont en haut de la liste ;
- alphabétique (A-Z) ;
- alphabétique (Z-A).

Les applications sont triés par défaut dans l'ordre décroissant du trafic (les applications au trafic maximal se trouvent en haut de la liste). Pour restaurer le tri par défaut, appuyez sur l'icône  sur l'écran **Filtre**.

Recherche

Pour accéder rapidement à une application, utilisez la recherche par le nom de l'application.

Pour ce faire, appuyez sur l'icône  en haut à droite de l'écran. Ensuite, appuyez sur **Recherche** et entrez des mots clés de recherche dans le champ en bas de l'écran.

Pop-up

Pour avoir toujours la possibilité de voir les connexions Internet actives et de contrôler le volume du trafic entrant et sortant, vous pouvez activer le pop-up qui sera affiché par-dessus toutes les applications (voir [Figure 25](#)).

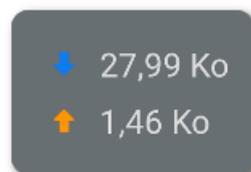


Figure 25. Pop-up

Pour activer le pop-up

1. Ouvrez l'écran **Applications actives** et appuyez sur l'icône  en haut à droite de l'écran (voir [Figure 24](#)).
2. Autorisez l'application à afficher le pop-up par-dessus les autres fenêtres.
Si l'autorisation d'affichage du pop-up par-dessus les autres fenêtres est révoquée, le pop-up ne s'affichera plus. Pour le réactiver, appuyez sur l'icône  en haut à droite de l'écran et accordez l'autorisation nécessaire.



Le volume total du trafic utilisée est calculé après l'activation de la fenêtre.

- Pour ouvrir la liste des applications qui utilisent des connexions Internet (voir [Figure 26](#)), appuyez sur la fenêtre pop-up.
- Pour fermer la liste des applications, appuyez sur .

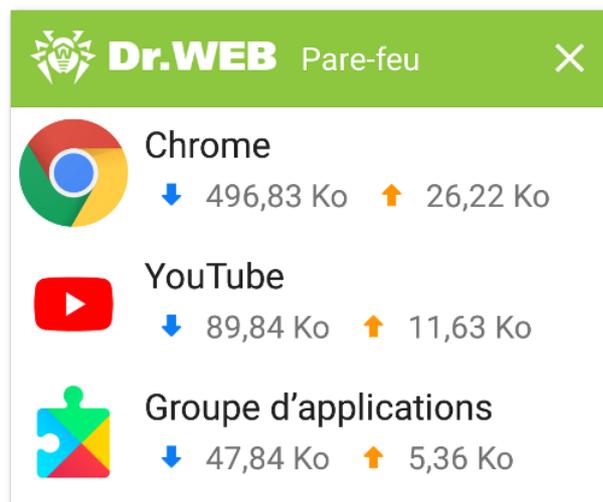


Figure 26. Liste des applications utilisant les connexions Internet

Pour désactiver le pop-up

- Ouvrez l'écran **Applications actives** et appuyez sur l'icône  en haut à droite de l'écran.

8.6.1.2. Toutes les applications

La section **Toutes les applications** contient la liste de toutes les connexions initiées par les applications installées sur l'appareil à partir du moment de l'activation du Pare-feu Dr.Web (y compris, par les applications supprimées si le [paramètre correspondant](#) est activé). La section permet de gérer l'accès de chaque application au trafic Internet.



La fiche de la section sur l'écran d'accueil du Pare-feu affiche le total du trafic entrant et sortant des applications à partir de l'activation du Pare-feu. Appuyez sur **En savoir plus** pour ouvrir la liste complète des applications.

Les informations suivantes s'affichent pour chaque application sur l'écran **Toutes les applications** :

- volume total du trafic entrant et sortant par les connexions établies ;
- accès à la transmission de données par Wi-Fi , Internet mobile  et en itinérance .

Appuyez sur le nom de l'application pour accéder à l'écran [Application](#) et voir les statistiques, les paramètres et les règles pour l'application.

Accès à la transmission de données

Avec le panneau **Accès à la transmission de données** sur l'écran **Toutes les applications**, vous pouvez configurer l'accès à la transmission des données par Wi-Fi, l'Internet mobile ou en itinérance pour toutes les applications ou certaines applications de la liste (pour en savoir plus, consultez la rubrique [Accès à la transmission de données](#)).

Filtrage et tri d'applications

Pour filtrer ou trier la liste d'applications, appuyez sur l'icône  en bas à droite de l'écran. Ensuite, appuyez sur **Filtre** et choisissez les paramètres de filtrage ou de tri nécessaires :

- Afficher les applications :
 - au trafic zéro.
- Trier :
 - tri décroissant du trafic - les applications au trafic maximal sont en haut de la liste ;
 - tri croissant du trafic - les applications au trafic minimal sont en haut de la liste ;
 - alphabétique (A-Z) ;
 - alphabétique (Z-A).

Les applications sont triées par défaut dans l'ordre décroissant du trafic (les applications au trafic maximal se trouvent en haut de la liste), les applications au trafic zéro ne s'affichent pas.

Pour restaurer l'affichage de la liste d'applications par défaut, appuyez sur l'icône  sur l'écran **Filtre**.

Recherche

Pour accéder rapidement à une application, utilisez la recherche dans la liste d'applications.

Pour ce faire, appuyez sur l'icône  en bas à droite de l'écran **Toutes les applications**.



Ensuite, appuyez sur **Recherche** et entrez un mot clé de recherche dans le champ en bas de l'écran.

Paramètres de toutes les applications

Pour spécifier les paramètres pour toutes les applications, appuyez sur **Menu**  sur l'écran **Toutes les applications** et sélectionnez l'option **Paramètres**.

Les paramètres suivants sont disponibles :

- **Utiliser le protocole Ipv6.** Permet d'activer ou de désactiver l'utilisation du protocole Ipv6 en parallèle avec IPv4.
- **Autoriser le protocole DNS au-dessus de TCP.** Permet d'activer ou de désactiver l'utilisation du protocole DNS par-dessus TCP pour la redirection de requêtes DNS et le masquage de noms de domaine.



L'utilisation du protocole DNS par-dessus TCP peut empêcher l'affichage de noms de domaine sur les écrans du Pare-feu.

Le paramètre fonctionne sur les appareils qui prennent en charge ce type de protocole. Par défaut, le paramètre est désactivé.

- **Bloquer les connexions pour les nouvelles applications** permet de bloquer l'accès des applications installées au réseau après l'activation de ce paramètre. Vous pouvez également bloquer les connexions par Wi-Fi et l'Internet mobile en cochant les cases correspondantes sous le paramètre.
- **Sauvegarder les règles et les statistiques après la suppression des applications** permet de sauvegarder les données d'une application supprimée de l'appareil pendant une période spécifiée : une semaine, un mois ou un an.

Toutes les règles

L'écran **Toutes les règles** comporte la liste de toutes les [règles de connexions](#) de toutes les applications (groupes d'applications).

Pour ouvrir la liste de toutes les règles, appuyez sur **Menu**  sur l'écran **Toutes les applications** et sélectionnez l'option **Toutes les règles**.

Les règles sont regroupées par le nom de l'application ou du groupe d'applications qui a établi la connexion. Les applications sont triées dans l'ordre alphabétique. Pour ouvrir la liste des règles pour les applications, appuyez sur l'icône ▼ à gauche du nom de l'application ou du groupe d'applications. Les règles de l'application s'affichent dans l'ordre de leur utilisation.



Pour modifier l'ordre d'utilisation des règles

- Appuyez et maintenez l'icône  contre la règle que vous voulez déplacer et faites glisser la règle à la position souhaitée dans la liste.

Pour effectuer une recherche dans la liste de toutes les règles

- Appuyez sur l'icône  en bas à droite de l'écran **Toutes les règles** et saisissez un mot clé dans le champ de recherche en bas de l'écran.

Les règles des applications peuvent être stockées sur l'appareil après la suppression de l'application pendant le délai indiqué si le [paramètre correspondant](#) est spécifié.

Effacer les données des applications

Pour supprimer les paramètres, les règles et les statistiques de toutes les applications

1. Appuyez sur **Menu**  sur l'écran **Toutes les applications** et sélectionnez l'option **Effacer**.
2. Cochez les cases contre les données que vous voulez supprimer.
3. Appuyez sur **Effacer**.

8.6.1.3. Accès à la transmission de données

Vous pouvez gérer l'accès des applications à la transmission de données. Vous pouvez configurer l'accès pour toutes les applications ou pour les applications individuelles :

- par Wi-Fi ,
- par l'Internet mobile ,
- par l'Internet mobile en itinérance .

Les modes d'accès disponibles sont marqués par la couleur verte, les modes d'accès bloqués - par la couleur grise.



La transmission de données par Wi-Fi et l'Internet mobile est autorisée par défaut pour toutes les applications, la transmission de données par l'Internet mobile en itinérance est bloquée.

Pour modifier l'accès à la transmission de données pour toutes les applications

- Sur l'écran **Toutes les applications**, appuyez sur **Wi-Fi**, **Internet mobile** ou **Itinérance** en haut de l'écran.

Pour modifier l'accès de certaines applications à la transmission de données

1. Sur l'écran **Toutes les applications**, appuyez et maintenez l'une des applications.
2. Sélectionnez les autres applications pour lesquels vous voulez modifier l'accès à la transmission de données.
3. Utilisez les icônes en haut à droite de l'écran pour autoriser/bloquer le mode correspondant de la transmission de données pour toutes les applications sélectionnées.
Pour quitter le mode de modification d'accès, appuyez sur **X** en haut à gauche de l'écran.

Pour modifier l'accès d'une seule application à la transmission de données

- Sur l'écran [Application](#), ouvrez l'onglet **Paramètres** et touchez l'icône ,  ou .

Les applications dont l'accès à la transmission de données a été modifié sont marquées par l'icône .

8.6.1.4. Limitation de l'utilisation du trafic mobile

Le Pare-feu Dr.Web permet de limiter l'utilisation du trafic mobile pendant la période spécifiée.



La fonction n'est pas disponible sur les appareils pour lesquelles l'utilisation des cartes SIM n'est pas prévue (il n'y a pas de logement de la carte SIM).

Pour spécifier une limite du trafic

1. Sur l'écran d'accueil du Pare-feu Dr.Web, appuyez sur **Menu**  et sélectionnez l'option **Limitation de trafic**.
2. Appuyez sur **Limite**.
3. Spécifiez une limite du trafic (en mégaoctets ou en gigaoctets).
4. Si nécessaire, indiquez le volume du trafic utilisé dès le début de la période de limitation sélectionnée (le décompte du temps commence à 00:00 le jour en cours).
5. Appuyez sur **Enregistrer**.
6. Sélectionnez la période de validité de la limite : jour, semaine ou mois. Si vous sélectionnez **Semaine** ou **Mois**, indiquez le jour de la semaine ou la date quand la limite sera actualisée pendant la période sélectionnée en cours.
7. Si nécessaire, cochez la case **Notifier lorsque la limite de l'Internet mobile est atteinte** pour recevoir les alertes lorsque la limite spécifiée est atteinte.
8. Appuyez sur l'icône  en haut à droite de l'écran.

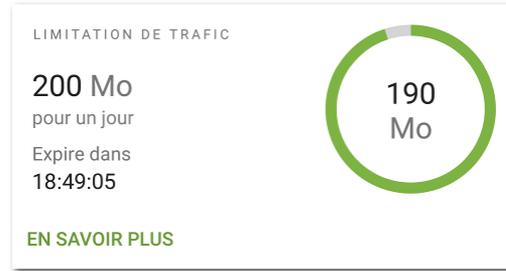


Figure 27. Limitation de trafic

Lorsque la limitation d'utilisation du trafic est activée, un diagramme s'affiche sur la fiche **Limitation de trafic** de l'écran d'accueil du Pare-feu Dr.Web. Le diagramme représente le volume du trafic mobile restant. La limite spécifiée et le compte à rebours de la validité de la limite sont affichés à côté du diagramme (voir [Figure 27](#)).



Le trafic mobile ne peut dépasser la limite spécifiée que de 4 Ko.

Appuyez sur **En savoir plus** sur la fiche de la limite pour accéder à l'écran **Limitation de trafic**.

Pour modifier la limite du trafic actuel

1. Ouvrez l'écran **Limitation de trafic**.
2. Apportez les modifications nécessaires.
3. Appuyez sur l'icône  en haut à droite de l'écran pour enregistrer les modifications.

Pour désactiver la limitation du trafic

- Appuyez sur le bouton **Désactiver** sur l'écran **Limitation de trafic** et confirmez l'action.

8.6.2. Trafic des applications individuelles

Le Pare-feu Dr.Web permet de configurer et de surveiller le traitement du trafic Internet au niveau des applications individuelles et des connexions qu'elles établissent. Ainsi, vous pouvez contrôler l'accès des programmes et des processus aux ressources réseau.

Sur l'écran **Application**, vous pouvez voir les statistiques d'utilisation du trafic, spécifier les règles individuelles et les paramètres d'utilisation du trafic et d'établissement de connexions pour chaque application (dans certains cas - pour un groupe d'applications). Vous pouvez également consulter tous les événements du Pare-feu liés à l'application.

Pour ouvrir l'écran **Application** (voir [Figure 28](#)), effectuez l'une des actions suivantes :

- Sur l'écran **Applications actives** ou **Toutes les applications**, appuyez sur le nom de l'application dans la liste.
- Sur l'écran [Connexion](#), appuyez sur l'icône ↗ à droite du nom de l'application.

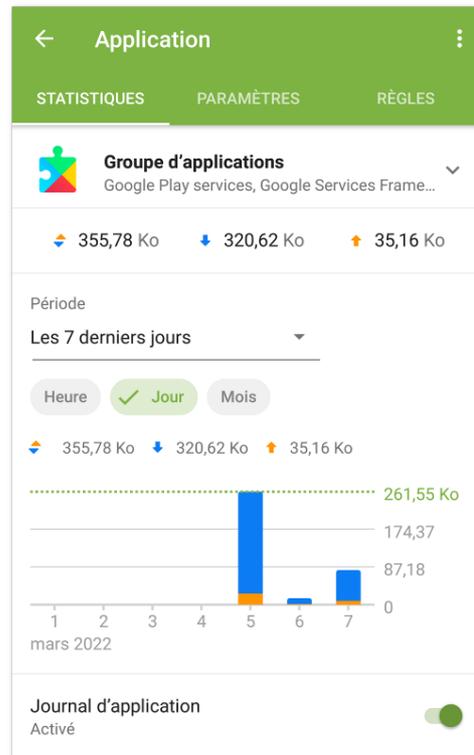


Figure 28. Écran Application

Trois onglets sont disponibles sur l'écran **Application** : **Statistiques**, **Paramètres** et **Règles**.

8.6.2.1. Statistiques d'utilisation du trafic Internet

Les statistiques d'utilisation du trafic Internet de toute application installée sont présentées sous forme d'un diagramme (voir [Figure 29](#)).

Pour consulter les statistiques d'utilisation du trafic, appuyez sur le nom de l'application dans la liste sur l'écran **Applications actives** ou **Toutes les applications**.

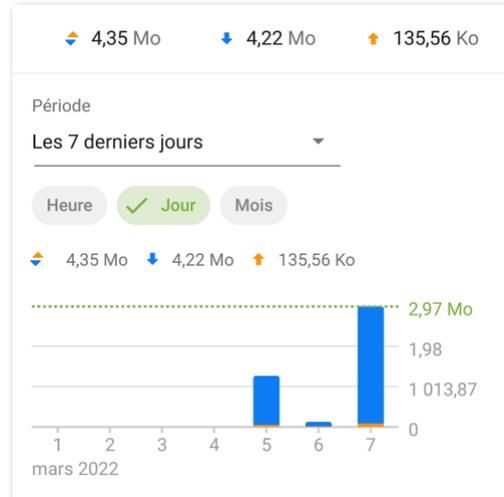


Figure 29. Statistiques d'utilisation du trafic Internet de l'application

Le volume du trafic consommé par l'application à partir de l'activation du Pare-feu est indiqué sous nom de l'application dans l'onglet **Statistiques**.

Dans le diagramme, le trafic sortant de l'application est marqué par la couleur orange, le trafic entrant est marqué par la couleur bleue. Les valeurs numériques du trafic (total, sortant et entrant) consommé pendant la période indiquée sont affichées sous le diagramme.

Lors de la consultation des statistiques d'utilisation du trafic Internet, vous pouvez effectuer les actions suivantes :

- Sélectionner une période d'affichage des statistiques. Vous pouvez consulter les statistiques pour la journée en cours, les 7 derniers jours, le mois actuel, le mois précédent ou spécifier les dates de début et de fin d'une période. Sélectionnez la période nécessaire dans la liste déroulante **Période** au-dessus du diagramme.
- Dans le cadre de la période sélectionnée, vous pouvez configurer l'affichage des statistiques par heures, jours ou mois. Sélectionnez l'option d'affichage correspondante au-dessus du diagramme.

Vous pouvez faire défiler le diagramme à gauche ou à droite jusqu'à la valeur nécessaire, si le graphique ne s'affiche pas entièrement.

Effacer les statistiques

- Effacer les statistiques d'une application spécifique :
 1. Sur l'écran **Applications actives** ou **Toutes les applications**, appuyez sur le nom de l'application dont vous voulez effacer les statistiques.
 2. Appuyez sur **Menu**  en haut à droite de l'écran **Application** et sélectionnez l'option **Effacer**.
 3. Dans la fenêtre qui s'affiche, cochez la case **Statistiques des applications** et appuyez sur **Effacer**.



- Effacer les statistiques de toutes les applications :
 1. Appuyez sur **Menu**  sur l'écran **Toutes les applications** et sélectionnez l'option **Effacer**.
 2. Dans la fenêtre qui s'affiche, cochez la case **Statistiques des applications** et appuyez sur **Effacer**.



Après la suppression de l'application de l'appareil, les statistiques de l'application seront effacées automatiquement dans le délai de 5 minutes.

Journal d'application

Les événements liés à l'activité réseau des applications installées sur l'appareil sont enregistrés dans les [journaux d'applications](#). Utilisez l'interrupteur pour commencer ou reprendre la journalisation de l'application. Pour accéder au journal, appuyez sur **Consulter le journal**.

8.6.2.2. Paramètres de l'application

Accès à la transmission de données

Vous pouvez autoriser ou bloquer pour l'application la transmission de données par Wi-Fi , l'Internet mobile  et l'Internet mobile en itinérance  en touchant l'icône correspondante (voir la section [Accès à la transmission de données](#)).

Bloquer toutes les connexions sauf celles autorisées par les règles

Pour bloquer par défaut toutes les connexions pour l'application, cochez la case **Bloquer toutes les connexions sauf celles autorisées par les règles**. Si les règles d'autorisation ne sont pas spécifiées pour l'application, elle ne pourra établir aucune connexion.

Si le paramètre **Bloquer toutes les connexions sauf celles autorisées par les règles** est activé pour l'application, une règle d'autorisation sera automatiquement ajoutée pour le port 53. La présence de la règle (pour les protocoles DNS, UDP ou ALL) est obligatoire pour le fonctionnement des règles avec les noms de domaine.



Lorsqu'il y a des règles d'autorisation avec les noms de domaine, il est nécessaire de désactiver également l'utilisation du serveur DNS personnel dans les paramètres de l'appareil pour un fonctionnement correct du paramètre.

Ne pas surveiller l'application



La fonction est disponible sur les appareils tournant sous Android 5.0 ou une version supérieure.

Le paramètre n'est pas disponible pour certaines applications système.

Le Pare-feu Dr.Web est réalisé sur la base du VPN pour Android. Le VPN empêche le fonctionnement des applications qui utilisent la technologie non compatible avec le VPN, par exemple, Wi-Fi Direct. Cela peut provoquer l'impossibilité de connexion de l'appareil aux autres appareils. Dans ce cas, vous pouvez désactiver le contrôle du Pare-feu Dr.Web pour l'application (le groupe d'applications) nécessaire en cochant la case **Ne pas surveiller l'application**.

Il est recommandé de désactiver le contrôle du Pare-feu Dr.Web uniquement pour les application fiables.

Une fois l'option activée, le Pare-feu Dr.Web ne contrôle pas les connexions réseau de cette application, même si les restrictions sont spécifiées dans les paramètres du Pare-feu. Le trafic de l'application n'est pas pris en compte.

8.6.2.3. Règles de connexions

La gestion du trafic se fait au niveau des connexions établies par les applications. Pour chaque application installée sur l'appareil, vous pouvez spécifier les règles d'autorisation, les règles de blocage et les règles de redirection des connexions avec les adresses IP et les ports spécifiques.

Les règles de connexions sont disponibles sur l'onglet [Règles](#) de l'écran **Application** ainsi que sur l'écran [Toutes les règles](#).

Connexions

Les informations générales s'affichent sur l'écran **Connexion** (voir [Figure 30](#)). Pour accéder à cet écran, effectuez l'une des actions suivantes :

- Sur l'écran [Applications actives](#), appuyez sur l'icône ▼ à gauche du nom de l'application. Ensuite, appuyez sur la ligne de la connexion.
- Dans le [journal du Pare-feu](#) :
 - En mode de groupement par date : appuyez sur la ligne de la connexion.
 - En mode de groupement par nom d'application : ouvrez la liste des connexions de l'application en appuyant sur l'icône ▼ à gauche du nom de l'application. Ensuite, appuyez sur la ligne de la connexion.
- Dans le [journal de l'application](#) : ouvrez la liste des connexions en appuyant sur l'icône ▼ à droite de la date de l'événement. Ensuite, appuyez sur la ligne de la connexion.

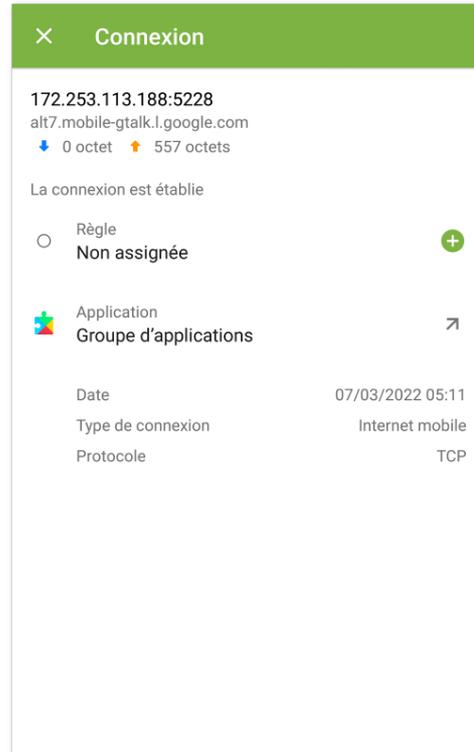


Figure 30. Écran Connexion

L'écran **Connexion** contient les informations suivantes :

- adresse et port de la connexion ;
- nom de l'hôte (si disponible) ;
- volume du trafic entrant et sortant reçu ou transmis par la connexion ;
- statut de la connexion ;
- règle de la connexion ;
- application qui a établi la connexion ;
- date et heure ;
- type de connexion ;
- protocole.

Pour copier l'adresse d'une connexion

1. Appuyez et maintenez la ligne d'adresse. Vous passerez en mode de copie. L'adresse sera marquée par le gris.
2. Appuyez sur l'icône  en haut à droite de l'écran. L'adresse sera copiée dans le presse-papier.

Pour quitter le mode de copie, appuyez sur l'icône  en haut à gauche de l'écran.



Règles de connexions

Création de règles

Pour créer une nouvelle règle pour la connexion

1. Pour une connexion sans règles :

- Sur l'écran **Connexion**, appuyez sur l'icône  à droite de l'élément **Règle**.
- Sur l'écran **Applications actives**, ouvrez la liste des connexions établies et appuyez sur l'icône  à droite de l'adresse de la connexion.

Pour toute connexion :

- Appuyez sur l'icône  dans l'onglet **Règles** en bas à droite de l'écran **Application**.

2. Dans la fenêtre qui s'ouvre, sélectionnez un type de règle :

-  règle d'autorisation,
-  règle de blocage,
-  règle de redirection.

3. Vérifiez si l'adresse IP/le nom de l'hôte est indiqué correctement. Si l'adresse n'est pas indiquée, entrez une adresse IP valide (au format a.b.c.d pour les adresses IPv4 ou [a:b:c:d:e:f:g:h] pour les adresses IPv6), une étendue d'adresses IP (au format a1.b1.c1.d1-a2.b2.c2.d2 ou [a1:b1:c1:d1:e1:f1:g1:h1]-[a2:b2:c2:d2:e2:f2:g2:h2]), un réseau entier (au format a.b.c.0/n, où n est un nombre entre 1 et 32). Si vous créez une règle de redirection, indiquez l'adresse de redirection dans le champ en bas. Vous pouvez indiquer le nom de l'hôte à la place de l'adresse.

4. Appuyez sur **Options supplémentaires** pour spécifier le paramètre supplémentaire **Protocole** — protocole réseau pour la connexion.

5. Appuyez sur l'icône  pour enregistrer les modifications.

Les applications ayant des règles de connexions spécifiées sont marquées par l'icône .

Consulter les règles

Pour consulter les règles de connexions

• Pour une application spécifique :

- Ouvrez l'écran **Application** et accédez à l'onglet **Règles**.

L'onglet contient la liste de toutes les règles spécifiées pour cette application dans l'ordre de leur utilisation.

• Pour toutes les applications :



1. Sur l'écran d'accueil du Pare-feu, appuyez sur **En savoir plus** dans la fiche de la section **Toutes les applications**.
2. Appuyez sur **Menu**  sur l'écran **Toutes les applications** et sélectionnez l'option **Toutes les règles**.

L'écran **Toutes les règles** contient la liste de toutes les règles de connexions regroupées par le nom de l'application ou du groupe d'applications qui a établi la connexion. Les applications sont triées dans l'ordre alphabétique. Pour ouvrir la liste des règles pour les applications, appuyez sur l'icône  à gauche du nom de l'application ou du groupe d'applications. Les règles de l'application s'affichent dans l'ordre de leur utilisation.

Pour modifier l'ordre d'utilisation des règles

- Appuyez et maintenez l'icône  contre la règle que vous voulez déplacer et faites glisser la règle à la position souhaitée dans la liste.

Pour effectuer une recherche dans la liste de toutes les règles

- Appuyez sur l'icône  en bas à droite de l'écran **Toutes les règles** et saisissez un mot clé dans le champ de recherche en bas de l'écran.

Les règles des applications peuvent être stockées sur l'appareil après la suppression de l'application pendant le délai indiqué si le [paramètre correspondant](#) est spécifié.

Modification des règles

Pour modifier une règle existante

1. Effectuez l'une des actions suivantes :
 - Sur l'écran **Connexion**, appuyez sur l'icône  à droite de la règle.
 - Sur l'écran **Applications actives**, appuyez sur l'icône  à gauche du nom de l'application. Ensuite, appuyez sur l'icône  contre la connexion dont vous voulez modifier la règle.
 - Appuyez sur la ligne de la connexion dans l'onglet **Règles** sur l'écran **Application**.
 - Appuyez sur l'icône  à gauche du nom de l'application sur l'écran **Toutes les règles**. Ensuite, appuyez sur la ligne de la règle.
2. Apportez les modifications nécessaires.
3. Appuyez sur l'icône  pour enregistrer les modifications.

Suppression des règles

Pour supprimer une règle

- Sur l'écran de modification de la règle :



1. Appuyez sur **Supprimer la règle**.
 2. Dans la fenêtre qui s'affiche, appuyez sur **Supprimer**.
- Dans l'onglet **Règles** ou sur l'écran **Toutes les règles** :
 1. Faites défiler la règle à gauche et appuyez sur l'icône .
 2. Dans la fenêtre qui s'affiche, appuyez sur **Supprimer**.

Pour supprimer toutes les règles pour une application particulière

1. Appuyez sur **Menu**  en haut à droite de l'écran **Application** et sélectionnez l'option **Effacer**.
2. Dans la fenêtre qui s'affiche, cochez la case **Règles pour les applications**. Appuyez sur **Effacer**.

Pour supprimer toutes les règles pour toutes les applications

1. Appuyez sur **Menu**  sur l'écran **Toutes les règles** et sélectionnez l'option **Effacer**.
2. Appuyez sur **Effacer**.

Importation et exportation des règles

Vous pouvez exporter les listes de règles créées dans un fichier de la mémoire interne de l'appareil. Vous pourrez les importer depuis ce fichier en cas de besoin, par exemple, si vous réinstallez Dr.Web ou l'utilisez sur un autre appareil.

Pour exporter les règles dans un fichier

- Règles pour une application spécifique :
 1. Appuyez sur **Menu**  en haut à droite de l'écran **Application** dans l'onglet **Règles** et sélectionnez l'option **Exportation des règles**.
 2. Appuyez sur **OK**.
- Règles de toutes les applications :
 1. Appuyez sur **Menu**  en haut à droite de l'écran **Toutes les règles** et sélectionnez l'option **Exportation des règles**.
 2. Appuyez sur **OK**.

Les règles sont exportées dans le fichier

`DrWeb_Firewall_Rules_<nom_de_l'application>.hsts` si ce sont les règles pour l'application ou dans le fichier `DrWeb_Firewall_Rules_ALL.hsts` si ce sont les règles pour toutes les applications. Le fichier contenant les règles est sauvegardé dans le dossier `Internal storage/Android/data/com.drweb/files/`.



Sur les appareils tournant sous Android 11.0 ou une version supérieure, le fichier comportant les règles est enregistré dans le dossier `Download/DrWeb`.

Pour importer les règles du fichier

- Règles pour une application spécifique :
 1. Appuyez sur **Menu** en haut à droite de l'écran **Application** dans l'onglet **Règles** et sélectionnez l'option **Importation des règles**.
 2. Dans l'arborescence de fichiers, trouvez le fichier de règles et appuyez dessus.
- Règles de toutes les applications :
 1. Appuyez sur **Menu** en haut à droite de l'écran **Toutes les règles** et sélectionnez l'option **Importation des règles**.
 2. Dans l'arborescence de fichiers, trouvez le fichier de règles et appuyez dessus.

Bloquer toutes les connexions sauf celles autorisées par les règles

En cochant la [case correspondante](#) sur l'écran des paramètres de l'application, vous pouvez bloquer toutes les connexions de l'application sauf celles qui sont autorisées par les règles.

8.6.2.4. Journal de l'application

Les événements des connexions réseau sont enregistrés dans les journaux d'applications.

Pour activer la journalisation de l'application

- Utilisez l'interrupteur **Journal d'application** dans l'onglet **Statistiques** sur l'écran **Application**.

Pour ouvrir le journal de l'application

- Sélectionnez l'élément **Consulter le journal** dans l'onglet **Statistiques** sur l'écran **Application**.

Toutes les connexions de cette application sont groupées par date. Pour ouvrir la liste des connexions pour une date précise, appuyez sur l'icône ▼ à droite de la date. Pour chaque connexion dans la liste, les informations suivantes sont disponibles :

- adresse et port de la connexion ;
- trafic consommé ;
- heure d'établissement de la connexion ;
- présence d'une règle pour la connexion :
 - ● règle d'autorisation,



- ● règle de blocage,
- ● règle de redirection,
- ○ aucune règle spécifiée.

Appuyez sur la ligne de connexion pour accéder à l'écran [Connexion](#) et configurer les règles pour cette connexion.

Pour copier l'adresse d'une connexion

- Appuyez et maintenez la ligne contenant l'adresse de la connexion. L'adresse sera copiée dans le presse-papiers.

Pour vider le journal de l'application

1. Appuyez sur l'icône  en haut à droite de l'écran du journal de l'application.
2. Dans la fenêtre qui s'affiche, appuyez sur le bouton **Effacer**.

Pour désactiver la journalisation de l'application

- Utilisez l'interrupteur **Journal d'application** dans l'onglet **Statistiques** sur l'écran **Application**.

8.6.3. Journal du Pare-feu Dr.Web

Les événements liés au fonctionnement du Pare-feu sont enregistrés dans le journal du Pare-feu Dr.Web.

Pour ouvrir la liste complète de tous les événements liés au fonctionnement du Pare-feu Dr.Web, appuyez sur **Menu**  sur l'écran d'accueil du composant Pare-feu et sélectionnez l'option **Journal**.

Le journal du Pare-feu contient les informations suivantes concernant l'événement :

- nom de l'application ;
- adresse et port de la connexion (ainsi que l'adresse de redirection si la règle correspondante est spécifiée) ;
- trafic consommé ;
- date et heure de l'événement ;
- présence d'une règle pour la connexion.

Quand vous appuyez sur l'événement, l'écran [Connexion](#) s'affiche.

Pour filtrer ou trier les événements dans le journal du Pare-feu

1. Appuyez sur l'icône  en bas à droite de l'écran **Journal**. Ensuite, appuyez sur **Filtre**.



2. Sélectionnez les paramètres de filtrage ou de tri nécessaires :

- Trier :
 - par ordre chronologique décroissant - les derniers événements sont en haut du journal ;
 - par ordre chronologique croissant — les derniers événements sont en bas du journal ;
 - alphabétique (A-Z) ;
 - alphabétique (Z-A).
- Afficher les connexions :
 - établies,
 - réinitialisées,
 - redirigées,
 - avec une erreur.

Par défaut les événements sont triés par date (les derniers événements se trouvent en haut du journal), tous les types de connexions sont affichés. Pour restaurer l’affichage du journal par défaut, appuyez sur l’icône  sur l’écran **Filtre**.

Pour faciliter la consultation du journal, vous pouvez également grouper les événements par application.

Pour grouper les événements par application

- Sur l’écran **Journal**, appuyez sur **Menu**  en haut à droite et cochez la case **Regrouper**.

Pour effectuer une recherche dans le journal du Pare-feu

1. Appuyez sur l’icône  en bas à droite de l’écran **Journal**. Ensuite, appuyez sur **Recherche**.
2. Saisissez un mot clé dans le champ de recherche en bas de l’écran.

Pour copier l’adresse d’une connexion

- Appuyez et maintenez la ligne contenant l’adresse de la connexion. L’adresse sera copiée dans le presse-papiers.

Pour vider le journal du Pare-feu

1. Appuyez sur **Menu**  et sélectionnez l’option **Effacer**.
2. Confirmez l’action en appuyant sur le bouton **Effacer**.



Taille du journal

Par défaut, la taille du fichier de journal est de 5 Mo.

Pour modifier la taille maximale du fichier de journal

1. Appuyez sur **Menu**  sur l'écran du journal du Pare-feu et sélectionnez l'option **Taille du journal**.
2. Dans la fenêtre qui s'affiche, modifiez la valeur et appuyez sur **OK**.



La taille maximale du journal doit être supérieure à 0 Mo et inférieure ou égale à 99 Mo .

8.7. Contrôleur de sécurité

Dr.Web effectue le diagnostic de votre appareil et donne des recommandations pour résoudre les problèmes et les vulnérabilités détectés à l'aide du composant spécifique Contrôleur de sécurité. Le composant est lancé automatiquement après le premier démarrage de l'application et l'enregistrement de la licence.

Problèmes de sécurité et moyens de les neutraliser

Dr.Web détecte les problèmes de sécurité suivants :

- [Vulnérabilités](#) ;
- [Paramètres système](#) qui influencent la sécurité de l'appareil.
- [Logiciels en conflit](#) ;
- [Administrateurs de l'appareil non affichés](#) ;
- [Applications utilisant la vulnérabilité Fake ID](#).
- [Paramètres d'optimisation](#).

Pour ouvrir la liste des problèmes de sécurité détectés (voir [Figure 31](#)), sélectionnez **Contrôleur de sécurité** sur l'écran d'accueil de Dr.Web.

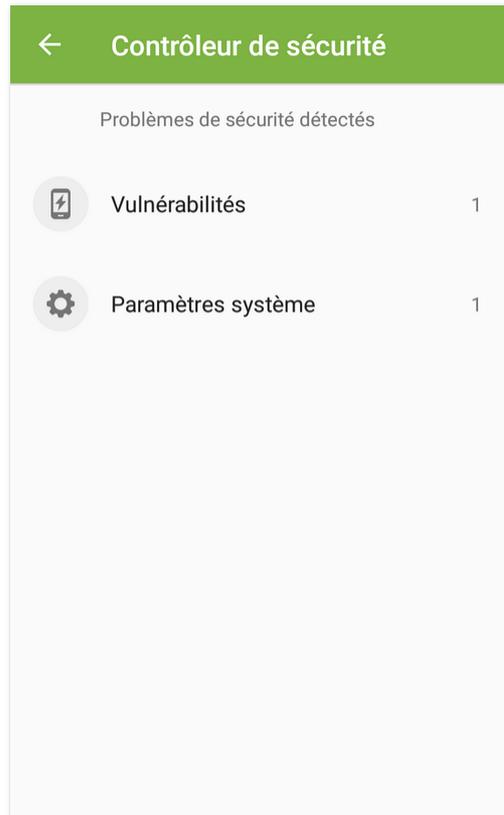


Figure 31. Contrôleur de sécurité

8.7.1. Vulnérabilités

Une *vulnérabilité* est une faille dans le code de programme qui peut être utilisée par les cybercriminels afin de perturber le fonctionnement du système.

Le Contrôleur de sécurité détecte les vulnérabilités suivantes dans le système de l'appareil : [BlueBorne](#), [EvilParcel](#), [Extra Field](#), [Fake ID](#), [Janus](#), [ObjectInputStream Serialization](#), [OpenSSLX509Certificate](#), [PendingIntent](#), [SIM Toolkit](#), [Stagefright](#) et [Stagefright 2.0](#).

En utilisant les vulnérabilités, les cybercriminels peuvent ajouter un code de programmation dans les applications. De ce fait, ces applications peuvent accomplir des fonctions dangereuses pour la sécurité de l'appareil.

Si le système de votre appareil contient une ou plusieurs vulnérabilités, veuillez vérifier s'il y a des mises à jour pour le système d'exploitation sur le site Web officiel du fabricant de votre appareil. Les vulnérabilités peuvent être résolues dans des nouvelles versions du système d'exploitation. S'il n'y a pas de mises à jour, il est recommandé d'installer des logiciels provenant uniquement des sources de confiance.



Accès root

L'appareil peut devenir vulnérable aux menaces s'il est rooté, c'est-à-dire, s'il a été soumis à une procédure de rootage afin d'obtenir les droits de super-utilisateur (root). Cela permet de modifier et de supprimer des fichiers système, ce qui peut rendre l'appareil inopérable. Si vous avez apporté ces modifications vous-même, il est recommandé de les annuler pour des raisons de sécurité. Si l'accès root est une particularité technique de votre appareil, ou qu'il est nécessaire pour exécuter certaines tâches, vous devez porter une attention particulière aux applications provenant de sources inconnues.

8.7.2. Paramètres système

Le Contrôleur de sécurité détecte les paramètres système suivants qui influencent la sécurité de l'appareil :

- **Débogage activé.** Le débogage USB est destiné aux développeurs et permet de copier les données depuis l'ordinateur sur l'appareil tournant sous Android et vice versa, d'installer les applications sur l'appareil, de voir des journaux des applications installées et de les supprimer dans certains cas. Si vous n'êtes pas développeur et n'utilisez pas ce mode de débogage, il est recommandé de le désactiver. Pour ouvrir la section correspondante des paramètres système, appuyez sur **Paramètres** sur l'écran contenant les informations détaillées sur ce problème.
- **Installation depuis des sources inconnues activée.** L'installation des applications depuis les sources inconnues est la raison principale de la diffusion des menaces sur les appareils tournant sous Android 7.1 ou une version antérieure.

Les applications installées depuis d'autres sources que la boutique d'applications officielle sont souvent dangereuses et elles peuvent endommager l'appareil. Pour réduire les risques d'installer des applications malveillantes, il est recommandé d'interdire l'installation d'applications depuis des sources inconnues. Pour ouvrir la section correspondante des paramètres système, appuyez sur **Paramètres** sur l'écran contenant les informations détaillées sur ce problème.

Il est recommandé d'effectuer l'analyse antivirus de toutes les applications avant leur installation. Avant l'analyse, assurez-vous que les bases virales Dr.Web [sont à jour](#).

- **Les notifications Dr.Web sont bloquées.** Dans ce cas, Dr.Web ne peut pas vous informer des menaces détectées. Cela réduit la protection de l'appareil et peut provoquer son infection. C'est pourquoi, il est recommandé d'accéder aux paramètres de votre appareil et d'activer les notifications de Dr.Web.
- **Un certificat racine utilisateur est installé.** Si des certificats utilisateur sont détectés sur l'appareil, les détails seront affichés dans le Contrôleur de sécurité. Les certificats utilisateur permettent à des tiers de consulter votre activité réseau. Si vous ne connaissez pas la désignation des certificats détectés, il est recommandé de les supprimer de votre appareil.



8.7.3. Logiciels en conflit

L'utilisation de logiciels en conflit, notamment des navigateurs non supportés par le Filtre URL affaiblit la protection de l'appareil. Dans ces navigateurs, l'utilisateur n'est pas protégé contre les ressources Internet indésirables ou malveillantes. Par conséquent, il est recommandé d'utiliser en tant que navigateur par défaut le navigateur standard Android, Google Chrome, Yandex.Browser, Microsoft Edge, Firefox, Firefox Focus, Opera, Adblock Browser, Dolphin Browser, Sputnik, Boat Browser et Atom.

8.7.4. Administrateurs de l'appareil non affichés

Les applications activées en tant qu'administrateurs de l'appareil, mais qui ne sont pas présentes dans la liste des administrateurs de la section correspondante des paramètres de l'appareil, ne peuvent pas être supprimées à l'aide des outils standard du système d'exploitation. Dans la plupart des cas, telles applications sont dangereuses.

Si vous ne savez pas pourquoi l'application masque sa présence dans la liste des administrateurs de l'appareil, il est recommandé de la supprimer. Pour supprimer l'application appuyez sur **Supprimer** sur l'écran contenant les informations détaillées sur le problème lié à cette application.

8.7.5. Applications utilisant la vulnérabilité Fake ID

Si les applications utilisant la vulnérabilité Fake ID sont détectées sur l'appareil, elles seront affichées dans une section à part du Contrôleur de sécurité. Ces applications peuvent être malveillantes, c'est pourquoi il est recommandé de les supprimer. Pour supprimer une application, appuyez sur le bouton **Supprimer** sur l'écran contenant les informations détaillées sur le problème lié à cette application ou utilisez les outils de l'OS.

8.7.6. Paramètres d'optimisation

Le système d'exploitation de l'appareil peut arrêter les processus des applications qui ne sont pas en cours d'utilisation. Cette optimisation des processus de fond permet d'économiser la batterie et d'améliorer les performances, mais elle peut influencer le fonctionnement des applications.

L'application Dr.Web doit fonctionner sans arrêt pour assurer une protection antivirus permanente et l'efficacité des composants supplémentaires : [Filtre des appels et des SMS](#), [Filtre URL](#), [Antivol](#), [Contrôle parental](#) et [Pare-feu](#).

Pour un fonctionnement correct de l'application, supprimez les restrictions de l'application en arrière-plan. Pour ce faire, vérifiez les paramètres de l'appareil et du gestionnaire d'applications intégré.



L'ensemble de paramètres dépend du modèle d'appareil :

- [Asus](#)
- [Huawei](#)
- [Meizu](#)
- [Nokia](#)
- [OnePlus](#)
- [Oppo](#)
- [Samsung](#)
- [Sony](#)
- [Xiaomi](#)



Les instructions fournies dans les sections indiquées peuvent ne pas correspondre en partie à certains appareils car les paramètres peuvent varier sur de différents modèles d'un appareil et dans des versions différentes du système d'exploitation. En cas d'incompatibilité, précisez l'ordre d'actions dans le manuel d'utilisateur de votre modèle d'appareil. Si le problème persiste, contactez le [support technique](#).

Suppression des autorisations



L'avertissement est affiché si Dr.Web n'a pas l'accès aux fonctionnalités spéciales.

A partir de la version Android 6.0, le système révoque les autorisations accordées par l'utilisateur, si vous n'utilisez pas l'application pendant quelques mois. Sous Android 12.0 ou une version supérieure, il bloque également l'affichage de notifications et vide le cache de l'application. Ainsi, le système économise la mémoire d'appareil et protège les données d'utilisateurs. Pourtant, Dr.Web ne pourra pas assurer une protection permanente de l'appareil si les [autorisations](#) nécessaires pour ses fonctionnalités essentielles et ses composants sont révoquées. Pour assurer un fonctionnement stable des composants, il est recommandé de désactiver la révocation automatique d'autorisations dans les paramètres de l'appareil. Pour aller à la section correspondante des paramètres système, appuyez sur le bouton **Paramètres** sur l'écran contenant les informations détaillées sur ce problème.

Accès aux paramètres

Sur les appareils tournant sous Android 13.0 ou une version supérieure, le système bloque par défaut l'accès des applications à certains paramètres. Cela permet de protéger les données confidentielles contre leur utilisation abusive par des applications malveillantes. Pourtant les composants de Dr.Web nécessitent l'accessibilité de l'appareil et la lecture de notifications pour protéger vos données et bloquer le contenu indésirable. Pour accéder au paramètre système autorisant l'accès aux paramètres nécessaires pour le fonctionnement de Dr.Web, suivez les instructions s'affichant à l'écran contenant les informations détaillées sur ce problème.



Le paramètre **Raccourci** dans le menu d'accessibilité active le bouton qui permet d'un seul appui d'activer et de désactiver l'accès de Dr.Web aux fonctionnalités spéciales depuis n'importe quel écran d'appareil. Il est recommandé de désactiver **Raccourci** afin d'éviter un appui accidentel.

8.7.6.1. Asus

Pour que l'application Dr.Web fonctionne correctement en arrière-plan sur les appareils Asus, effectuez les actions suivantes :

- [Autorisez le démarrage automatique](#)

Le démarrage automatique permet de lancer les application une fois l'appareil allumé. Cela est nécessaire pour une protection antivirus permanente de l'appareil et pour un fonctionnement correct des composants supplémentaires : [Filtre des appels et des SMS](#), [Filtre URL](#), [Antivol](#), [Contrôle parental](#) et [Pare-feu](#).

- [Autorisez le fonctionnement en arrière-plan](#)

Le fonctionnement en arrière-plan permet à l'application de rester lancée même si elle n'est pas active. Cela est nécessaire pour une protection antivirus permanente de l'appareil et pour un fonctionnement correct des composants supplémentaires : [Filtre des appels et des SMS](#), [Filtre URL](#), [Antivol](#), [Contrôle parental](#) et [Pare-feu](#).



Les paramètres peuvent différer selon les modèles d'appareil et les systèmes d'exploitation. Si ces instructions ne résolvent pas le problème, contactez le [support technique](#).

Pour autoriser le démarrage automatique

1. Dans les paramètres de l'appareil, ouvrez **Gestionnaire de démarrage automatique**.
2. Autoriser le démarrage automatique de l'application Dr.Web.

Pour autoriser le fonctionnement en arrière-plan

1. Dans l'application **Gestionnaire mobile**, ouvrez **Paramètres**.
2. Désactivez les paramètres **Nettoyage suspendu**.

8.7.6.2. Huawei

Appareils prenant en charge la gestion manuelle

Sur les appareils Huawei prenant en charge la gestion automatique et manuelle du lancement des applications, autorisez la gestion manuelle du lancement pour l'application Dr.Web.



La gestion manuelle permet à l'application de rester lancée même si elle n'est pas active et lancer les processus une fois l'appareil allumé. Cela est nécessaire pour une protection antivirus permanente de l'appareil et pour un fonctionnement correct des composants supplémentaires : [Filtre des appels et SMS](#), [Filtre URL](#), [Antivol](#), [Contrôle parental](#) et [Pare-feu](#).

Pour activer la gestion manuelle

- Sur les appareils tournant sous Android :
 1. Ouvrez **Batterie** > **Lancement d'application** dans les paramètres de l'appareil.
 2. Sélectionnez **Gérer manuellement**.
- Sur les appareils tournant sous l'OS Harmony :
 1. Dans les paramètres de l'appareil, ouvrez la section des paramètres du lancement des applications.
 2. Trouvez Dr.Web dans la liste et utilisez l'interrupteur qui se trouve à droite pour activer la gestion manuelle.
 3. Dans la fenêtre qui s'affiche, activez tous les paramètres de gestion supplémentaires et appuyez sur **OK**.

Autres appareils Huawei

Pour que l'application Dr.Web fonctionne correctement sur les appareils Huawei, modifiez les paramètres suivants :

- [Autorisez le fonctionnement en arrière-plan](#)

Le fonctionnement en arrière-plan permet à l'application de rester lancée même si elle n'est pas active. Cela est nécessaire pour une protection antivirus permanente de l'appareil et pour un fonctionnement correct des composants supplémentaires : [Filtre des appels et des SMS](#), [Filtre URL](#), [Antivol](#), [Contrôle parental](#) et [Pare-feu](#).

- [Désactivez l'optimisation de batterie](#)



Si Dr.Web est l'administrateur de l'appareil, ce paramètre d'optimisation n'est pas disponible.

Pour optimiser l'utilisation de la batterie, le système d'exploitation peut arrêter l'application Dr.Web. Cela suspendra la protection antivirus permanente de l'appareil et le fonctionnement des composants supplémentaires activés : [Filtre des appels et des SMS](#), [Filtre URL](#), [Antivol](#), [Contrôle parental](#) et [Pare-feu](#).

- [Autorisez le fonctionnement avec écran éteint](#)

Le fonctionnement avec écran éteint est nécessaire pour une protection antivirus permanente de l'appareil et pour le fonctionnement des composants supplémentaires : [Filtre des appels et des SMS](#), [Antivol](#) et [Pare-feu](#).

- [Autorisez les fenêtres pop-up](#) si l'[Antivol](#) ou le [Contrôle Parental](#) est activé



En arrière-plan, l'[Antivol](#) et le [Contrôle parental](#) utilisent les fenêtres pop-up pour limiter l'accès à une application ou à l'appareil entier.



Les paramètres peuvent différer selon les modèles d'appareil et les systèmes d'exploitation. Si ces instructions ne résolvent pas le problème, contactez le [support technique](#).

Pour autoriser le fonctionnement en arrière-plan

1. Ouvrez les applications récentes.
2. Appuyez sur l'icône de cadenas à côté de l'application Dr.Web.

Pour désactiver l'optimisation de la batterie

1. Ouvrez **Paramètres avancés** > **Gestionnaire de batterie** > **Application protégées** dans les paramètres de l'appareil.
2. Sélectionnez **Protégé** pour l'application Dr.Web.

Pour autoriser le fonctionnement avec écran éteint

1. Dans les paramètres de l'appareil, sélectionnez **Applications** > **Dr.Web** > **Batterie**.
2. Activez l'option **Fonctionnement avec écran éteint**.

Pour autoriser les fenêtres pop-up

1. Dans les paramètres de l'appareil, sélectionnez **Applications**.
2. Sélectionnez Dr.Web dans la liste d'applications.
3. Dans la liste d'autorisations, activez l'affichage de fenêtres pop-up en arrière-plan.

8.7.6.3. Meizu

Pour que l'application Dr.Web fonctionne correctement en arrière-plan sur les appareils Meizu, modifiez les paramètres suivants :

- [Désactivez l'optimisation de batterie](#)



Si Dr.Web est l'administrateur de l'appareil, ce paramètre d'optimisation n'est pas disponible.

Pour optimiser l'utilisation de la batterie, le système d'exploitation peut arrêter l'application Dr.Web. Cela suspendra la protection antivirus permanente de l'appareil et le fonctionnement des composants supplémentaires activés : [Filtre des appels et des SMS](#), [Filtre URL](#), [Antivol](#), [Contrôle parental](#) et [Pare-feu](#).

- [Verrouillez Dr.Web en arrière-plan](#)

Le fonctionnement en arrière-plan permet à l'application de rester lancée même si elle n'est



pas active. Cela est nécessaire pour une protection antivirus permanente de l'appareil et pour un fonctionnement correct des composants supplémentaires : [Filtre des appels et des SMS](#), [Filtre URL](#), [Antivol](#), [Contrôle parental](#) et [Pare-feu](#).

- [Autorisez le fonctionnement avec écran éteint](#)

Le fonctionnement avec écran éteint est nécessaire pour une protection antivirus permanente de l'appareil et pour le fonctionnement des composants supplémentaires : [Filtre des appels et des SMS](#), [Antivol](#) et [Pare-feu](#).



Les paramètres peuvent différer selon les modèles d'appareil et les systèmes d'exploitation. Si ces instructions ne résolvent pas le problème, contactez le [support technique](#).

Pour désactiver l'optimisation de la batterie

1. Ouvrez **Paramètres avancés** > **Gestionnaire de batterie** > **Application protégées** dans les paramètres de l'appareil.
2. Sélectionnez **Protégé** pour l'application Dr.Web.

Pour verrouiller Dr.Web en arrière-plan

1. Ouvrez les applications récentes.
2. Appuyez sur l'icône de cadenas à côté de l'application Dr.Web.

Pour autoriser le fonctionnement avec écran éteint

1. Dans les paramètres de l'appareil, sélectionnez **Applications** > **Dr.Web** > **Batterie**.
2. Activez l'option **Fonctionnement avec écran éteint**.

8.7.6.4. Nokia

Pour que l'application Dr.Web fonctionne correctement en arrière-plan sur les appareils Nokia, arrêtez l'application Power saver.



Si Dr.Web est l'administrateur de l'appareil, ce paramètre d'optimisation n'est pas disponible.

L'application Power saver optimise l'utilisation de la batterie, ce qui peut arrêter l'application Dr.Web. Cela suspendra la protection antivirus permanente de l'appareil et le fonctionnement des composants supplémentaires activés : [Filtre des appels et des SMS](#), [Filtre URL](#), [Antivol](#), [Contrôle parental](#) et [Pare-feu](#).



Les paramètres peuvent différer selon les modèles d'appareil et les systèmes d'exploitation. Si ces instructions ne résolvent pas le problème, contactez le [support technique](#).

Pour arrêter Power saver

1. Ouvrez **Applications** > **Toutes les applications** dans les paramètres de l'appareil.
2. Appuyez sur Menu en haut à droite de l'écran et sélectionnez **Afficher les applications système**.
3. Sélectionnez **Power saver** et appuyez **Arrêter**.

L'application sera arrêtée jusqu'au prochain redémarrage de l'appareil.

8.7.6.5. OnePlus

Pour que l'application Dr.Web fonctionne correctement en arrière-plan sur les appareils One Plus, modifiez les paramètres suivants :

- [Désactivez l'optimisation de batterie](#)



Si Dr.Web est l'administrateur de l'appareil, ce paramètre d'optimisation n'est pas disponible.

Pour optimiser l'utilisation de la batterie, le système d'exploitation peut arrêter l'application Dr.Web. Cela suspendra la protection antivirus permanente de l'appareil et le fonctionnement des composants supplémentaires activés : [Filtre des appels et des SMS](#), [Filtre URL](#), [Antivol](#), [Contrôle parental](#) et [Pare-feu](#).

- [Verrouillez Dr.Web en arrière-plan](#)

Le fonctionnement en arrière-plan permet à l'application de rester lancée même si elle n'est pas active. Cela est nécessaire pour une protection antivirus permanente de l'appareil et pour un fonctionnement correct des composants supplémentaires : [Filtre des appels et des SMS](#), [Filtre URL](#), [Antivol](#), [Contrôle parental](#) et [Pare-feu](#).

De plus, sur certains appareils il faut [désactiver l'optimisation profonde](#) et le [démarrage automatique](#).

Après l'installation des mises à jour du système d'exploitation, les paramètres d'optimisation peuvent être réinitialisés. Dans ce cas, il vous faudra les modifier encore une fois.



Les paramètres peuvent différer selon les modèles d'appareil et les systèmes d'exploitation. Si ces instructions ne résolvent pas le problème, contactez le [support technique](#).



Pour désactiver l'optimisation de la batterie

1. Ouvrez **Batterie** > **Optimisation de batterie** dans les paramètres de l'appareil.
2. Sélectionnez l'application Dr.Web.
3. Sélectionnez l'option **Ne pas optimiser** et appuyez sur **Terminer**.

Pour verrouiller Dr.Web en arrière-plan

1. Ouvrez les applications récentes.
2. Appuyez sur l'icône de cadenas à côté de l'application Dr.Web.

Pour désactiver l'optimisation profonde

1. Ouvrez **Batterie** > **Optimisation de batterie** dans les paramètres de l'appareil.
2. Appuyez sur l'icône de paramètres en haut à droite.
3. Désactivez l'optimisation profonde.

Pour désactiver le démarrage automatique

1. Dans les paramètres de l'appareil, ouvrez **Applications**.
2. Appuyez sur l'icône de paramètres en haut à droite.
3. Sélectionnez **Démarrage automatique**.
4. Désactivez le démarrage automatique de l'application Dr.Web.

8.7.6.6. Oppo

Pour que l'application Dr.Web fonctionne correctement en arrière-plan sur les appareils Oppo, modifiez les paramètres suivants :

- [Autorisez le démarrage automatique](#)

Le démarrage automatique permet de lancer les application une fois l'appareil allumé. Cela est nécessaire pour une protection antivirus permanente de l'appareil et pour un fonctionnement correct des composants supplémentaires : [Filtre des appels et des SMS](#), [Filtre URL](#), [Antivol](#), [Contrôle parental](#) et [Pare-feu](#).

- [Verrouillez Dr.Web en arrière-plan](#)

Le fonctionnement en arrière-plan permet à l'application de rester lancée même si elle n'est pas active. Cela est nécessaire pour une protection antivirus permanente de l'appareil et pour un fonctionnement correct des composants supplémentaires : [Filtre des appels et des SMS](#), [Filtre URL](#), [Antivol](#), [Contrôle parental](#) et [Pare-feu](#).

- [Autorisez le fonctionnement en arrière-plan](#) si l'application Centre de sécurité est installée sur votre appareil



Les paramètres peuvent différer selon les modèles d'appareil et les systèmes d'exploitation. Si ces instructions ne résolvent pas le problème, contactez le [support technique](#).

Pour autoriser le démarrage automatique

1. Dans les paramètres de l'appareil, ouvrez **Gestion des applications**.
2. Sélectionnez l'application Dr.Web.
3. Autorisez le démarrage automatique.

Pour verrouiller Dr.Web en arrière-plan

1. Ouvrez les applications récentes.
2. Définissez l'icône de cadenas pour l'application Dr.Web.

Pour autoriser le fonctionnement en arrière-plan

1. Ouvrez **Centre de sécurité**.
2. Sélectionnez **Autorisations de confidentialité** > **Gestion du démarrage automatique**.
3. Autorisez Dr.Web à fonctionner en arrière-plan.

8.7.6.7. Samsung

Pour que l'application Dr.Web fonctionne correctement en arrière-plan sur les appareils Samsung, modifiez les paramètres suivants :

- [Verrouillez Dr.Web en arrière-plan](#)

Le fonctionnement en arrière-plan permet à l'application de rester lancée même si elle n'est pas active. Cela est nécessaire pour une protection antivirus permanente de l'appareil et pour un fonctionnement correct des composants supplémentaires : [Filtre des appels et des SMS](#), [Filtre URL](#), [Antivol](#), [Contrôle parental](#) et [Pare-feu](#).



Les paramètres peuvent différer selon les modèles d'appareil et les systèmes d'exploitation. Si ces instructions ne résolvent pas le problème, contactez le [support technique](#).

Pour verrouiller Dr.Web en arrière-plan

1. Ouvrez les applications récentes.
2. Cliquez sur l'icône Dr.Web. Dans le menu déroulant, sélectionnez **Laisser ouverte** ou **Épingler cette application**.

L'icône de cadenas s'affiche pour l'application verrouillée.



8.7.6.8. Sony

Pour que l'application Dr.Web fonctionne correctement en arrière-plan sur les appareils Sony, désactivez l'optimisation de batterie pour Dr.Web.



Si Dr.Web est l'administrateur de l'appareil, ce paramètre d'optimisation n'est pas disponible.

Pour optimiser l'utilisation de la batterie, le système d'exploitation peut arrêter l'application Dr.Web. Cela suspendra la protection antivirus permanente de l'appareil et les composants supplémentaires activés : [Filtre des appels et des SMS](#), [Filtre URL](#), [Antivol](#), [Contrôle parental](#) et [Pare-feu](#).



Les paramètres peuvent différer selon les modèles d'appareil et les systèmes d'exploitation. Si ces instructions ne résolvent pas le problème, contactez le [support technique](#).

Pour désactiver l'optimisation de la batterie

1. Appuyez sur  sur l'écran d'accueil de l'appareil.
2. Sélectionnez **Paramètres** > **Batterie**.
3. Appuyez sur  et sélectionnez **Optimisation de batterie**.
4. Appuyez sur **Applications**. La liste des applications qui économisent la batterie va s'afficher.
5. Cochez la case contre Dr.Web. L'application s'affichera dans l'onglet **Non optimisé**.



Il est impossible d'exclure des applications de l'optimisation en mode Ultra STAMINA.

8.7.6.9. Xiaomi

Pour que l'application Dr.Web fonctionne correctement en arrière-plan sur les appareils Xiaomi, modifiez les paramètres suivants :

- [Autorisez le démarrage automatique](#)

Le démarrage automatique permet de lancer les application une fois l'appareil allumé. Cela est nécessaire pour une protection antivirus permanente de l'appareil et pour un fonctionnement correct des composants supplémentaires : [Filtre des appels et des SMS](#), [Filtre URL](#), [Antivol](#), [Contrôle parental](#) et [Pare-feu](#).

- [Autorisez le fonctionnement en arrière-plan](#)

Le fonctionnement en arrière-plan permet à l'application de rester lancée même si elle n'est pas active. Cela est nécessaire pour une protection antivirus permanente de l'appareil et pour



un fonctionnement correct des composants supplémentaires : [Filtre des appels et des SMS](#), [Filtre URL](#), [Antivol](#), [Contrôle parental](#) et [Pare-feu](#).

- [Verrouillez Dr.Web en arrière-plan](#)

Le fonctionnement en arrière-plan permet à l'application de rester lancée même si elle n'est pas active. Cela est nécessaire pour une protection antivirus permanente de l'appareil et pour un fonctionnement correct des composants supplémentaires : [Filtre des appels et des SMS](#), [Filtre URL](#), [Antivol](#), [Contrôle parental](#) et [Pare-feu](#).

- [Autorisez les fenêtres pop-up](#) si l'[Antivol](#) ou le [Contrôle Parental](#) est activé

En arrière-plan, l'[Antivol](#) et le [Contrôle parental](#) utilisent les fenêtres pop-up pour limiter l'accès à une application ou à l'appareil entier.



Les paramètres peuvent différer selon les modèles d'appareil et les systèmes d'exploitation. Si ces instructions ne résolvent pas le problème, contactez le [support technique](#).

Pour autoriser le démarrage automatique

1. Dans les paramètres de l'appareil, sélectionnez **Applications**.
2. Sélectionnez Dr.Web dans la liste d'applications.
3. Autorisez le démarrage automatique.

Pour autoriser le fonctionnement en arrière-plan

1. Dans les paramètres de l'appareil, sélectionnez **Applications**.
2. Sélectionnez Dr.Web dans la liste d'applications.
3. Sélectionnez le paramètre **Économiseur de batterie**.
4. Sélectionnez l'option **Pas de restriction**.

Pour verrouiller Dr.Web en arrière-plan

1. Ouvrez les applications récentes.
2. Appuyez sur l'icône de cadenas à côté de l'application Dr.Web.

Certaines versions du système d'exploitation permettent de verrouiller les applications en arrière-plan via l'application intégrée **Sécurité** :

1. Ouvrez la section **Augmenter la vitesse** dans l'application **Sécurité**.
2. Appuyez sur l'icône de paramètres  en haut à droite de l'écran.
3. Sélectionnez l'élément **Verrouiller les applications**.
4. Trouvez Dr.Web dans la liste d'applications.
5. Utilisez l'interrupteur à droite de Dr.Web pour verrouiller l'application en arrière-plan.



Pour autoriser les fenêtres pop-up

1. Dans les paramètres de l'appareil, sélectionnez **Applications**.
2. Sélectionnez Dr.Web dans la liste d'applications.
3. Sélectionnez **Autres autorisations**.
4. Dans la liste d'autorisations, activez l'affichage de fenêtres pop-up en arrière-plan.

8.8. Statistiques

Dr.Web enregistre les statistiques des menaces détectées et des actions effectuées par l'application.

Pour voir les statistiques de fonctionnement de l'application, appuyez sur **Menu**  sur l'écran d'accueil de Dr.Web et sélectionnez l'élément **Statistiques**.

Voir les statistiques

L'onglet **Statistiques** contient deux sections d'informations (voir [Figure 32](#)) :

- **Total**. Contient les informations sur le nombre total des fichiers scannés et sur le nombre des menaces détectées et neutralisées.
- **Événement** contient les informations sur les résultats de l'analyse effectuée par le Scanner Dr.Web, l'activation et la désactivation du composant SplDer Guard, le statut de la mise à jour de bases virales, les menaces détectées et les actions appliquées pour les neutraliser.

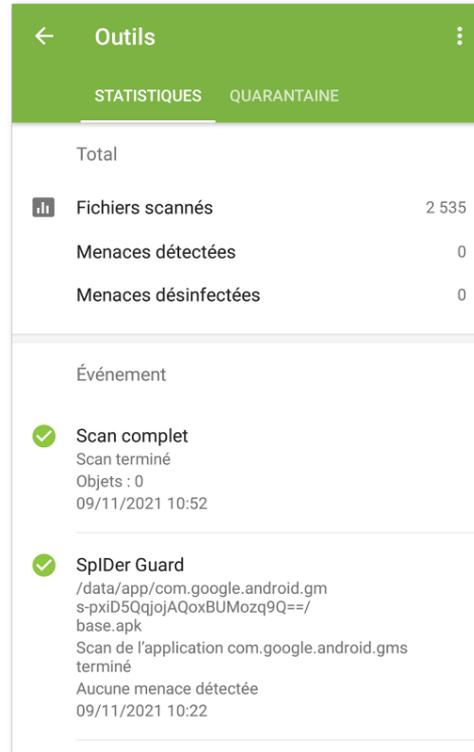


Figure 32. Statistiques

Pour effacer les statistiques

Pour effacer toutes les statistiques recueillies de l'application, appuyez sur **Menu**  dans l'onglet **Statistiques** et sélectionnez l'élément **Effacer les statistiques**.

Sauvegarder le journal des événements

Vous pouvez enregistrer le journal des événements de l'application et l'envoyer au support technique de Doctor Web si vous rencontrez des problèmes lors de l'utilisation de l'application.

1. Appuyez sur **Menu**  dans l'onglet **Statistiques** et sélectionnez **Sauvegarder le journal**.
2. Le journal est enregistré dans les fichiers `DrWeb_Log.txt` et `DrWeb_Err.txt` situés dans le dossier `Android/data/com.drweb/files` dans la mémoire interne de l'appareil.



Sur les appareils tournant sous Android 11.0 ou une version supérieure, les journaux sont enregistrés dans le dossier `Download/DrWeb`.

8.9. Quarantaine

Il existe une option permettant de déplacer les menaces détectées en quarantaine, dossier spécial destiné à isoler et à stocker les fichiers en toute sécurité (voir [Figure 33](#)).

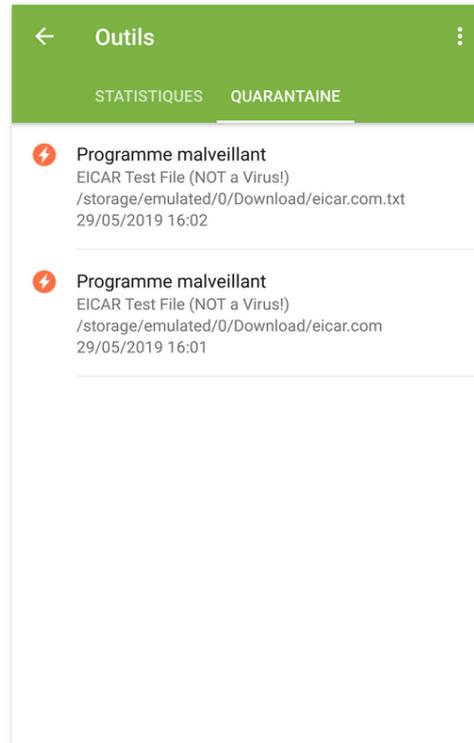


Figure 33. Quarantaine

Consulter la liste des objets en quarantaine

Pour consulter la liste des menaces placées en quarantaine :

1. Appuyez sur **Menu**  sur l'écran d'accueil de Dr.Web.



Sous Android TV, sélectionnez l'élément **Divers** sur l'écran d'accueil de Dr.Web.

2. Sélectionnez l'élément **Quarantaine**.

La liste des menaces placées en quarantaine s'ouvrira.

Consulter les informations sur les menaces

Pour consulter les informations sur une menace, appuyez sur son nom dans la liste.

Pour chaque menace, vous pouvez voir les informations suivantes :

- nom de fichier ;
- chemin d'accès au fichier ;
- heure et date de la mise en quarantaine.



Options disponibles

Les options suivantes sont disponibles pour chaque menace :

- **En savoir plus sur Internet** : pour voir la description de la menace sur le site de Doctor Web.
- **Restaurer** : pour remettre le fichier dans le dossier où il se trouvait avant le déplacement (utilisez cette option uniquement si vous êtes absolument sûr que le fichier n'est pas dangereux).
- **Supprimer** : pour supprimer le fichier de la Quarantaine et du système.
- **Faux positif** : pour envoyer le fichier au laboratoire antivirus pour l'analyse. L'analyse montrera si le fichier présente un danger ou bien, il s'agit d'un faux positif. Si c'est un faux positif, il sera corrigé. Pour obtenir les résultats de l'analyse, indiquez votre adresse e-mail.



L'option **Faux positif** est disponible uniquement pour les modifications des menaces.

Supprimer tous les objets de la quarantaine

Pour supprimer tous les objets placés en quarantaine :

1. Ouvrez la section **Quarantaine**.
2. Sur l'écran **Quarantaine**, appuyez sur **Menu**  et sélectionnez l'élément **Supprimer tout**.
3. Appuyez sur **OK**, pour confirmer l'action.
Appuyez sur **Annuler**, pour annuler la suppression et revenir dans la section **Quarantaine**.

Taille de la quarantaine

Vous pouvez consulter les informations sur la taille de la mémoire occupée par la Quarantaine et sur l'espace libre dans la mémoire interne de l'appareil :

1. Ouvrez la section **Quarantaine**.
2. Sur l'écran **Quarantaine**, appuyez sur **Menu**  et sélectionnez l'élément **Taille de la Quarantaine**.
3. Appuyez sur **OK**, pour revenir dans la section **Quarantaine**.



9. Paramètres

Pour accéder aux paramètres de l'application (voir [Figure 34](#)), appuyez sur **Menu**  sur l'écran d'accueil de Dr.Web et sélectionnez l'élément **Paramètres**.

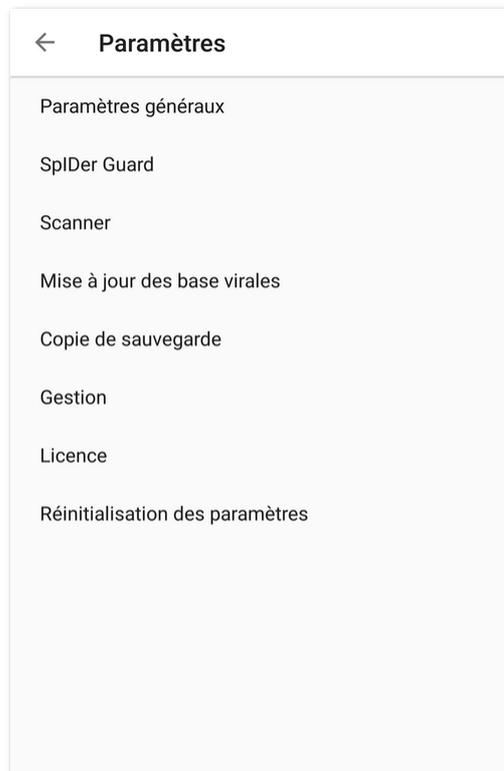


Figure 34. Paramètres

Si vous avez spécifié un mot de passe, il vous faudra entrer le mot de passe du compte pour accéder aux paramètres de l'application.

Sur l'écran **Paramètres**, les options suivantes sont disponibles :

- **Paramètres généraux.** Permet de configurer le panneau de notifications, activer et désactiver les notifications sonores, et modifier les paramètres d'envoi des statistiques (voir la section [Paramètres généraux](#)).
- **SplDer Guard.** Permet de spécifier les paramètres du composant SplDer Guard qui analyse constamment le système de fichiers pour la présence de menaces et surveille les modifications dans la zone système (voir la section [Paramètres de SplDer Guard](#)).
- **Scanner.** Permet de configurer le Scanner qui effectue l'analyse sur demande de l'utilisateur (voir la section [Paramètres du Scanner Dr.Web](#)).
- **Mise à jour des bases virales.** Permet d'interdire l'utilisation de l'Internet mobile pour la mise à jour des bases virales (voir la section [Mise à jour des base virales](#)).
- **Copie de sauvegarde.** Permet d'importer et d'exporter les paramètres de l'application (voir la section [Copie de sauvegarde](#)).



- **Gestion.** Permet de transférer l'application en [mode de protection centralisée](#) (l'option est disponible pour la version de l'application installée depuis le site de Doctor Web).
- **Licence.** Permet d'activer et de désactiver l'utilisation des notifications informant de la proche expiration de la licence (voir la section [Configuration des notifications de l'expiration de la licence](#)).
- **Réinitialisation des paramètres.** Permet de réinitialiser les paramètres par défaut (voir la section [Réinitialisation des paramètres](#)).



Si le composant [Antiviol Dr.Web](#) est activé sur l'appareil, le mot de passe du compte Dr.Web est requis pour modifier certains paramètres de l'application (**Réinitialisation des paramètres**, **Copie de sauvegarde** et **Gestion**).

9.1. Paramètres généraux

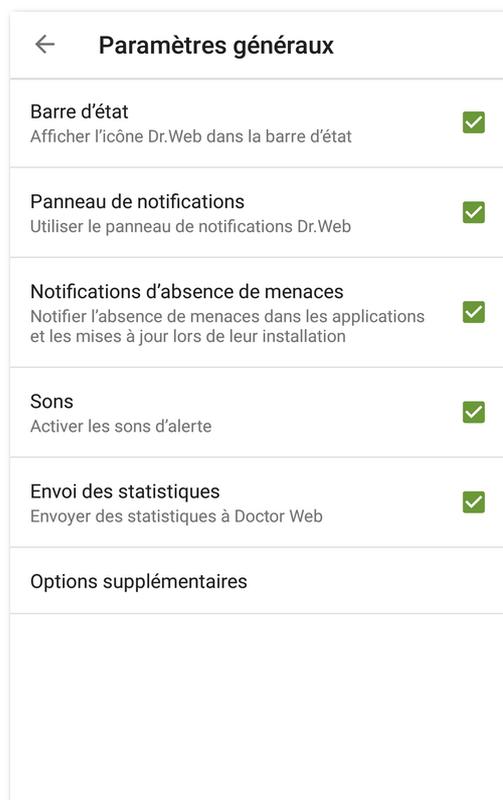


Figure 35. Paramètres généraux

Sur l'écran **Paramètres généraux** (voir [Figure 35](#)) les options suivantes sont disponibles :

- **Barre d'état** : permet de configurer l'affichage de l'icône de l'application dans la barre d'état. Cette option permet également de désactiver l'affichage du panneau Dr.Web dans la zone de notification (voir la rubrique [Panneau de notifications](#)).



Le paramètre n'est pas disponible sur les appareils tournant sous Android 8.0 ou une version supérieure.

- **Panneau de notifications** : permet de déterminer l'affichage du panneau Dr.Web dans la zone de notifications. Si l'option est activée, le panneau Dr.Web sera utilisé. Si l'option est désactivée, le panneau aura l'affichage classique du panneau de notifications Android.
- **Notifications d'absence de menaces** : permet d'activer et de désactiver les notifications indiquant qu'aucune menace n'est détectée dans les applications ou les mises à jour qui viennent d'être installées.



Le paramètre n'est pas disponible sur les appareils tournant sous Android 8.0 ou une version supérieure. Dans ce cas, vous pouvez désactiver les notifications de la catégorie **Applications sécurisées** dans les paramètres de l'appareil.

- **Sons** : permet de configurer les alertes sonores de détection, suppression et déplacement des menaces en Quarantaine. Les alertes sonores sont activées par défaut.
- **Envoi des statistiques** : permet d'activer et de désactiver l'envoi des statistiques à la société Doctor Web.
- **Options supplémentaires** contient les paramètres avancés :
 - **Applications systèmes** permet d'activer et de désactiver la notification des [menaces dans les applications système](#) qui ne peuvent pas être supprimées sans perte d'efficacité de l'appareil. L'option est désactivée par défaut.

9.2. Mise à jour des bases virales

Afin de détecter les menaces de sécurité, Dr.Web utilise les bases virales spéciales qui contiennent les informations sur toutes les menaces informatiques créées pour infecter les appareils tournant sous Android connues par les spécialistes de Doctor Web. Les bases nécessitent la mise à jour périodique, car de nouveaux logiciels malveillants apparaissent régulièrement. C'est pourquoi, l'application possède la fonctionnalité de mise à jour des bases virales via Internet.



La mise à jour manuelle de bases virales est bloquée en [mode de protection centralisée](#). Les mises à jour sont téléchargées automatiquement depuis le serveur de protection centralisée. Si le lancement de l'application en mode mobile est autorisé sur le serveur de protection centralisée, la mise à jour des bases virales peut être lancée manuellement en cas d'une connexion interrompue avec le serveur.

Mise à jour

Les bases virales sont mises à jour automatiquement par Internet quelque fois par jour. Si les bases virales ne sont pas mises à jour depuis plus de 24 heures (par exemple, en cas d'absence d'une connexion Internet), vous devez lancer la mise à jour manuellement.



Pour savoir si une mise à jour manuelle est requise

1. Appuyez sur **Menu**  sur l'écran d'accueil de Dr.Web et sélectionnez l'élément **Bases virales**.
2. Dans la fenêtre qui s'ouvre, vous verrez le statut des bases virales et la date de la dernière mise à jour. Si la dernière mise à jour a eu lieu plus de 24 heures auparavant, vous devez effectuer une mise à jour manuelle.

Pour lancer une mise à jour

1. Appuyez sur **Menu**  sur l'écran d'accueil de Dr.Web et sélectionnez l'élément **Bases virales**.
2. Dans la fenêtre qui s'affiche, appuyez sur **Mise à jour**.



Il est fortement recommandé d'effectuer la mise à jour des bases virales juste après l'installation de l'application pour que Dr.Web puisse utiliser les dernières informations sur les menaces connues. Dès que les experts du laboratoire antivirus de Doctor Web découvrent de nouvelles menaces, les signatures virales, les caractéristiques des virus et leurs modes d'actions sont mis à jour. Dans certains cas, les mises à jour peuvent être éditées plusieurs fois par heure.

Paramètres des mises à jour

Par défaut, les mises à jour sont téléchargées automatiquement quelques fois par jour.

Pour autoriser ou interdire l'utilisation du réseau mobile pour le téléchargement des mises à jour

1. Appuyez sur **Menu**  sur l'écran d'accueil Dr.Web et sélectionnez **Paramètres** (voir [Figure 34](#)).
2. Sélectionnez la section **Mise à jour des bases virales**.
3. Pour ne pas utiliser le réseau mobile pour le téléchargement des mises à jour, cochez la case **Mise à jour par Wi-Fi**.

Si des réseaux Wi-Fi actifs ne sont pas détectés, on vous proposera d'utiliser l'Internet mobile. La modification de ce paramètre n'influence pas l'utilisation du réseau mobile par d'autres fonctions de l'application et de l'appareil mobile.



Les mises à jour sont téléchargées sur Internet. Des frais supplémentaires de transmission de données peuvent s'appliquer. Pour plus de détails, contactez votre opérateur de téléphonie mobile.

En [mode de protection centralisée](#), certains paramètres de mises à jour peuvent être modifiés ou bloqués conformément à la politique de sécurité de votre entreprise ou à la liste des services payés.



9.3. Copie de sauvegarde

Vous pouvez exporter les paramètres actuels de l'application dans un fichier dans la mémoire interne de l'appareil. Vous pourrez les importer depuis ce fichier en cas de besoin, par exemple, si vous réinstallez Dr.Web ou l'installez sur un autre appareil.



L'importation et l'exportation des paramètres ne sont pas disponibles dans le [mode de protection centralisée](#).

Pour exporter les paramètres actuels dans un fichier

1. Sur l'écran de configuration (voir [Figure 34](#)), sélectionnez la section **Copie de sauvegarde**.
2. Entrez le mot de passe du compte.

Le mot de passe est requis au cas où le composant Antivol Dr.Web serait activé et configuré.

3. Dans la fenêtre qui s'ouvre, sélectionnez **Exportation des paramètres**.
4. Spécifiez le mot de passe pour protéger le fichier de paramètres et appuyez sur **OK**.

Tous les paramètres sont sauvegardés dans le fichier

Internal storage/Android/data/com.drweb/files/DrWebPro.bkp.



Sur les appareils tournant sous Android 11.0 ou une version supérieure, le fichier de configurations est enregistré dans le dossier `Download/DrWeb`.

Pour importer les paramètres depuis le fichier

1. Sur l'écran de configuration (voir [Figure 34](#)), sélectionnez la section **Copie de sauvegarde**.
2. Entrez le mot de passe du compte.

Le mot de passe est requis au cas où le composant Antivol Dr.Web serait activé et configuré.

3. Sélectionnez **Importation des paramètres**.
4. Confirmez l'importation des paramètres depuis le fichier.
5. Dans l'arborescence de fichiers, trouvez le fichier de paramètres et appuyez dessus.
6. Entrez le mot de passe spécifié pour le fichier de paramètres et appuyez sur **OK**.

Tous les paramètres actuels seront supprimés et remplacés par les paramètres importés du fichier.

9.4. Réinitialisation des paramètres

A tout moment, vous pouvez réinitialiser les paramètres de l'application, y compris les paramètres de filtrage des appels et des messages, de l'Antivol Dr.Web, du Pare-feu Dr.Web et du filtre URL et restaurer les paramètres par défaut.



La réinitialisation des paramètres n'est pas disponible dans le [mode de protection centralisée](#).

Pour réinitialiser les paramètres

1. Sur l'écran de configuration (voir [Figure 34](#)) appuyez sur **Réinitialisation des paramètres** et sélectionnez l'élément **Réinitialisation des paramètres**.
2. Entrez le mot de passe du compte Dr.Web.
3. Confirmez la réinitialisation des paramètres par défaut.



10. Mode de protection centralisée

Les ordinateurs et d'autres appareils sur lesquels les composants interagissants de Dr.Web sont installés forment un *réseau antivirus*. Le réseau antivirus fonctionne sur une architecture client-serveur. Le serveur gère le client à l'aide de l'Agent Dr.Web. Le mode de protection centralisée est un mode de fonctionnement de l'application géré par l'Agent Dr.Web.

La version Dr.Web Security Space pour les appareils mobiles décrite dans ce manuel est compatible avec Dr.Web AV-Desk en version 10 et 13 et Dr.Web Enterprise Security Suite en version 10, 11, 12 et 13.

Le mode de protection centralisée est disponible pour les versions suivantes de Dr.Web :

- Les versions téléchargées sur le site de la société Doctor Web <https://download.drweb.com/android/>.
- Les versions téléchargées dans votre espace privé du fournisseur du service Antivirus Dr.Web.
- Les versions reçues de l'administrateur du réseau antivirus de votre entreprise.

Le mode de protection centralisée n'est pas disponible :

- Pour les versions Dr.Web installées depuis Google Play.
- Pour la version installée depuis HUAWEI AppGallery.
- Pour les appareils tournant sous Android TV.

Composants contrôlés par le serveur de protection centralisée

Les paramètres des composants de Dr.Web peuvent être modifiés ou bloqués conformément à la politique de sécurité de votre entreprise ou à la liste des services payés.

Les composants suivants peuvent être contrôlés depuis le serveur de protection centralisée :

- [Scanner Dr.Web](#). Scan de l'appareil sur demande de l'utilisateur et selon la planification. Le lancement du scan distant depuis le serveur de protection centralisée est également supporté.
- [SpIDer Guard](#).
- [Filtre des appels et des SMS](#).
- [Antivol Dr.Web](#).
- [Filtre URL](#).
- [Filtre d'applications](#).

Octroi de la licence en mode de protection centralisée

En mode de protection centralisée, le [fichier clé de licence](#) est téléchargé automatiquement depuis le serveur de protection centralisée et votre licence personnelle n'est pas utilisée. En cas



d'expiration de la licence ou de son blocage une notification correspondante sera affichée. Contactez l'administrateur du réseau antivirus de votre entreprise pour obtenir une nouvelle licence ou renouvelez l'abonnement au service Antivirus Dr.Web.

Mise à jour des bases virales en mode de protection centralisée

La mise à jour manuelle de bases virales est bloquée en mode de protection centralisée. Les mises à jour sont téléchargées automatiquement depuis le serveur de protection centralisée. Les paramètres des mises à jour peuvent être modifiés ou bloqués conformément à la politique de sécurité de votre entreprise ou à la liste des services payés. Si le lancement de l'application en mode mobile est autorisé sur le serveur de protection centralisée, la mise à jour des bases virales peut être lancée manuellement en cas d'une connexion interrompue avec le serveur.

Mise à jour de l'application en mode de protection centralisée

Certaines version du serveur de protection centralisée supportent la mise à jour de Dr.Web Security Space pour les appareils mobiles. Si la case **Nouvelle version** est cochée dans les paramètres de l'application, vous recevrez des notifications de disponibilité de la nouvelle version de l'application et vous pourrez l'installer rapidement. Pour en savoir plus, contactez l'administrateur du réseau antivirus de votre entreprise.

La mise à jour depuis le serveur de protection centralisée n'est pas disponible pour les versions d'application téléchargées sur le site de la société Doctor Web. Seules les bases virales de ces versions peuvent être mises à jour en mode de protection centralisée.

10.1. Passage en mode de protection centralisée

Pour mettre l'application en mode de protection centralisée, [connectez-vous](#) au serveur de protection centralisée.



Pour la connexion au serveur de protection centralisée 11.0.0 ou à une version supérieure, Dr.Web 11.0.0 (ou une version supérieure) est requis.

Après la connexion au serveur, les autorisations suivantes peuvent être requises :

- Autorisations principales (l'accès aux photos, médias, fichiers, contacts, etc) : pour le fonctionnement de la plupart des fonctions de l'application.
- Filtre des appels et des SMS (utilisation de Dr.Web comme application d'appels par défaut) : pour le filtrage des appels et des SMS entrants.
- Administration de l'appareil : pour la protection de l'application contre la suppression et le fonctionnement complet de l'Antivol.
- Accès aux fonctionnalités spéciales : pour le filtrage des applications et le fonctionnement complet du Filtre URL, de l'Antivol et du Contrôle parental.



- Superposition au-dessus des autres fenêtres : pour le filtrage des applications et le fonctionnement du Pare-feu.

Connexion au serveur de protection centralisée

Connexion automatique

Les versions de Dr.Web reçues de l'administrateur du réseau antivirus de votre entreprise ou du fournisseur du service Antivirus Dr.Web se connectent automatiquement au serveur de protection centralisée. Pour cela, le paquet d'installation doit être lancé depuis la mémoire interne de l'appareil.

Connexion avec l'entrée de paramètres

Pour se connecter au serveur de protection centralisée les paramètres de connexion fournis par l'administrateur du réseau antivirus de votre entreprise ou par le fournisseur du service Antivirus Dr.Web, sont requis.

1. Assurez-vous que la connexion au réseau est établie.
2. Sur l'écran **Paramètres** (voir [Figure 34](#)), sélectionnez **Gestion**.
Si l'Antivol Dr.Web est activé sur l'appareil, entrez le mot de passe du compte Dr.Web.
3. Cochez la case **Agent Dr.Web**.



La case **Agent Dr.Web** est cochée par défaut dans les versions de Dr.Web reçues de l'administrateur du réseau antivirus de votre entreprise ou du fournisseur du service Antivirus Dr.Web.

4. Lorsque le mode de protection centralisée est activé, les précédents paramètres de la connexion sont restaurés.

Pourtant si le [fichier de configuration](#) est sauvegardé sur votre appareil, ce sont les paramètres de connexion de ce fichier qui sont utilisés. Pour utiliser d'autres paramètres de connexions, par exemple, ceux du package d'installation, [réinitialisez les paramètres de connexion](#).

Si c'est votre première connexion ou que les paramètres de la connexion ont été modifiés, spécifiez les paramètres suivants :

- Adresse IP du serveur de protection centralisée.
 - Paramètres supplémentaires d'authentification du poste de travail : l'ID de poste (identificateur associé à votre ordinateur pour l'authentifier sur le serveur) et le mot de passe. Cette configuration est sauvegardée, lors de la connexion suivante vous n'aurez pas besoin de ressaisir ces paramètres. Pour vous connecter en tant que nouvelle station (novice), appuyez sur **Menu**  et sélectionnez l'option **Se connecter en tant que novice**.
5. Appuyez sur **Se connecter**.



Connexion avec un fichier de configuration

Les paramètres de connexion au serveur de protection centralisée se trouvent dans le fichier `install.cfg` fourni par l'administrateur du réseau antivirus de l'entreprise ou par le fournisseur du service Antivirus Dr.Web.

1. Assurez-vous que la connexion au réseau est établie.
2. Placez le fichier `install.cfg` dans le dossier racine ou dans un des dossiers de premier niveau dans la mémoire interne de l'appareil.
3. Sur l'écran de configuration (voir [Figure 34](#)), sélectionnez **Gestion**.

Si l'Antivol Dr.Web est activé, vous devez entrer le mot de passe du compte Dr.Web en ouvrant la section **Gestion**.

4. Cochez la case **Agent Dr.Web**.

Lorsque le fichier est copié sur l'appareil mobile, les paramètres de connexion au serveur sont entrés automatiquement.



La case **Agent Dr.Web** est cochée par défaut dans les versions de Dr.Web reçues de l'administrateur du réseau antivirus de l'entreprise ou du fournisseur du service Antivirus Dr.Web. L'application commence à chercher le fichier de configuration et essaie de se connecter au serveur aussitôt après l'installation. Si le fichier n'est pas trouvé ou qu'il contient des paramètres de connexion incorrects, il est nécessaire de décocher et cocher de nouveau la case **Agent Dr.Web** et entrer les paramètres [manuellement](#) ou d'utiliser un fichier de configuration avec les paramètres corrects.

5. Appuyez sur **Se connecter**.

Réinitialisation des paramètres de la connexion

1. Appuyez sur **Menu**  sur l'écran d'entrée des paramètres de la connexion.
2. Sélectionnez l'option **Réinitialiser les paramètres de la connexion**.

Après la réinitialisation des paramètres, le fichier `install.cfg`, contenant les paramètres de connexion utilisés, sera supprimé. Si l'appareil contient un autre fichier `install.cfg`, les paramètres de connexion de ce fichier seront utilisés. Ainsi, les paramètres de connexion seront réinitialisés seulement après la suppression de tous les fichiers `install.cfg`.

Erreurs de connexion

Option non supportée. Une erreur survient, si les options de chiffrement et/ou compression du trafic, non supportées par Dr.Web, sont activées. Pour résoudre ce problème, adressez-vous à l'administrateur du réseau antivirus ou au fournisseur du service Antivirus Dr.Web.

La licence (la souscription) a expiré. Contactez l'administrateur du réseau antivirus pour obtenir la licence ou renouvelez l'abonnement au service Antivirus Dr.Web.



La souscription est bloquée. Contactez le fournisseur du service Antivirus Dr.Web pour débloquer l'abonnement.

Le lancement de Dr.Web pour Android est interdit sur le serveur. Une erreur survient si votre tarif ne prévoit pas l'utilisation de Dr.Web pour Android ou que le lancement de Dr.Web pour Android est interdit par l'administrateur du réseau antivirus.

10.2. Gestion

Si l'option permettant de modifier la configuration du Filtre d'applications est activée sur le serveur de protection centralisée, vous pouvez sélectionner les applications qui peuvent être lancées sur votre appareil.

Vous pouvez autoriser/bloquer le lancement d'applications système et d'applications d'utilisateur. Les applications système se trouvent en haut de la liste et sont marquées comme autorisées par défaut. Les applications d'utilisateur se trouvent plus bas dans la liste.

Pour configurer le Filtre d'applications

1. Sur l'écran d'accueil de Dr.Web, ouvrez la section **Gestion**.
2. Sélectionnez les applications qui seront disponibles pour l'appareil.
3. Appuyez sur le bouton **Autoriser les sélectionnées**. Les paramètres spécifiés seront transmis sur le serveur en tant que paramètres personnalisés de votre appareil.



Les paramètres de lancement d'applications configurés sur un appareil utilisateur seront appliqués uniquement si le Filtre d'applications est activé sur le serveur de protection centralisée pour cet appareil.

Si vous êtes administrateur du réseau antivirus, vous pouvez configurer sur le serveur de protection centralisée les listes des applications disponibles pour tous les appareils de réseau basées sur vos paramètres personnalisés, enregistrés sur le serveur.

10.3. Passage en mode standalone

Pour transférer Dr.Web en mode standalone, ouvrez l'écran de configuration (voir [Figure 34](#)) et sélectionnez l'élément **Gestion**. Après cela, décochez la case **Agent Dr.Web**.

Lorsque le mode standalone est activé, tous les paramètres de l'antivirus sont restaurés à leur configuration précédente ou par défaut. L'accès aux fonctionnalités de Dr.Web est également restauré.

Pour le fonctionnement en mode autonome, une [licence](#) personnelle valide est requise. Dans ce mode, il est impossible d'utiliser la licence obtenue automatiquement depuis le serveur de



protection centralisée. Si nécessaire, vous pouvez [acheter](#) ou [renouveler](#) votre licence personnelle.

11. Dr.Web sous Android TV

Sur l'écran d'accueil de Dr.Web (voir [Figure 36](#)), les options suivantes sont disponibles :

- [Événement](#)
- [Scanner](#)
- [Pare-feu](#)
- [Contrôleur de sécurité](#)
- [Divers](#)

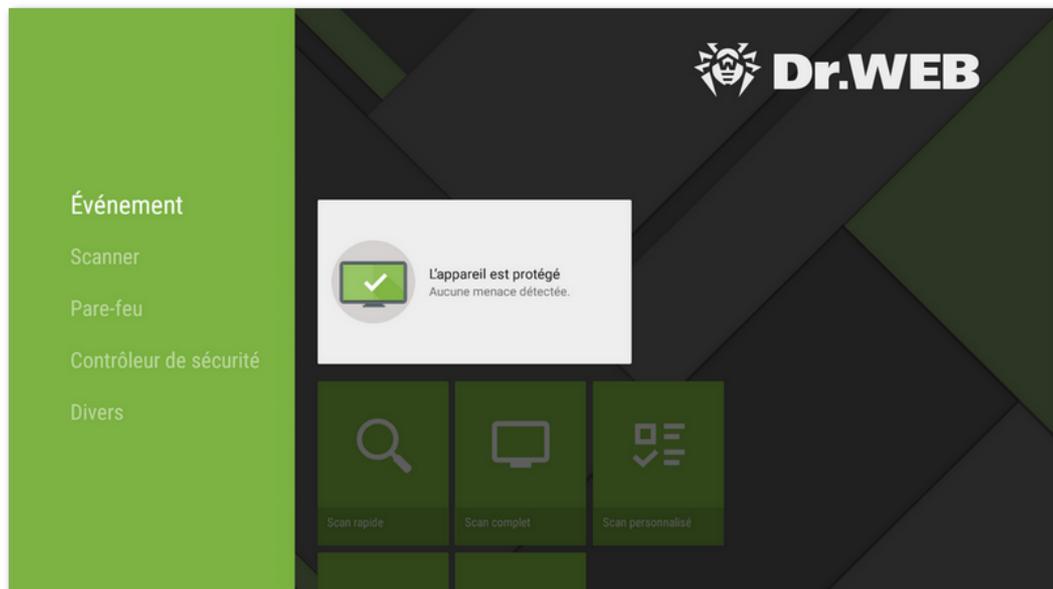


Figure 36. Dr.Web sous Android TV

Particularités de fonctionnement de Dr.Web sous Android TV



Sur les appareils tournant sous Android TV, le mode de protection centralisée n'est pas disponible.

Autorisations

Au premier lancement, l'application vous demande d'accorder les [autorisations](#) suivantes :

- L'accès aux photos, médias et fichiers sur l'appareil.
- L'accès aux contacts.

Autorisez l'application à accéder aux fonctions et aux données nécessaires.



Sur les appareils tournant sous Android 11.0 ou une version supérieure, l'application demande également l'autorisation d'accéder à tous les fichiers.

Pour accorder l'accès à tous les fichiers

1. Dans la fenêtre de demande d'autorisation, appuyez sur le bouton **Aller aux Paramètres**.
2. Sur l'écran de paramètres système de Dr.Web, sélectionnez l'élément **Autorisations**.
3. Sélectionnez l'élément **Fichiers et contenus multimédias**.
4. Sélectionnez l'option **Toujours autoriser**.
5. Dans la boîte de dialogue, appuyez sur le bouton **Autoriser**.

Interface

- Impossible de créer un [widget](#) pour le bureau.
- Le [panneau de notifications](#) n'est pas disponible.

11.1. Événements sous Android TV

La barre **Événement** affiche l'état actuel de la protection de l'appareil.

- L'indicateur vert signifie que l'appareil est protégé. Aucune intervention n'est requise.
- L'indicateur jaune signifie que Dr.Web a détecté des problèmes de sécurité, par exemple, l'absence de la licence ou une vulnérabilité. Pour en savoir plus sur les problèmes détectés et les résoudre, sélectionnez la barre d'état.
- L'indicateur rouge signifie que Dr.Web a détecté des modifications suspectes dans la zone système ou des menaces. Pour ouvrir les résultats de l'analyse et neutraliser les menaces, sélectionnez la barre d'état.

Si Dr.Web a détecté plusieurs événements nécessitant l'attention de l'utilisateur, sélectionnez la barre d'état. La fenêtre **Événement** va s'ouvrir. Tous les messages importants seront affichés dans cette fenêtre.

11.2. Protection antivirus sous Android TV

- [SpIDer Guard](#) analyse le système de fichiers en temps réel.
- Le [Scanner Dr.Web](#) permet de lancer l'analyse manuellement.
- Sur l'écran [Résultats du scan](#), vous pouvez sélectionner des actions pour neutraliser les menaces détectées.



11.2.1. Protection permanente SpIDer Guard sous Android TV

Pour activer la protection constante

Quand vous ouvrez Dr.Web pour la première fois, la protection constante est activée automatiquement une fois le Contrat de Licence accepté. SpIDer Guard fonctionne indépendamment du fait que l'application est lancée ou non. Si SpIDer Guard détecte une modification suspecte dans la zone système ou une menace, un message correspondant s'affichera en bas de l'écran.

Configuration

Pour activer, désactiver ou configurer la protection permanente, sélectionnez **Divers** > **Paramètres** > **SpIDer Guard** sur l'écran d'accueil de Dr.Web (voir la rubrique [Paramètres de Dr.Web sous Android TV](#)).

Statistiques

L'application enregistre les événements liés au fonctionnement de SpIDer Guard : activation/désactivation, détection des menaces de sécurité et résultats du scan de la mémoire de l'appareil et des applications installées. Les statistiques de SpIDer Guard sont affichées dans la section **Événement** de l'onglet **Statistiques**. Les statistiques sont triées par date (voir la rubrique [Statistiques](#)).

11.2.2. Scanner Dr.Web sous Android TV

Le composant Scanner Dr.Web effectue le scan du système sur demande de l'utilisateur. Il permet d'effectuer un scan rapide ou complet du système de fichiers, ainsi que de scanner des dossiers et des fichiers particuliers.

Il est fortement recommandé de scanner périodiquement le système, notamment si le composant SpIDer Guard n'a pas été actif pendant quelque temps. D'habitude, il suffit d'effectuer un scan rapide.

Analyse

Pour analyser le système, sélectionnez l'option **Scanner** sur l'écran d'accueil de Dr.Web (voir [Figure 37](#)) et effectuez l'une des actions suivantes :

- Pour scanner seulement les applications installées, sélectionnez l'élément **Scan rapide**.
- Pour scanner tous les fichiers dans le système, sélectionnez l'élément **Scan complet**.
- Pour analyser certains dossiers et fichiers, sélectionnez l'élément **Scan personnalisé**, puis sélectionnez les objets à scanner dans la fenêtre qui s'affiche.

Vous pouvez analyser le dossier entier. Pour cela, sélectionnez l'option **Scanner le dossier**.
Pour passer au niveau supérieur, sélectionnez l'option **Haut de page**.

Si votre appareil est rooté, vous pouvez sélectionner pour l'analyse les dossiers `/sbin` et `/data` situés dans le dossier racine.

Lorsque le scan est terminé, les informations suivantes s'affichent sur l'écran :

- Nombre d'objets analysés.
- Nombre de menaces détectées.
- Heure de lancement de scan.
- Durée de scan.

Pour ouvrir les résultats du scan, sélectionnez **OK**.

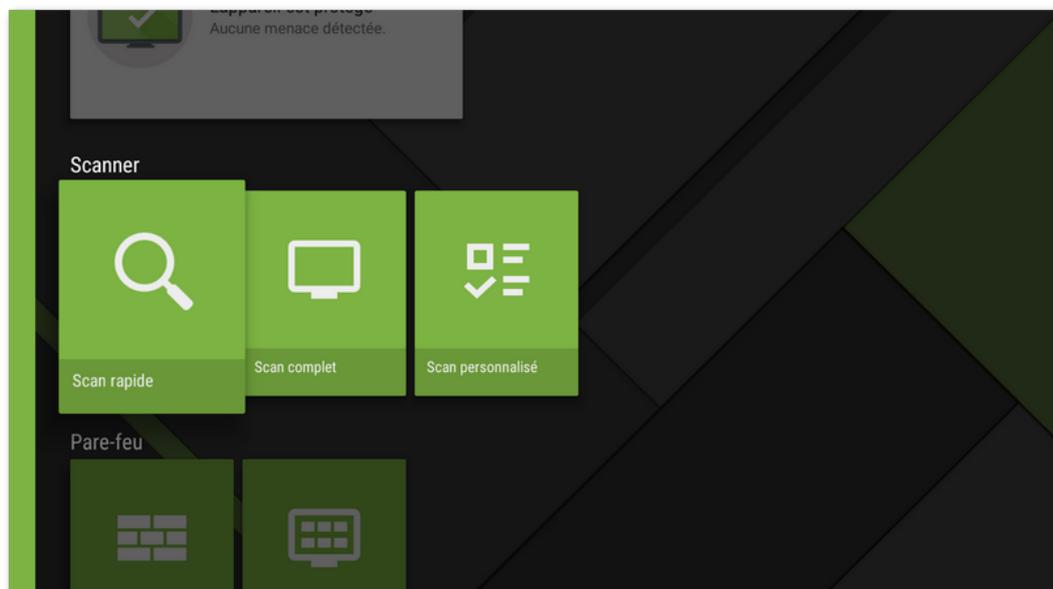


Figure 37. Scanner Dr.Web

Paramètres du Scanner Dr.Web

Pour accéder aux paramètres du Scanner Dr.Web, sélectionnez **Divers > Paramètres > Scanner** sur l'écran d'accueil de Dr.Web (voir la rubrique [Paramètres de Dr.Web sous Android TV](#)).

Statistiques

L'application enregistre les événements liés au fonctionnement du Scanner Dr.Web (le mode et les résultats du scan, la détection des menaces de sécurité). Les actions de l'application sont affichées dans la section **Événement** de l'onglet **Statistiques**. Les actions sont triées par date (voir la rubrique [Statistiques](#)).



11.2.3. Résultats du scan sous Android TV

Comment ouvrir les résultats du scan

Si le composant [SpIDer Guard](#) détecte une modification suspecte dans la zone système ou une menace, une alerte s'affichera en bas de l'écran. Pour ouvrir les résultats du scan, sélectionnez l'option **Événement** sur l'écran d'accueil de Dr.Web.

Pour ouvrir les résultats du scan du [Scanner Dr.Web](#), sélectionnez **OK** après la fin de l'analyse.

Neutralisation des menaces

Sur l'écran **Résultats du scan**, vous pouvez consulter la liste de menaces ou de modifications suspectes dans la zone système. Le type et le nom sont indiqués pour chaque objet, ainsi que l'icône de l'option recommandée pour cet objet.

Les objets sont marquées de couleurs différentes en fonction du niveau de danger. Types d'objets classés dans l'ordre décroissant de danger :

1. Programme malveillant.
2. Riskware.
3. Hacktool.
4. Adware.
5. [Modifications dans la zone système](#) :
 - Nouveaux fichiers dans la zone système.
 - Modification de fichiers système.
 - Suppression de fichiers système.
6. Canular.

Pour voir le chemin d'accès au fichier, sélectionnez l'objet correspondant. Le nom de package de l'application est également indiqué pour les menaces détectées dans les applications.

Neutralisation de toutes les menaces

Pour supprimer toutes les menaces en même temps

- Sélectionnez **Menu**  > **Supprimer tout** en haut à droite de l'écran **Résultats du scan**.

Pour déplacer toutes les menaces en quarantaine en même temps

- Sélectionnez **Menu**  > **Mettre tout en quarantaine** en haut à droite de l'écran **Résultats du scan**.



Neutralisation de menaces une par une

Un ensemble d'options est disponible pour chaque objet. Pour ouvrir une liste d'options, sélectionnez un objet. Les options recommandées sont les premières dans la liste. Sélectionnez l'une des options suivantes :

 **Désinfecter** : pour désinfecter une application infectée.

L'option est disponible pour certaines [menaces se trouvant dans les applications système](#), si l'accès root est autorisé.

 **Supprimer** : pour supprimer définitivement la menace de l'appareil.

Dans certains cas, Dr.Web ne peut pas supprimer les applications qui utilisent les fonctionnalités spéciales d'Android. Si vous sélectionnez l'option **Supprimer**, mais Dr.Web ne supprime pas l'application, passez en mode sécurisé et supprimez l'application manuellement. Si Dr.Web a l'accès aux fonctionnalités spéciales, la suppression se fera automatiquement une fois l'option **Supprimer** sélectionnée.

L'option n'est pas disponible pour les [menaces se trouvant dans les applications système](#) dans les cas suivants :

- Si l'accès root n'est pas autorisé sur l'appareil.
- Si la suppression de l'application peut provoquer la perte d'efficacité de l'appareil.
- Si une modification de menace est détectée. Pour déterminer si l'application présente une menace, signalez un faux positif.

 **Déplacer vers la Quarantaine** : pour déplacer une menace dans le dossier isolé (voir la rubrique [Quarantaine](#)).

Si la menace est détectée dans une application installée, il n'est pas possible de la placer en quarantaine. Dans ce cas, l'option **Déplacer vers la Quarantaine** n'est pas disponible.

 **Ignorer** : pour laisser intacte pour le moment la modification de la zone système ou la menace.

 **Bloquer**, pour bloquer l'accès de l'application aux connexions Internet.

L'option est disponible pour les [menaces se trouvant dans les applications système](#).

 **Envoyer au Laboratoire** ou **Faux positif** : pour envoyer le fichier pour l'analyse au laboratoire antivirus de Doctor Web. L'analyse montrera si le fichier présente un danger ou qu'il s'agit d'un faux positif. Si c'est un faux positif, il sera corrigé. Pour obtenir les résultats de l'analyse, indiquez l'adresse e-mail.

Si le fichier est envoyé avec succès au laboratoire, l'action **Ignorer** s'applique automatiquement à l'objet.

L'option **Envoyer au Laboratoire** est disponible uniquement pour les fichiers ajoutés ou les fichiers exécutables modifiés dans la zone système : `.jar`, `.odex`, `.so`, fichiers aux formats APK, ELF, etc.

L'option **Faux positif** est disponible uniquement pour les modifications des menaces et pour



les menaces détectées dans la zone système.

 **En savoir plus sur Internet** pour ouvrir la page contenant la description de l'objet détecté sur le site de Doctor Web.

11.3. Pare-feu Dr.Web sous Android TV

Le Pare-feu Dr.Web protège votre appareil contre l'accès non autorisé et prévient la fuite de données importantes via le réseau. Ce composant permet de contrôler les connexions Internet et les transferts de données et de bloquer les connexions suspectes.

Technologie

Le Pare-feu Dr.Web se base sur la technologie VPN pour Android, ce qui lui permet de fonctionner sans obtenir les droits du super-utilisateur (root) de l'appareil. La réalisation de la technologie VPN sur Android est liée aux limitations particulières :

- Premièrement, une seule application installée sur l'appareil peut utiliser le VPN. Quand l'application active le VPN sur l'appareil, une fenêtre demandant l'autorisation d'utiliser VPN pour cette application s'ouvre. Si l'utilisateur permet à l'application d'utiliser le VPN, elle commence à l'utiliser, mais une autre application qui avait utilisé le VPN auparavant, ne peut plus y accéder. Une demande pareille s'affiche au premier démarrage du Pare-feu Dr.Web et puis, à chaque redémarrage de l'appareil. On peut aussi la voir apparaître quand les autres applications demandent l'accès au VPN. Le VPN est partagé par les applications dans le temps, et le Pare-feu ne peut fonctionner que s'il possède les droits exclusifs d'utiliser le VPN.
- L'activation du Pare-feu Dr.Web peut provoquer l'impossibilité de connecter l'appareil sur lequel il est lancé aux autres appareils via Wi-Fi ou via le réseau local. Cela dépend du modèle de l'appareil et des applications utilisées pour la connexion.
- Si le Pare-feu Dr.Web est activé, l'appareil ne peut pas être utilisé comme un point d'accès Wi-Fi.



Le Pare-feu Dr.Web n'utilise la technologie VPN pour Android que pour exécuter ses fonctionnalités, il n'établit pas de tunnel VPN et le trafic n'est pas chiffré.

Pour activer le Pare-feu Dr.Web

1. Sur l'écran d'accueil de Dr.Web, sélectionnez l'option **Pare-feu** (voir [Figure 38](#)).
2. Effectuez l'une des actions suivantes :
 - Utilisez l'interrupteur se trouvant à droite de l'élément **Journal**.
 - Sélectionnez l'élément **Trafic** ou **Journal** et appuyez sur **Activer**.

Par défaut, le Pare-feu est désactivé. Dr.Web demande l'autorisation de se connecter au VPN. Il faut accorder cette autorisation pour un fonctionnement correct du Pare-feu.



Si les droits d'utiliser le VPN sont reçus par une autre application, le Pare-feu Dr.Web est désactivé et l'utilisateur est notifié par une alerte spéciale.

Si vous gérez l'appareil en mode d'accès limité (en mode d'invité), les paramètres du Pare-feu Dr.Web ne sont pas disponibles pour vous.

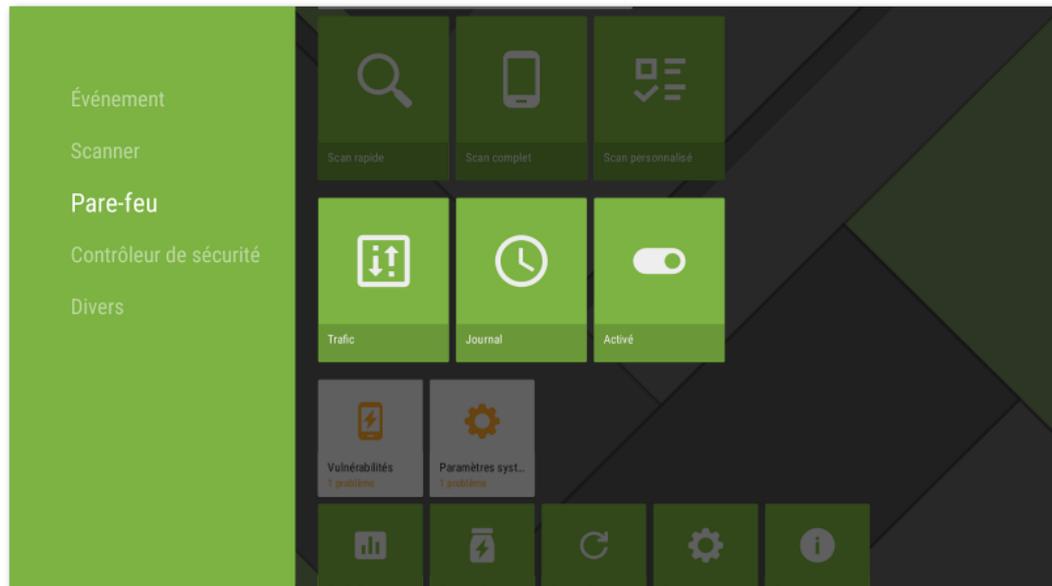


Figure 38. Pare-feu Dr.Web sous Android TV

11.3.1. Activité des connexions réseau sous Android TV

Vous pouvez consulter les informations sur l'activité des connexions réseau sur l'écran **Trafic**. L'écran comporte deux onglets : **Applications actives** et **Toutes les applications** (voir [Figure 39](#)).

Onglet Applications actives

Sur l'onglet, vous pouvez voir en temps réel la liste des connexions initiées par les applications installées sur l'appareil.

Les informations suivantes s'affichent pour chaque application sur l'onglet **Applications actives** :

- Volume total du trafic entrant et sortant par les connexions établies.
- [Accès à la transmission de données par Wi-Fi](#).
- Présence des paramètres utilisateur. Les applications dont l'accès à la transmission de données a été modifié sont marquées par l'icône

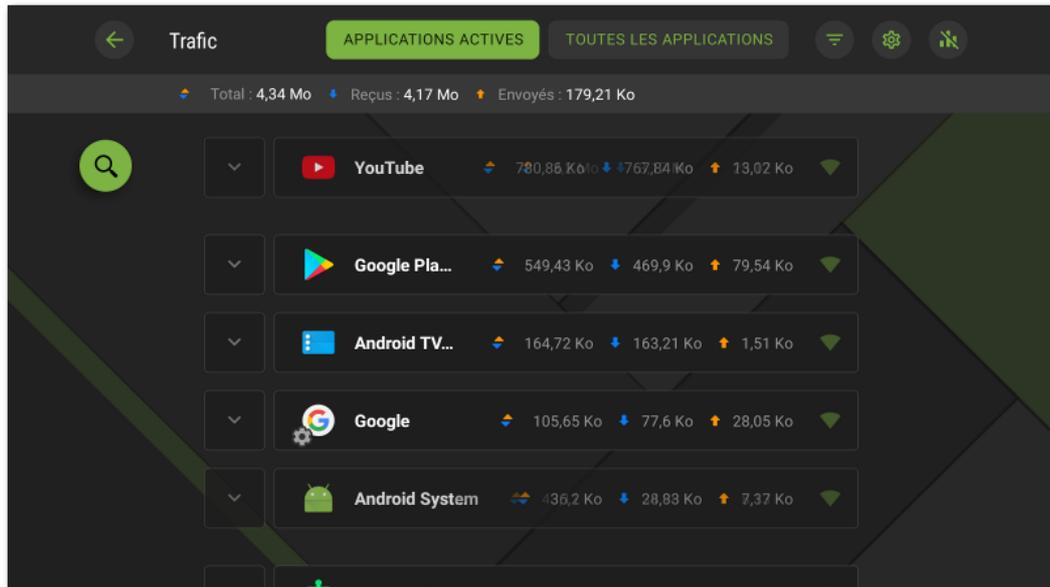


Figure 39. Onglet Applications actives

Connexion des applications

Pour voir les informations détaillées sur les connexions établies par une application, appuyez sur l'icône ▼ à gauche du nom de l'application :

- liste des connexions établies ;
- volume du trafic entrant et sortant par chaque connexion établie ;
- présence d'une règle pour la connexion :
 - ● règle d'autorisation,
 - ● règle de blocage,
 - ● règle de redirection,
 - ○ aucune règle spécifiée.

Appuyez sur la ligne de connexion pour accéder à l'écran [Connexion](#).

Onglet Toutes les applications

Sur l'onglet **Toutes les applications**, vous pouvez voir les informations sur le trafic Internet utilisé par les applications installées sur votre appareil et configurer les règles d'accès aux ressources réseau.

Le volume total des données transmises via le réseau et le volume du trafic envoyé et reçu sont affichés dans l'onglet **Toutes les applications**. Vous pouvez consulter la liste d'applications (et de groupes d'applications). Le volume du trafic Internet utilisé est indiqué pour chaque application.



Les informations suivantes s'affichent pour chaque application sur l'onglet **Toutes les applications** :

- Volume total du trafic entrant et sortant par les connexions établies.
- [Accès à la transmission de données par Wi-Fi](#).
- Présence des paramètres utilisateur. Les applications dont l'accès à la transmission de données a été modifié sont marquées par l'icône .

Filtrage et tri d'applications

Pour filtrer et trier la liste d'applications, appuyez sur l'icône  en bas à droite de l'écran et choisissez les paramètres de filtrage et de tri nécessaires :

- Afficher les applications au trafic zéro.
- Trier :
 - tri décroissant du trafic - les applications au trafic maximal sont en haut de la liste ;
 - tri croissant du trafic - les applications au trafic minimal sont en haut de la liste ;
 - alphabétique (A-Z) ;
 - alphabétique (Z-A).

Les applications sont triés par défaut dans l'ordre décroissant du trafic (les applications au trafic maximal se trouvent en haut de la liste), les applications au trafic zéro ne s'affichent pas. Pour restaurer l'affichage de la liste d'applications par défaut, appuyez sur **Réinitialiser** sur l'écran **Filtre**.

Recherche

Pour accéder rapidement à l'application nécessaire, utilisez la recherche par le nom de

l'application. Pour ce faire, appuyez sur l'icône  dans la partie gauche de l'écran et entrez un mot clé dans le champ de recherche.

Paramètres

Pour spécifier les paramètres pour toutes les applications, appuyez sur  en haut à droite de l'écran **Trafic**.

Les paramètres suivants sont disponibles :

- **Utiliser le protocole Ipv6**. Permet d'activer ou de désactiver l'utilisation du protocole Ipv6 en parallèle avec IPv4.

- **Autoriser le protocole DNS au-dessus de TCP.** Permet d'activer ou de désactiver l'utilisation du protocole DNS par-dessus TCP pour la redirection de requêtes DNS et le masquage de noms de domaine.



L'utilisation du protocole DNS par-dessus TCP peut empêcher l'affichage de noms de domaine sur les écrans du Pare-feu.

Le paramètre fonctionne sur les appareils qui prennent en charge ce type de protocole. Par défaut, le paramètre est désactivé.

- **Bloquer les connexions pour les nouvelles applications** permet de bloquer l'accès des applications installées après l'activation du paramètre au réseau. Le paramètre est actif par défaut.
- **Bloquer les connexions pour toutes les applications** permet de bloquer l'accès de toutes les applications installées sur l'appareil au réseau. Si l'accès au réseau est [accordé](#) à une application, le paramètre sera désactivé.
- **Sauvegarder les règles et les statistiques après la suppression des applications** permet de sauvegarder les données d'une application supprimée de l'appareil pendant une période spécifiée : une semaine, un mois ou un an.

Suppression des statistiques, des paramètres et des règles pour les applications

Pour supprimer les statistiques, les paramètres et les règles pour toutes les applications

1. Sur l'écran **Trafic**, appuyez sur  en haut à droite de l'écran.
2. Cochez la case contre l'option nécessaire et appuyez sur **Effacer**.

11.3.2. Traitement du trafic des applications sous Android TV

Le Pare-feu Dr.Web permet de configurer le traitement du trafic Internet au niveau des applications et de contrôler ainsi l'accès des logiciels et des processus aux ressources réseau. Vous pouvez voir les informations sur le trafic Internet utilisé par une application installée sur votre appareil et configurer ses règles d'accès aux ressources réseau sur l'écran de l'application (voir [Figure 40](#)).

L'écran comporte deux onglets :

- Sur l'onglet [Statistiques](#), vous pouvez consulter les statistiques d'utilisation du trafic Internet et modifier les paramètres individuels de l'application.
- Sur l'onglet [Règles](#), vous pouvez gérer les règles des connexions initiées par l'application.

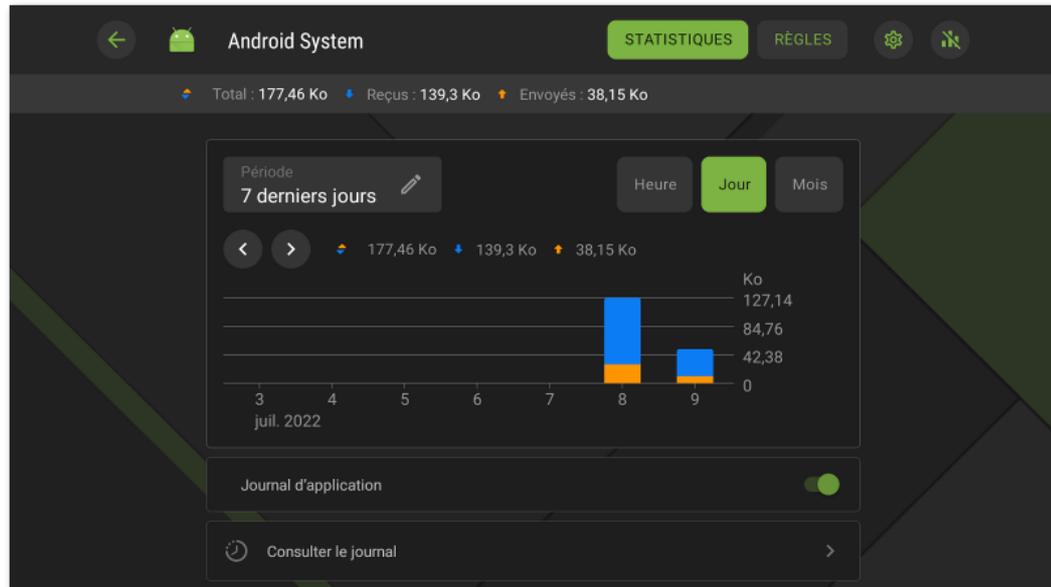


Figure 40. Écran de l'application

Groupe d'applications

Certaines applications de service peuvent être réunies dans un groupe d'applications. Pour voir la liste des applications faisant partie d'un groupe, appuyez sur le compteur à droite de l'entête **Groupe d'applications** sur l'écran de l'application.

11.3.2.1. Statistiques et paramètres de l'application sous Android TV

L'onglet **Statistiques** de l'écran comportant les informations détaillées sur le trafic d'une application (ou d'un groupe d'applications) contient les statistiques d'utilisation de l'Internet par cette application représentées sous forme d'un diagramme (voir [Figure 41](#)). Dans cet onglet, vous pouvez également modifier les paramètres du Pare-feu pour cette application.

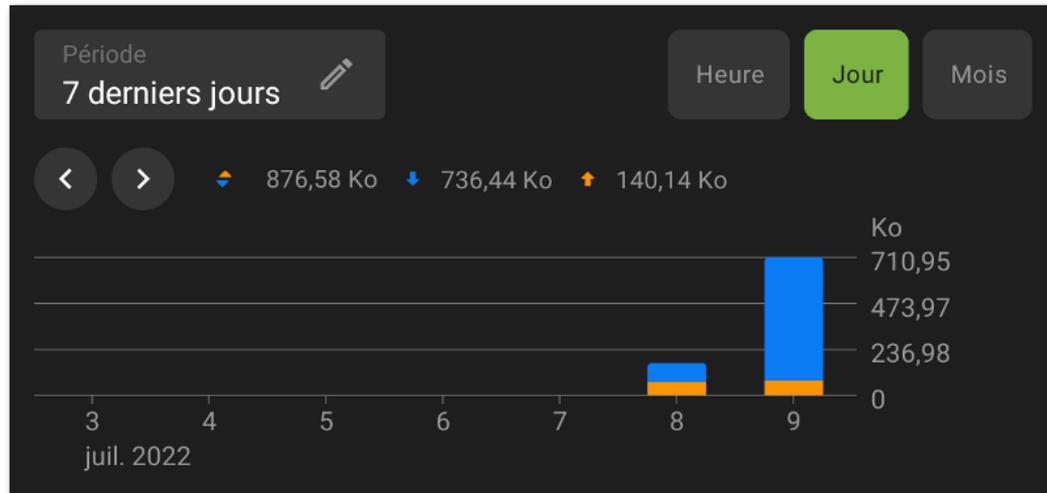


Figure 41. Statistiques d'utilisation du trafic Internet

Statistiques d'utilisation du trafic Internet

Dans le diagramme, le trafic sortant de l'application est marqué par la couleur orange, le trafic entrant est marqué par la couleur bleue. Les valeurs numériques du trafic (total, sortant et entrant) sont affichées sous le diagramme.

Lors de la consultation des statistiques d'utilisation du trafic Internet, vous pouvez effectuer les actions suivantes :

- Sélectionner une période d'affichage des statistiques dans le champ correspondant au-dessus du diagramme. Vous pouvez consulter les statistiques pour la journée en cours, les 7 derniers jours, le mois actuel, le mois précédent ou spécifier les dates de début et de fin d'une période.
- Dans le cadre de la période sélectionnée, vous pouvez configurer l'affichage des statistiques par heures, jours ou mois à l'aide des options se trouvant au-dessus du diagramme.

Effacer les statistiques

- Effacer les statistiques de toutes les applications :
 1. Sur l'écran **Pare-feu**, sélectionnez **Trafic**.
 2. Sur l'écran **Trafic**, appuyez sur  en haut à droite.
 3. Cochez la case **Statistiques des applications** et appuyez sur **Effacer**.
- Effacer les statistiques d'une application spécifique :
 1. Dans l'onglet **Trafic**, sélectionnez l'application dont vous voulez effacer les statistiques.
 2. Sur l'écran de l'application, appuyez sur  en haut à droite.
 3. Cochez la case **Statistiques des applications** et appuyez sur **Effacer**.



Après la suppression de l'application de l'appareil, les statistiques de l'application seront effacées automatiquement dans le délai de 5 minutes.

Journal d'application

Les événements liés à l'activité réseau des applications installées sur l'appareil sont enregistrés dans les [journaux d'applications](#). Utilisez l'interrupteur pour commencer ou reprendre la journalisation de l'application. Pour accéder au journal, appuyez sur **Consulter le journal**.

Paramètres de l'application

Pour accéder aux paramètres d'une application (d'un groupe d'application), appuyez sur  en haut à droite de l'écran, dans l'onglet **Statistiques** (voir [Figure 40](#)).

Accès à la transmission de données par Wi-Fi

Utilisez l'interrupteur pour bloquer ou autoriser la transmission de données par Wi-Fi pour cette application. Par défaut, l'accès est autorisé. L'indicateur d'accès s'affiche à droite, dans la ligne de l'application sur l'écran **Trafic** (l'indicateur vert - l'accès est autorisé, l'indicateur gris - l'accès est bloqué).

Bloquer toutes les connexions sauf celles autorisées par les règles

Pour bloquer par défaut toutes les connexions pour l'application, utilisez l'interrupteur **Bloquer toutes les connexions sauf celles autorisées par les règles**. Si les règles d'autorisation ne sont pas spécifiées pour l'application, elle ne pourra établir aucune connexion.

Si le paramètre **Bloquer toutes les connexions sauf celles autorisées par les règles** est activé pour l'application, une règle d'autorisation sera automatiquement ajoutée pour le port 53. La présence de la règle (pour les protocoles DNS, UDP ou ALL) est obligatoire pour le fonctionnement des règles avec les noms de domaine.



Lorsqu'il y a des règles d'autorisation avec les noms de domaine, il est nécessaire de désactiver également l'utilisation du serveur DNS personnel dans les paramètres de l'appareil pour un fonctionnement correct du paramètre.

Ne pas surveiller l'application



Le paramètre n'est pas disponible pour certaines applications système.



Le pare-feu est réalisé sur la base du VPN pour Android. Le VPN empêche le fonctionnement des applications qui utilisent la technologie non compatible avec le VPN, par exemple, Wi-Fi Direct. Cela peut provoquer l'impossibilité de connexion de l'appareil aux autres appareils. Dans ce cas, il n'est pas recommandé de désactiver le Pare-feu Dr.Web complètement. Au lieu de cela, désactivez le contrôle du Pare feu Dr.Web pour l'application (le groupe d'applications) nécessaire. Pour ce faire, utilisez l'interrupteur **Ne pas surveiller l'application**.

Il est recommandé de désactiver le contrôle du Pare-feu Dr.Web uniquement pour les application fiables.

Une fois l'option activée, le Pare-feu Dr.Web ne contrôle pas les connexions réseau de cette application, même si les restrictions sont spécifiées dans les paramètres du Pare-feu. Le trafic de l'application n'est pas pris en compte.

11.3.2.2. Règles de connexions sous Android TV

La gestion du trafic se fait au niveau des connexions établies par les applications. Pour chaque application installée sur l'appareil, vous pouvez spécifier les règles d'autorisation, les règles de blocage et les règles de redirection des connexions avec les adresses IP et les ports spécifiques.

Connexions

Les informations générales s'affichent sur l'écran **Connexion** (voir [Figure 42](#)). Pour accéder à cet écran, effectuez l'une des actions suivantes :

- Dans l'onglet [Applications actives](#) de l'écran **Trafic**, appuyez sur l'icône ▼ à gauche du nom de l'application. Ensuite, appuyez sur la ligne de la connexion.
- Dans le [journal du Pare-feu](#) :
 - En mode de groupement par date : appuyez sur la ligne de la connexion.
 - En mode de groupement par nom d'application : ouvrez la liste des connexions de l'application en appuyant sur l'icône ▼ à gauche du nom de l'application. Ensuite, appuyez sur la ligne de la connexion.
- Dans le [journal de l'application](#) : ouvrez la liste des connexions en appuyant sur l'icône ▼ à droite de la date de l'événement. Ensuite, appuyez sur la ligne de la connexion.

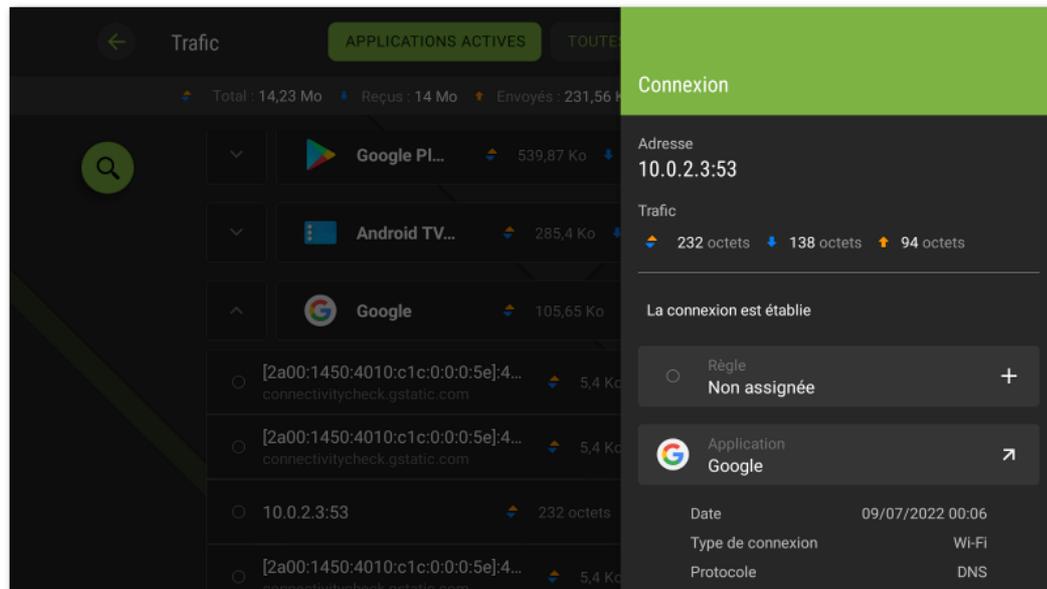


Figure 42. Écran Connexion

L'écran **Connexion** contient les informations suivantes :

- adresse et port de la connexion ;
- nom de l'hôte (si disponible) ;
- volume du trafic entrant et sortant reçu ou transmis par la connexion ;
- statut de la connexion ;
- règle de la connexion ;
- application qui a établi la connexion ;
- date et heure ;
- type de connexion ;
- protocole.

Les règles de connexions sont disponibles sur l'onglet [Règles](#) de l'écran de l'application.

Règles de connexions

Création de règles

Pour créer une nouvelle règle pour la connexion

1. Pour une connexion sans règles :

- Sur l'écran **Connexion**, appuyez sur l'icône **+** à droite de l'élément **Règle**.

Pour toute connexion :

- Appuyez sur l'icône  dans la partie gauche de l'écran **Règles**.
2. Dans la fenêtre qui s'ouvre, sélectionnez un type de règle :
 -  règle d'autorisation,
 -  règle de blocage,
 -  règle de redirection.
 3. Vérifiez si l'adresse IP/le nom de l'hôte est indiqué correctement. Si l'adresse n'est pas indiquée, entrez une adresse IP valide (au format a.b.c.d pour les adresses IPv4 ou [a:b:c:d:e:f:g:h] pour les adresses IPv6), une étendue d'adresses IP (au format a1.b1.c1.d1-a2.b2.c2.d2 ou [a1:b1:c1:d1:e1:f1:g1:h1]-[a2:b2:c2:d2:e2:f2:g2:h2]), un réseau entier (au format a.b.c.0/n, où n est un nombre entre 1 et 32). Si vous créez une règle de redirection, indiquez l'adresse de redirection dans le champ en bas. Vous pouvez indiquer le nom de l'hôte à la place de l'adresse.
 4. Appuyez sur **Options supplémentaires** pour spécifier le paramètre supplémentaire **Protocole** — protocole réseau pour la connexion.
 5. Appuyez sur **Enregistrer**.

Les applications ayant des règles de connexions spécifiées sont marquées par l'icône .

Consulter les règles

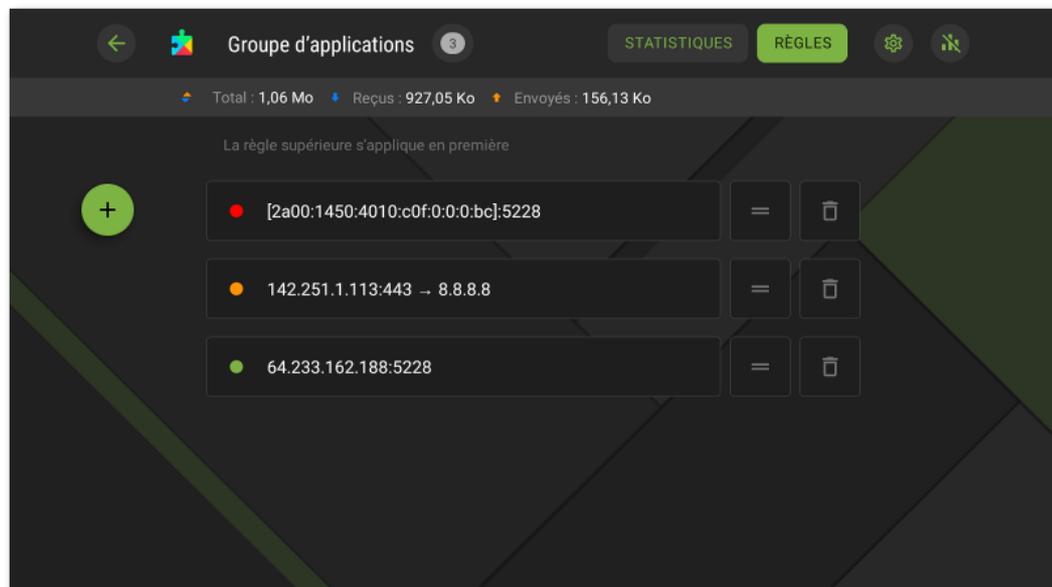


Figure 43. Onglet Règles

Pour consulter les règles des connexions de l'application

- Ouvrez l'écran de l'application et accédez à l'onglet **Règles** (voir [Figure 43](#)).



L'onglet contient la liste de toutes les règles spécifiées pour cette application dans l'ordre de leur utilisation.

Pour modifier l'ordre d'utilisation des règles

- Appuyez et maintenez l'icône  contre la règle que vous voulez déplacer et faites-glisser la règle à la position souhaitée dans la liste.

Modification des règles

Pour modifier une règle existante

1. Effectuez l'une des actions suivantes :
 - Sur l'écran **Connexion**, appuyez sur l'icône  à droite de la règle.
 - Appuyez sur la ligne de la connexion dans l'onglet **Règles** de l'écran de l'application.
2. Apportez les modifications nécessaires.
3. Appuyez sur **Enregistrer**.

Suppression des règles

Pour supprimer une règle

- Sur l'écran de modification de la règle :
 1. Appuyez sur **Supprimer la règle**.
 2. Dans la fenêtre qui s'affiche, appuyez sur **Supprimer**.
- Dans l'onglet **Règles** de l'écran de l'application :
 1. Appuyez sur l'icône  à droite de la règle.
 2. Dans la fenêtre qui s'affiche, appuyez sur **Supprimer**.

Pour supprimer toutes les règles pour une application particulière

1. Appuyez sur l'icône  en haut à droite de l'écran de l'application, dans l'onglet **Règles**.
2. Dans la fenêtre qui s'affiche, cochez la case **Règles pour les applications** et appuyez sur **Effacer**.

Pour supprimer toutes les règles pour toutes les applications

1. Sur l'écran **Pare-feu**, sélectionnez **Trafic**.
2. Appuyez sur l'icône  en haut à droite de l'écran **Trafic**.
3. Dans la fenêtre qui s'affiche, cochez la case **Paramètres et règles pour les applications** et appuyez sur **Effacer**.



Bloquer toutes les connexions sauf celles autorisées par les règles

Avec l'[interrupteur correspondant](#) sur l'écran des paramètres de l'application, vous pouvez bloquer toutes les connexions de l'application sauf celles qui sont autorisées par les règles.

11.3.2.3. Journal de l'application sous Android TV

Les journaux des applications contiennent la liste des événements liés aux connexions réseau d'une des applications installées sur votre appareil.

Pour activer la journalisation de l'application

1. Sélectionnez l'application nécessaire sur l'écran **Trafic**.
2. Utilisez l'interrupteur **Journal d'application** sur l'écran de l'application.

Pour ouvrir le journal de l'application

1. Dans l'onglet **Trafic**, sélectionnez l'application nécessaire dans la liste.
2. Appuyez sur **Consulter le journal** sur l'écran de l'application.

Afficher le journal de l'application

Tous les événements sont groupés par date. Pour afficher les événements pour une date précise, sélectionnez la date dans la liste.

Pour chaque événement, les informations suivantes sont affichées :

- adresse et port de la connexion ;
- trafic consommé ;
- présence d'une règle pour la connexion :
 -  règle d'autorisation,
 -  règle de blocage,
 -  règle de redirection,
 -  aucune règle spécifiée.

Appuyez sur la ligne de connexion pour accéder à l'écran [Connexion](#) et configurer les règles pour cette connexion.

Pour vider le journal de l'application

1. Appuyez sur l'icône  en haut à droite de l'écran **Journal d'application**.
2. Appuyez sur **Effacer**.

Pour désactiver la journalisation de l'application

1. Sélectionnez l'application nécessaire sur l'écran **Trafic**.
2. Utilisez l'interrupteur **Journal d'application** sur l'écran de l'application.

11.3.3. Journal du Pare-feu Dr.Web sous Android TV

Pour afficher la liste de tous les événements liés au fonctionnement du Pare-feu Dr.Web, sélectionnez **Journal** sur l'écran **Pare-feu**.

Le journal du Pare-feu (voir [Figure 44](#)) contient les informations suivantes concernant l'événement :

- nom de l'application ;
- adresse et port de la connexion (ainsi que l'adresse de redirection si la règle correspondante est spécifiée) ;
- trafic consommé ;
- date et heure de l'événement ;
- présence d'une règle pour la connexion.

Quand vous appuyez sur l'événement, l'écran [Connexion](#) s'affiche.

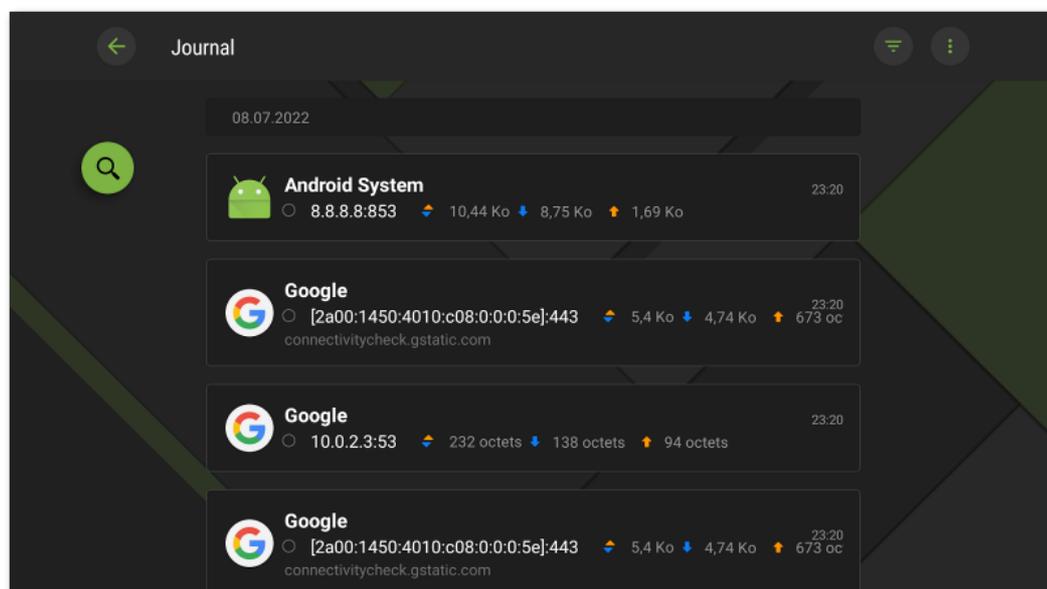


Figure 44. Journal du Pare-feu Dr.Web

Pour filtrer ou trier les événements dans le journal du Pare-feu

1. Appuyez sur l'icône  en haut à droite de l'écran **Journal**.



2. Sélectionnez les paramètres de filtrage ou de tri nécessaires :

- Trier :
 - par ordre chronologique décroissant - les derniers événements sont en haut du journal ;
 - par ordre chronologique croissant — les derniers événements sont en bas du journal ;
 - alphabétique (A-Z) ;
 - alphabétique (Z-A).
- Afficher les connexions :
 - établies,
 - réinitialisées,
 - redirigées,
 - avec une erreur.

Par défaut les événements sont triés par date (les derniers événements se trouvent en haut du journal), tous les types de connexions sont affichés. Pour restaurer l’affichage du journal par défaut, appuyez sur **Réinitialiser** sur l’écran **Filtre**.

Pour faciliter la consultation du journal, vous pouvez également grouper les événements par application.

Pour grouper les événements par application

- Sur l’écran **Journal**, appuyez sur  en haut à droite de l’écran et utilisez l’interrupteur **Regrouper par nom d’application**.

Pour effectuer une recherche dans le journal du Pare-feu

- Appuyez sur l’icône  dans la partie gauche de l’écran et entrez un mot clé dans le champ de recherche.

Pour vider le journal du Pare-feu

1. Sur l’écran **Journal**, appuyez sur  en haut à droite de l’écran et sélectionnez l’option **Vider le journal**.
2. Confirmez l’action en appuyant sur le bouton **Effacer**.



Taille du journal

Par défaut, la taille du fichier de journal est de 5 Mo.

Pour modifier la taille maximale du fichier de journal

1. Sur l'écran **Journal**, appuyez sur  en haut à droite de l'écran et sélectionnez l'option **Taille du journal**.
2. Dans la fenêtre qui s'affiche, modifiez la valeur et appuyez sur **Enregistrer**.



La taille maximale du journal doit être supérieure à 0 Mo et inférieure ou égale à 99 Mo .

11.4. Contrôleur de sécurité sous Android TV

Dr.Web effectue le diagnostic de votre appareil et donne des recommandations pour résoudre les problèmes et les vulnérabilités détectés à l'aide du composant spécifique Contrôleur de sécurité. Le composant est lancé automatiquement après le premier démarrage de l'application et l'enregistrement de la licence.

Problèmes de sécurité et moyens de les neutraliser

Dr.Web détecte les problèmes de sécurité suivants :

- [Vulnérabilités](#) ;
- [Paramètres système](#) qui influencent la sécurité de l'appareil ;
- [Administrateurs de l'appareil non affichés](#) ;
- [Applications utilisant la vulnérabilité Fake ID](#).

Pour ouvrir la liste des problèmes de sécurité détectés (voir [Figure 45](#)), sélectionnez **Contrôleur de sécurité** sur l'écran d'accueil de Dr.Web.

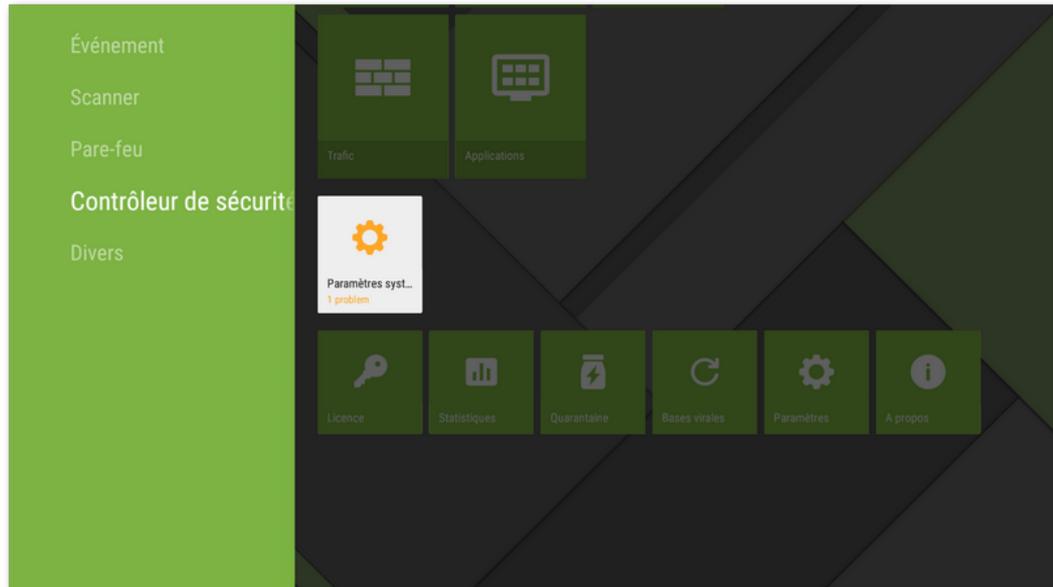


Figure 45. Contrôleur de sécurité

Vulnérabilités

Une *vulnérabilité* est une faille dans le code de programme qui peut être utilisée par les cybercriminels afin de perturber le fonctionnement du système.

Le Contrôleur de sécurité détecte les vulnérabilités suivantes dans le système de l'appareil : [BlueBorne](#), [EvilParcel](#), [Extra Field](#), [Fake ID](#), [Janus](#), [ObjectInputStream Serialization](#), [OpenSSLX509Certificate](#), [PendingIntent](#), [SIM Toolkit](#), [Stagefright](#) et [Stagefright 2.0](#).

En utilisant les vulnérabilités, les cybercriminels peuvent ajouter un code de programmation dans les applications. De ce fait, ces applications peuvent accomplir des fonctions dangereuses pour la sécurité de l'appareil.

Si le système de votre appareil contient une ou plusieurs vulnérabilités, veuillez vérifier s'il y a des mises à jour pour le système d'exploitation sur le site Web officiel du fabricant de votre appareil. Les vulnérabilités peuvent être résolues dans des nouvelles versions du système d'exploitation. S'il n'y a pas de mises à jour, il est recommandé d'installer des logiciels provenant uniquement des sources de confiance.

Accès root

L'appareil peut devenir vulnérable aux menaces s'il est rooté, c'est-à-dire, s'il a été soumis à une procédure de rootage afin d'obtenir les droits du super-utilisateur (root). Cela permet de modifier et de supprimer les fichiers système, ce qui peut rendre l'appareil inopérable. Si vous avez rooté l'appareil vous-même, il est recommandé d'annuler ces modifications pour des raisons de sécurité. Si l'accès root est une particularité technique de votre appareil, ou bien qu'il



est nécessaire pour exécuter certaines tâches, vous devez porter une attention particulière aux applications provenant de sources inconnues.

Paramètres système

Le Contrôleur de sécurité détecte les paramètres système suivants qui influencent la sécurité de l'appareil :

- **Débogage activé.** Le débogage USB est destiné aux développeurs et permet de copier les données depuis l'ordinateur sur un appareil tournant sous Android et vice versa, d'installer les applications sur l'appareil, de voir les journaux des applications installées et de les supprimer dans certains cas. Si vous n'êtes pas développeur et n'utilisez pas ce mode de débogage, il est recommandé de le désactiver. Pour ouvrir la section correspondante des paramètres système, sélectionnez **Paramètres** sur l'écran contenant les informations détaillées sur ce problème.
- **Installation depuis des sources inconnues activée.** L'installation d'applications depuis des sources inconnues est une cause principale de diffusion de menaces pour les appareils tournant sous Android. Les applications installées depuis d'autres sources que la boutique d'applications officielle sont souvent dangereuses et elles peuvent endommager l'appareil. Pour réduire les risques d'installer des applications malveillantes, il est recommandé d'interdire l'installation des applications provenant des sources inconnues. Pour ouvrir la section correspondante des paramètres système, sélectionnez **Paramètres** sur l'écran contenant les informations détaillées sur ce problème. De plus, il est recommandé de scanner par l'antivirus toutes les applications avant de les installer. Avant l'analyse, assurez-vous que les bases virales Dr.Web sont à jour.
- **Les notifications Dr.Web sont bloquées.** Dans ce cas, Dr.Web ne peut pas vous informer des menaces détectées. Cela réduit la protection de l'appareil et peut provoquer son infection. C'est pourquoi, il est recommandé d'accéder aux paramètres de votre appareil et d'activer les notifications de Dr.Web.
- **Un certificat racine utilisateur est installé.** Si des certificats utilisateur sont détectés sur l'appareil, les détails seront affichés dans le Contrôleur de sécurité. Les certificats utilisateur permettent à des tiers de consulter votre activité réseau. Si vous ne connaissez pas la désignation des certificats détectés, il est recommandé de les supprimer de votre appareil.

Administrateurs de l'appareil non affichés

Les applications activées en tant qu'administrateurs de l'appareil, mais qui ne sont pas présentes dans la liste des administrateurs de la section correspondante des paramètres de l'appareil, ne peuvent pas être supprimées à l'aide des outils standard du système d'exploitation. Dans la plupart des cas, telles applications sont dangereuses.

Si vous ne savez pas pourquoi l'application masque sa présence dans la liste des administrateurs de l'appareil, il est recommandé de la supprimer. Pour supprimer l'application, sélectionnez **Supprimer** sur l'écran contenant les informations détaillées sur le problème lié à cette application.

Applications utilisant la vulnérabilité Fake ID

Si les applications utilisant la vulnérabilité Fake ID sont détectées sur l'appareil, elles seront affichées dans une section à part du Contrôleur de sécurité. Ces applications peuvent être malveillantes, c'est pourquoi il est recommandé de les supprimer. Pour supprimer une application, appuyez sur **Supprimer** sur l'écran contenant les informations détaillées sur le problème lié à cette application ou utilisez les outils de l'OS.

11.5. Divers

La section **Divers** (voir [Figure 46](#)) permet d'ouvrir les paramètres de l'application, d'accéder à la quarantaine et aux statistiques. Vous pouvez consulter les informations sur la version de l'application, la licence et les dates de son activation et de son expiration. Vous pouvez également consulter la date de la dernière mise à jour des bases virales et lancer la mise à jour manuellement.

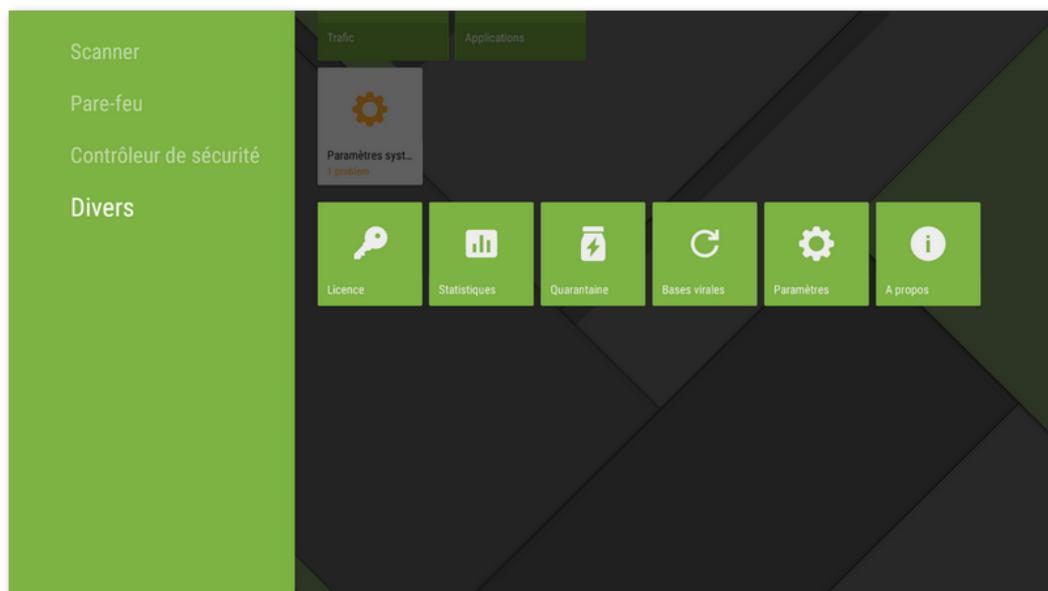


Figure 46. Divers

Licence

Vous pouvez regarder les dates d'enregistrement et d'expiration de la licence.

Dans cette fenêtre, vous pouvez également [acheter](#) et [activer](#) une nouvelle licence.



Statistiques

La section **Statistiques** permet de consulter les informations sur les résultats de l'analyse effectuée par le Scanner Dr.Web, l'activation/la désactivation du composant SpIDer Guard, les menaces détectées et les actions appliquées pour les neutraliser (voir la rubrique [Statistiques](#)).

Quarantaine

Quarantaine est un dossier spécial destiné à isoler et à sauvegarder en sécurité les menaces détectées (voir la rubrique [Quarantaine](#)).

Bases virales

Afin de détecter les menaces de sécurité, Dr.Web utilise les bases virales spéciales qui contiennent les informations sur toutes les menaces informatiques créées pour infecter les appareils tournant sous Android connues par les spécialistes de Doctor Web. Les bases nécessitent la mise à jour périodique, car de nouveaux logiciels malveillants apparaissent régulièrement. C'est pourquoi, l'application possède la fonctionnalité de mise à jour des bases virales via Internet.

Mise à jour

Pour savoir si une mise à jour manuelle est requise :

1. Ouvrez la section **Bases virales**.
2. Dans la fenêtre qui s'ouvre, vous verrez le statut des bases virales et la date de la dernière mise à jour.

Si les bases virales sont obsolètes, vous devez les mettre à jour manuellement. Pour ce faire, sélectionnez **Mise à jour** dans le panneau à droite.



Il est fortement recommandé d'effectuer la mise à jour des bases virales juste après l'installation de l'application pour que Dr.Web puisse utiliser les dernières informations sur les menaces connues. Dès que les experts du laboratoire antivirus de Doctor Web découvrent de nouvelles menaces, les signatures virales, les caractéristiques des virus et leurs modes d'actions sont mis à jour. Dans certains cas, les mises à jour peuvent être éditées plusieurs fois par heure.

Paramètres

La section **Paramètres** permet de configurer les composants de la protection antivirus, de spécifier les paramètres de l'application, d'activer et de désactiver la fonction d'envoi des statistiques et de réinitialiser les paramètres par défaut (voir la rubrique [Paramètres de Dr.Web sous Android TV](#)).



A propos

Sur l'écran **A propos**, vous pouvez consulter la version de l'application. De plus, sur cet écran, vous trouverez les liens vers le site officiel de la société Doctor Web.

11.5.1. Paramètres de Dr.Web sous Android TV

Paramètres généraux

- **Sons** permet de configurer les alertes sonores de détection, suppression et déplacement des menaces en quarantaine. Les alertes sonores sont activées par défaut.
- **Envoi des statistiques** permet d'activer et de désactiver l'envoi des statistiques à la société Doctor Web.
- **Options supplémentaires** contient les paramètres avancés suivants :
 - **Applications systèmes** permet d'activer et de désactiver la notification des [menaces dans les applications système](#) qui ne peuvent pas être supprimées sans perte d'efficacité de l'appareil. L'option est désactivée par défaut.

SpIDer Guard

- **Fichiers archivés** permet d'activer l'analyse des fichiers dans des archives.



Par défaut, l'analyse des fichiers dans les archives est désactivée. L'activation de cette fonctionnalité peut affecter les performances du système. En tout cas, même si l'analyse des archives est désactivée, la protection reste fiable, parce que SpIDer Guard analyse les fichiers d'installation APK indépendamment de la valeur spécifiée pour le paramètre **Fichiers archivés**.

- **Carte SD intégrée et supports amovibles** permet d'activer le scan de la carte SD intégrée ou des supports amovibles lors de chaque montage. Si ce paramètre est activé, le scan est lancé à chaque activation du composant SpIDer Guard.
- **Zone système** permet de suivre les [modifications](#) dans la zone système. Si ce paramètre est activé, SpIDer Guard suit les modifications (ajout, modification et suppression des fichiers) et vous informe de la suppression de tout fichier, ainsi que de l'ajout ou de la modification des fichiers exécutables : `.jar`, `.odex`, `.so`, fichiers aux formats APK, ELF, etc.
- **Nouvelle analyse de la zone système** permet de relancer le scan de la zone système. SpIDer Guard analysera de nouveau toutes les menaces dans la zone système qui ont été ignorées auparavant.
- **Notifications de la zone système** permet d'activer la notification de la modification de tous les fichiers dans la zone système (non seulement des fichiers exécutables).
- **Options supplémentaires** permet d'activer et de désactiver le scan du système pour la présence des adwares et des riskwares (y compris les hacktools et les canulars).



Scanner

- **Fichiers archivés** permet d'activer l'analyse des fichiers dans des archives.



Par défaut, le scan des fichiers dans les archives est désactivé. L'activation de cette fonctionnalité peut affecter les performances du système. En tout cas, même si l'analyse des archives est désactivée, la protection reste fiable, parce que le Scanner Dr.Web analyse les fichiers d'installation `.apk` indépendamment de la valeur spécifiée pour le paramètre **Fichiers archivés**.

- **Options supplémentaires** permet d'activer et de désactiver le scan du système pour la présence des adwares et des riskwares (y compris les hacktools et les canulars).

Plus

- **Réinitialisation des paramètres** permet de réinitialiser les paramètres par défaut à tout moment.
- **Nouvelle version** (l'option est disponible dans la version installée depuis le site de Doctor Web) permet de configurer la vérification de la disponibilité d'une nouvelle version à chaque mise à jour des bases virales de l'application. Lorsqu'une nouvelle version de l'application devient disponible, vous recevrez une notification standard et vous pourrez la télécharger et installer.



12. Service de support technique

En cas de problèmes liés à l'installation ou au fonctionnement des produits de la société, avant de contacter le support technique, essayez de trouver la solution par un des moyens suivants :

1. Consultez les dernières versions des descriptions et des manuels à l'adresse <https://download.drweb.com/doc/>.
2. Lisez la rubrique de questions fréquentes à l'adresse https://support.drweb.com/show_faq/.
3. Visitez des forums de Doctor Web à l'adresse <https://forum.drweb.com/>.

Si après avoir tout essayé, vous n'avez pas résolu le problème, utilisez un des moyens suivants pour contacter le support technique de Doctor Web :

1. Remplissez le formulaire de question dans la section correspondante de la rubrique <https://support.drweb.com/>.
2. Appelez le numéro de l'assistance technique française 0 825 300 230 ou le numéro de l'assistance internationale +7 (495) 789 45 86. Les utilisateurs en Russie peuvent nous contacter en appelant le numéro vert 8 800 333 7932.

Vous pouvez trouver les informations sur les bureaux régionaux de Doctor Web sur le site officiel à l'adresse <https://company.drweb.com/contacts/offices/>.



13. Mot de passe oublié ?

Si vous avez oublié le mot de passe du compte Dr.Web, réinitialisez-le et créez un nouveau mot de passe :

- [Par e-mail](#). Vous avez indiqué cette adresse e-mail lors de la création du compte ou la configuration de l'Antivol Dr.Web.
- [Par SMS](#). Cette option est disponible uniquement dans la version de l'application téléchargée depuis le site, si au moins un numéro de téléphone est ajouté dans la liste d'amis dans l'Antivol.
- [Avec une notification](#). Cette option est disponible si au moins un ami a accepté votre demande d'ami dans l'application Dr.Web Security Space.
- [A l'aide d'une demande envoyée au support technique](#). Le service du support technique peut vous aider s'il s'assure que vous êtes le propriétaire de l'appareil.



Si Dr.Web fonctionne en [mode de protection centralisée](#) et que l'Antivol Dr.Web est configuré sur le serveur, vous ne pourrez pas spécifier un nouveau mot de passe par les moyens indiqués. Dans ce cas, contactez l'administrateur du réseau antivirus de votre entreprise ou le fournisseur du service Antivirus Dr.Web et utilisez [le code symbolique ou le code QR de récupération](#).

Réinitialiser le mot de passe à l'aide de l'e-mail

Le panneau de réinitialisation du mot de passe à l'aide de l'e-mail (voir [Figure 47](#)) contient :

- **Clé**. C'est une séquence unique de caractères générée pour votre compte.
- **Adresse e-mail**. Vous avez utilisé cette adresse e-mail lors de la création du compte ou la configuration de l'Antivol Dr.Web.

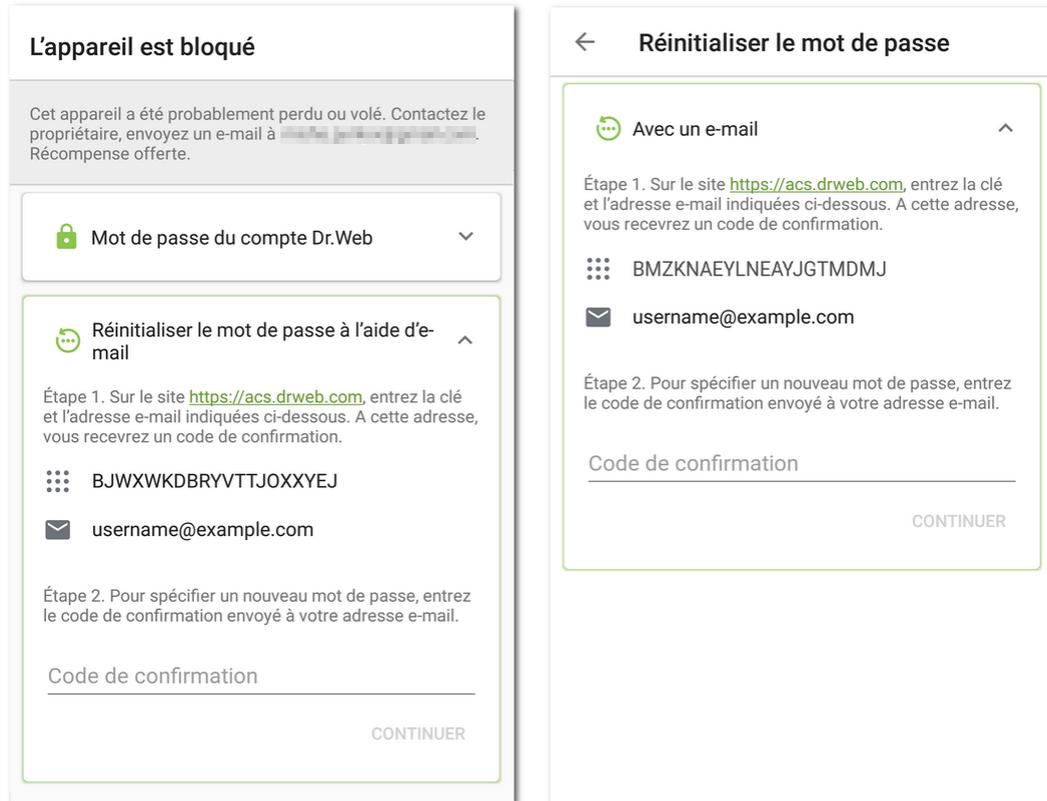


Figure 47. Réinitialiser le mot de passe par e-mail
Appareil bloqué (à gauche) et non bloqué (à droite)

Pour réinitialiser le mot de passe

1. Sur un ordinateur ou un autre appareil, ouvrez la page Web du compte Dr.Web : <https://acs.drweb.com> (voir [Figure 48](#)).



Si Dr.Web 11.1.3 ou une version antérieure est installée sur votre appareil, pour réinitialiser le mot de passe, accédez à la page de l'Antivol Dr.Web <https://antitheft.drweb.com/> ou mettez à niveau l'application vers la version 12.



Figure 48. Compte Dr.Web

2. Sur cette page, entrez la clé et l'adresse e-mail (voir [Figure 49](#)) indiquées dans l'application Dr.Web.

Figure 49. Saisie de la clé et de l'e-mail

3. Appuyez sur **Obtenir le code**.



Si toutes les données sont saisies correctement, un message s'affichera vous informant qu'un e-mail contenant un code de confirmation a été envoyé sur votre adresse e-mail (voir [Figure 50](#)).

Si vous ne recevez pas l'e-mail dans les 10 minutes qui suivent :

1. Vérifiez le dossier Spam.
2. Essayez de saisir les données encore une fois. Il se peut que vous ayez spécifié une clé invalide ou une adresse e-mail différente de celle indiquée dans l'application Dr.Web.
3. Si après toutes ces actions, vous n'avez toujours pas d'e-mail, contactez le support technique de Doctor Web. Pour ce faire, appuyez sur **Toujours pas d'e-mail ?** (voir [Figure 50](#)).



Figure 50. Notification d'envoi du code de confirmation

4. Ouvrez le message du service « Compte Dr.Web ». Le message contient le code de confirmation.



- Dans l'application Dr.Web, saisissez le code de confirmation dans le champ **Code de confirmation** (voir [Figure 51](#)).

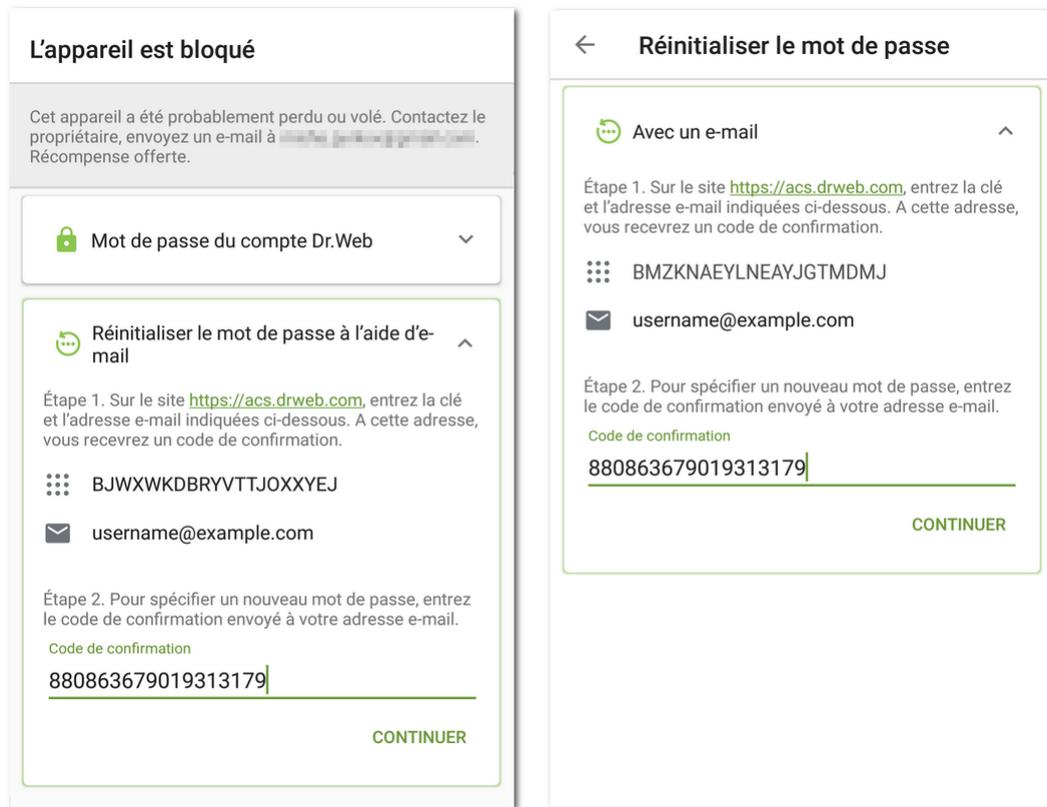


Figure 51. Saisie du code de confirmation reçu par e-mail

Appareil bloqué (à gauche) et non bloqué (à droite)

- Appuyez sur **Continuer**.
- Entrez un nouveau mot de passe sur l'écran **Modifier le mot de passe**. Le mot de passe doit contenir au moins 4 caractères.
Appuyez sur l'icône  à droite du champ de saisie pour afficher les caractères entrés. Pour masquer les caractères, appuyez sur l'icône .
- Confirmez le mot de passe et appuyez sur **Enregistrer**.

Réinitialiser le mot de passe à l'aide d'un SMS envoyé depuis le numéro d'un ami

Vous pouvez réinitialiser le mot de passe de cette façon si les conditions suivantes sont satisfaites :

- La version de l'application téléchargée depuis le site de Doctor Web est installée sur votre appareil.
- Votre appareil est allumé et il se trouve dans la zone de portée.
- L'Antivol Dr.Web est activé sur votre appareil.



4. Au moins un numéro de téléphone est ajouté dans la liste [Je leur fais confiance](#) dans l'Antivol.
5. Le numéro depuis lequel la commande SMS sera envoyée est ajouté dans la liste [Je leur fais confiance](#).
6. Vous avez le numéro de téléphone de la carte SIM utilisée sur votre appareil. La commande SMS peut être envoyée seulement sur ce numéro.

Si vous n'avez pas ce numéro, insérez une carte SIM avec un numéro connu.



Si vous utilisez deux cartes SIM sur votre appareil, vous pouvez envoyer la commande SMS sur chacun de ces deux numéros.

Pour réinitialiser le mot de passe

1. Envoyez un SMS avec le texte **#RESETPASSWORD#** sur l'appareil de votre ami.

La liste des numéros depuis lesquels on peut envoyer la commande SMS se trouve sur l'écran **L'appareil est bloqué** ou **Réinitialiser le mot de passe** (voir [Figure 52](#)). La commande SMS n'est pas sensible à la casse.

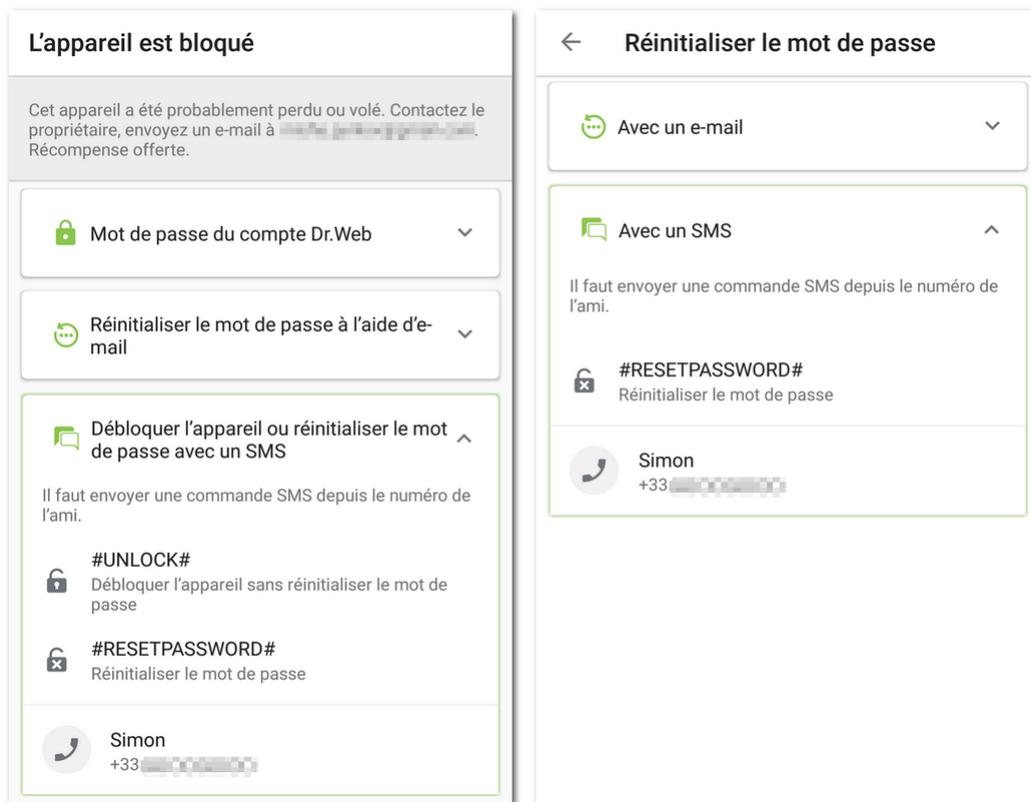


Figure 52. Réinitialiser le mot de passe à l'aide d'un SMS envoyé depuis le numéro d'un ami

Appareil bloqué (à gauche) et non bloqué (à droite)



2. Une fois le SMS reçu, l'écran **Modifier le mot de passe** s'affiche automatiquement sur votre appareil. Spécifiez un nouveau mot de passe. Si l'appareil est bloqué, il se débloquent.



Si l'appareil est bloqué, vous pouvez le débloquent sans réinitialiser le mot de passe. Pour ce faire, envoyez la commande SMS **#UNLOCK#** sur l'appareil.

Réinitialiser le mot de passe à l'aide d'une notification

Vous pouvez réinitialiser le mot de passe à l'aide d'une notification si les conditions suivantes sont satisfaites :

• Pour votre appareil

1. L'appareil est allumé et connecté à Internet.
2. L'Antivol Dr.Web est activé.
3. Au moins une adresse e-mail est ajoutée à la liste [Je leur fais confiance](#) dans l'Antivol.

• Pour l'appareil de l'ami

- Si votre appareil est bloqué :
 1. L'appareil de l'ami est allumé et connecté à Internet.
 2. L'application Dr.Web Light ou Dr.Web Security Space est installée sur l'appareil de l'ami.
 3. L'ami a accepté votre demande d'ami dans le composant Aide à l'ami ou dans l'Antivol Dr.Web. Pour recevoir votre notification, il faut que tous les composants soient activés.
- Si votre appareil n'est pas bloqué :
 1. L'appareil de l'ami est allumé et connecté à Internet.
 2. L'application Dr.Web Security Space est installée sur l'appareil de l'ami.
 3. L'ami a accepté votre demande d'ami dans l'Antivol Dr.Web. Pour recevoir votre notification, il faut que le composant soit activé.

Pour réinitialiser le mot de passe

1. Envoyez une notification à l'ami. Pour ce faire, appuyez sur l'icône ► (voir [Figure 53](#)).
2. Communiquez à votre ami le code de confirmation indiqué dans le même panneau.
L'ami doit entrer le code de confirmation sur son appareil et envoyer la commande de réinitialiser le mot de passe à l'Antivol.
3. Une fois la commande reçue, l'écran **Modifier le mot de passe** s'affiche automatiquement sur votre appareil. Spécifiez un nouveau mot de passe. Si l'appareil est bloqué, il se débloquent.

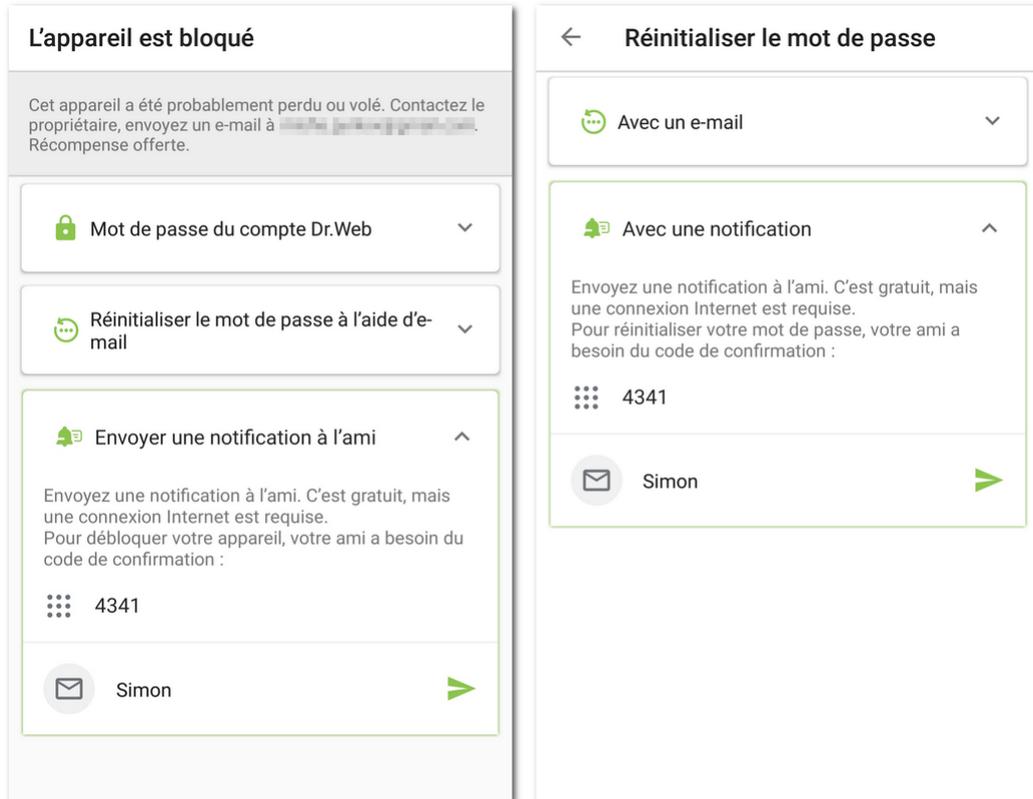


Figure 53. Réinitialiser le mot de passe à l'aide d'une notification

Appareil bloqué (à gauche) et non bloqué (à droite)

Réinitialiser le mot de passe à l'aide d'une demande envoyée au support technique

Si vous ne pouvez pas débloquer l'appareil ou spécifier un nouveau mot de passe, envoyez une demande au service de support technique Dr.Web :

1. Ouvrez la page du service de support technique : <https://support.drweb.com/>.
2. Dans la section **Service de support technique**, sélectionnez l'élément **Fonctionnement de l'application Dr.Web**.
3. Indiquez les données de votre licence ou le numéro de commande.
4. Dans l'onglet **Protection d'un PC/Mac à domicile**, sélectionnez l'élément **Android**.
5. Remplissez tous les champs sur la page qui s'ouvre.
6. Veuillez joindre à la demande les fichiers suivants :
 - Photo de l'écran **L'appareil est bloqué** ou **Réinitialiser le mot de passe** contenant la clé et l'adresse e-mail (voir [Figure 47](#)).
 - Si vous avez conservé l'emballage original de l'appareil, veuillez joindre une photo de l'emballage avec le numéro IMEI (un identificateur unique de votre appareil composé de 15 chiffres).



- Photo ou scan de la facture de l'appareil.
- Photo ou scan du certificat de garantie rempli.
- Documents prouvant votre paiement de la licence Dr.Web (message de la boutique en ligne, document de paiement, etc.). Si vous avez gagné la licence aux enchères Dr.Web, indiquez le login de votre profil sur le site Doctor Web. Si vous utilisez la version démo, sautez cet étape.



Le texte sur l'image doit être lisible : les spécialistes du service de support technique doivent s'assurer que vous êtes le propriétaire de l'appareil et de la licence Dr.Web.

7. Appuyez sur **Envoyer**.

Sur l'e-mail indiqué dans votre demande, vous recevrez un message contenant un lien sur votre demande. Le code de confirmation sera indiqué sur la page de votre demande.

8. Sur l'écran **L'appareil est bloqué** ou **Réinitialiser le mot de passe** entrez le code de confirmation dans le champ **Code de confirmation** (voir [Figure 51](#)) et appuyez sur **Continuer**.

9. Entrez un nouveau mot de passe sur l'écran **Modifier le mot de passe**. Le mot de passe doit contenir au moins 4 caractères.

Appuyez sur l'icône  à droite du champ de saisie pour afficher les caractères entrés. Pour masquer les caractères, appuyez sur l'icône .

10. Confirmez le mot de passe et appuyez sur **Enregistrer**.

Débloquer l'appareil avec la requête envoyée à l'administrateur

Si Dr.Web fonctionne en mode de protection centralisée et que l'Antivol Dr.Web est configuré sur le serveur, vous devez contacter l'administrateur du réseau antivirus de votre entreprise ou le fournisseur du service Antivirus Dr.Web pour débloquer l'appareil. Vous pouvez utiliser deux options de déblocage :

- Avec un code QR :

1. Contactez l'administrateur du réseau antivirus de votre entreprise ou le fournisseur du service Antivirus Dr.Web à l'aide de n'importe quelle méthode disponible.
2. Communiquez à l'administrateur le code QR de l'écran **L'appareil est bloqué**. Appuyez et maintenez le code QR pour le sauvegarder sur l'appareil. Vous pouvez également communiquer une photo de l'écran avec le code QR lisible.

L'administrateur vous enverra un code QR pour confirmer le déblocage de l'appareil.

3. Assurez-vous que vous avez reçu le code QR de déblocage et appuyez sur **Continuer**.
4. Dans la fenêtre qui s'ouvre, appuyez sur le bouton **Scanner le code QR** et pointez votre appareil photo sur le code QR de déblocage reçu de l'administration.

Si le code QR est reconnu, l'appareil sera débloqué.

- Avec un code de caractère :

1. Sur l'écran **L'appareil est bloqué**, appuyez sur **Autre moyen**.



2. Contactez l'administrateur du réseau antivirus de votre entreprise ou le fournisseur du service Antivirus Dr.Web à l'aide de n'importe quelle méthode disponible.
3. Communiquez à l'administrateur l'identificateur et le code de récupération affichés sur l'écran **L'appareil est bloqué**.

L'administrateur vous enverra le code de déblocage de l'appareil.

4. Assurez-vous que vous avez reçu le code de déblocage et appuyez sur **Continuer**.
5. Dans la fenêtre qui s'ouvre, saisissez le code reçu de l'administrateur dans le champ **Code de déblocage** et appuyez sur **Débloquer**.

Si le code de déblocage est saisi correctement, l'appareil sera débloqué.

Si vous n'arrivez pas à terminer la procédure de déblocage de l'appareil de façon choisie, appuyez sur **Autre moyen** sur l'écran **L'appareil est bloqué** pour utiliser une option alternative.

Une fois le mot de passe réinitialisé après le déblocage de l'appareil, contactez l'administrateur du réseau antivirus de votre entreprise ou le fournisseur du service Antivirus Dr.Web.

