



Dr.WEB®

CureNet!

Protège votre univers

**Manuel abrégé de
configuration et
démarrage**

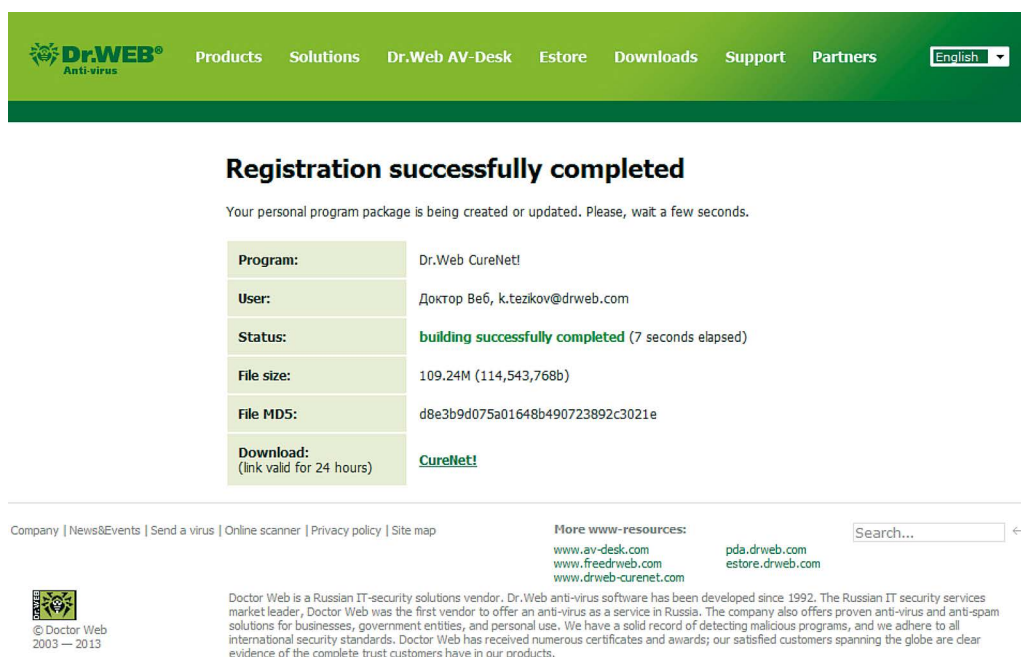


Dr.Web CureNet! est destiné à une analyse antivirus centralisée des ordinateurs réunis au sein d'un réseau, sans installer l'antivirus sur les ordinateurs distants. Dr.Web CureNet! vous permet de scanner les postes de travail et serveurs fonctionnant sous le système d'exploitation Microsoft® Windows®, quelle que soit la structure du réseau auquel ils sont liés.

Attention ! Dr.Web CureNet! n'est pas conçu pour assurer une protection permanente en temps réel des ordinateurs, car dans les intervalles entre les sessions de scan, ils peuvent être contaminés par des programmes malveillants de différents types. Pour une protection permanente des ordinateurs réunis dans un réseau local, les produits suivants sont recommandés : Dr.Web Security Space Pro et Dr.Web Enterprise Security Suite.

Obtenir un package d'installation Dr.Web CureNet!

Afin d'obtenir un package d'installation Linux vous devez enregistrer le numéro de série sur la page <http://products.drweb.com/register/>. Après la fin de l'enregistrement, un package d'installation personnalisé sera créé et disponible en téléchargement depuis votre Espace personnel.



The screenshot shows the Dr.Web CureNet! registration success page. At the top, there is a navigation bar with links for Products, Solutions, Dr.Web AV-Desk, Estore, Downloads, Support, and Partners, along with a language dropdown set to English. The main heading is "Registration successfully completed". Below this, a message states: "Your personal program package is being created or updated. Please, wait a few seconds." A table provides the following details:

Program:	Dr.Web CureNet!
User:	Доктор Веб, k.tezikov@drweb.com
Status:	building successfully completed (7 seconds elapsed)
File size:	109.24M (114,543,768b)
File MD5:	d8e3b9d075a01648b490723892c3021e
Download: (link valid for 24 hours)	CureNet!

At the bottom, there is a footer with company information, a search bar, and a list of resources: www.av-desk.com, www.free-drweb.com, www.drweb-curenet.com, pda.drweb.com, and estore.drweb.com. A copyright notice for Doctor Web 2003-2013 is also present.

Vous pouvez accéder à votre Espace personnel directement depuis le logiciel ou après avoir saisi le numéro de série, sur la page <http://support.drweb.com/get+cabinet+link/>.

Si le numéro de série Dr.Web CureNet! a déjà été enregistré, alors vous avez seulement besoin d'entrer dans votre Espace personnel Dr.Web CureNet! et de télécharger la dernière version du package d'installation.

Pré-requis système

Pour scanner des ordinateurs distants avec Dr.Web CureNet!, il faut satisfaire aux pré-requis suivants :

- les ordinateurs analysés doivent être accessibles via le réseau;
- le compte utilisé par Dr.Web CureNet! pour se connecter aux ordinateurs à scanner doit exister et disposer des droits administrateur;
- sur les machines scannées, les ports 139 et 445 doivent être ouverts.

Pour effectuer un scan antivirus avec l'utilitaire antivirus Dr.Web CureNet! vous devez disposer des droits administrateur sur les postes de travail et les serveurs concernés. L'analyse à distance ne nécessite aucun paramétrage supplémentaire des ordinateurs faisant partie du domaine s'ils tournent sous le compte de l'administrateur du domaine. Dans le cas où un poste distant n'appartient pas au domaine ou fonctionne sous un compte local, sous certaines versions de Windows, un paramétrage supplémentaire du poste sera requis. Les paramètres détaillés de Windows sont décrits dans la rubrique «Pré-requis système» de ce guide. Vous pouvez également consulter les documents vidéo.

Compte tenu du fait que la configuration de l'analyse distante peut affaiblir la sécurité du poste distant, il est fortement recommandé de prendre connaissance des paramètres en question avant d'apporter des modifications dans le système, ou de refuser le scan distant et de réaliser l'analyse antivirus directement sur le poste distant hors du domaine ou sous un compte local.

La configuration de Windows 2000 comprend deux étapes :

1. L'activation du compte administrateur.
2. La configuration des composants réseau.

Important ! Le système doit comporter le Service Pack Update Rollup 4 avec le correctif cumulatif 1.

Téléchargez le Service Pack 4 pour Windows 2000:

<http://www.microsoft.com/ru-ru/download/details.aspx?id=4127>

Télécharger la mise à jour cumulative 1 pour Windows 2000 avec Service Pack 4:

<http://www.microsoft.com/ru-ru/download/details.aspx?id=18997>

1. Activez le compte administrateur.

Cliquez sur le bouton « Démarrer » et sélectionnez → Panneau de configuration → Outils d'administration → Gestion de l'ordinateur → Outils système, puis Utilisateurs et groupes locaux → Utilisateurs.

D'autres manipulations peuvent être effectuées en tant qu'administrateur, mais pour renforcer le niveau de sécurité, il est recommandé de créer un compte administrateur alternatif. Dans la fenêtre de droite, cliquez droit et depuis le menu contextuel, sélectionnez l'élément « Nouvel utilisateur ».

- En tant que nom d'utilisateur, entrez DrWebCurennet
- Dans les champs Mot de passe et Confirmer le mot de passe, entrez un mot de passe complexe.
- Désactivez l'option Changer de mot de passe à la prochaine connexion.
- Activez l'option Mot de passe n'expire jamais.
- Cliquez sur Créer puis sur Fermer.

Avec le bouton gauche de la souris double-cliquez sur le compte créé de DrWebCurennet et allez à l'onglet « Appartenance aux groupe ». Sélectionnez « Utilisateurs » et cliquez sur le bouton « Supprimer ». Puis cliquez sur « Ajouter ». La fenêtre Sélection: Groupes va s'ouvrir, en haut de la fenêtre, sélectionnez l'élément « Administrateurs » puis cliquez sur « Ajouter », ensuite sur OK. Dans la fenêtre « Propriétés de Dr.WebCurennet », cliquez successivement sur les boutons « Appliquer » et OK.

2. Configurez les composants réseau.

Cliquez sur le bouton « Démarrer » et dans le menu « Paramètres », sélectionnez « Réseau » puis « Accès à distance au réseau ». Avec le curseur, sélectionnez la connexion réseau et pressez le bouton droit de la souris. Dans le menu contextuel qui apparaît, sélectionnez l'élément « Propriétés ».

Assurez-vous que les composants suivants sont activés :

- Client pour les réseaux Microsoft
- Service de partage de fichiers et d'imprimantes pour les réseaux Microsoft
- Protocole Internet (TCP / IP)

Cliquez sur le bouton OK.

Si vous utilisez un pare-feu, ouvrez les ports 139 et 445.

La configuration de Windows XP (Windows 2003) se compose de quatre phases :

- L'activation du compte administrateur.
- Configuration du partage de fichiers (ceci n'est pas requis en cas de Windows 2003)
- Configuration de la stratégie de sécurité locale
- Configuration du pare-feu Windows
- La configuration des composants réseau.

Important ! Le système Windows XP doit contenir Service Pack 2 ou 3.

Téléchargez le Service Pack 2 pour Windows XP: <http://www.microsoft.com/ru-ru/download/details.aspx?id=28>

Téléchargez le Service Pack 3 pour Windows XP (recommandé):
<http://www.microsoft.com/ru-ru/download/details.aspx?id=24>

Version prise en charge:

- Windows XP Professionnel

Compte tenu du fait que le lancement de programmes à distance n'est pas pris en charge, les versions suivantes ne sont pas supportées :

- Windows XP Starter
- Windows XP Home Edition

Le système Windows 2003 doit contenir Service Pack 1 ou 2.

Téléchargez le Service Pack 1 pour Windows 2003:
<http://www.microsoft.com/ru-ru/download/details.aspx?id=11435>

Téléchargez le Service Pack 2 pour Windows 2003 (recommandé):
<http://www.microsoft.com/ru-ru/download/details.aspx?id=41>

1. Activez le compte administrateur.

Cliquez sur le bouton « Démarrer » et sélectionnez Panneau de configuration → Outils d'administration → Gestion de l'ordinateur → Outils système, puis Utilisateurs et groupes locaux → Utilisateurs. D'autres manipulations peuvent être effectuées en tant qu'administrateur, mais pour renforcer le niveau de sécurité, il est recommandé de créer un compte administrateur alternatif.

Dans la partie droite de la fenêtre, faites un clic droit. Dans le menu contextuel qui apparaît, choisissez « Nouvel utilisateur ». Entrez le nom d'utilisateur Dr.WebCureNET, dans les champs Mot de passe et Confirmer le mot de passe, entrez un mot de passe complexe. Désactivez l'option « Changer de mot de passe » à la prochaine connexion. Activez l'option « Mot de passe n'expire jamais ». Cliquez sur « Créer » puis sur le bouton « Fermer ». Double-cliquez sur le compte créé DrWebCurenet. La fenêtre « Propriétés DrWebCurenet » apparaît. Allez à l'onglet « Appartenance aux groupes ». Dans la fenêtre « Membre de groupes »: sélectionnez « Utilisateurs » et cliquez sur le bouton « Supprimer ». Puis cliquez sur « Ajouter ». La fenêtre Sélection : Groupes va s'ouvrir. Cliquez sur « Avancé » puis sur « Rechercher ». Dans la liste, sélectionnez « Administrateurs », cliquez sur OK, puis cliquez sur le bouton OK dans la fenêtre « Sélection : Groupes ». Dans la fenêtre « Propriétés : Dr.WebCurenet » cliquez successivement sur Appliquer, puis sur OK.

2. Configurez le partage de fichiers.

Cliquez sur le bouton « Démarrer », allez dans le Panneau de configuration → puis passez à l'affichage classique → Options des dossiers. La fenêtre « Options des dossiers » va s'ouvrir. Passez à l'onglet « Affichage ». Décochez la case « Utiliser le partage de fichiers simple ». Cliquez successivement sur « Appliquer », puis sur OK.

3. Configurer la stratégie de sécurité locale.

Allez au Panneau de configuration → Outils d'administration → Stratégie de sécurité locale → Stratégies locales → Options de sécurité. Placez le curseur sur les Politiques d'accès au réseau: modèle de partage pour les comptes locaux, puis double-cliquez sur le bouton gauche de la souris. La fenêtre « Propriétés » va s'ouvrir. Sélectionnez l'option « Normal ». Cliquez successivement sur « Appliquer », puis sur OK. Quittez les Paramètres de sécurité locaux.

4. Configurez le pare-feu.

Si vous utilisez un pare-feu tiers, ouvrez les ports 139 et 445. Si vous utilisez le pare-feu Windows, procédez comme suit. Cliquez sur le bouton « Démarrer » et passez dans le Panneau de configuration puis cliquez sur → Pare-feu Windows. La fenêtre du Pare-feu Windows va s'ouvrir. Passez à l'onglet « Exceptions ». Activez l'option « Partage de fichiers et imprimantes », cliquez sur le bouton OK.

5. Configurez les composants réseau.

Cliquez sur le bouton « Démarrer » et passer dans le Panneau de configuration puis cliquez sur « Connexions réseau ». Avec le curseur, sélectionnez la connexion réseau et pressez le bouton droit de la souris. Dans le menu contextuel qui apparaît, sélectionnez l'élément « Propriétés ». Une fenêtre permettant de configurer la connexion réseau va s'ouvrir. Cliquez sur l'onglet « Général ».

Assurez-vous que les composants suivants sont activés :

- Client pour les réseaux Microsoft
- Service de partage de fichiers et d'imprimantes pour les réseaux Microsoft
- Protocole Internet (TCP / IP)

Cliquez sur le bouton OK.

La configuration de Windows Vista comprend six étapes :

3. Configuration du contrôle de comptes utilisateur
4. Configuration du partage
5. L'activation du compte administrateur.
6. Configuration du pare-feu Windows
7. La configuration des composants réseau.
8. Configuration de la stratégie de sécurité locale

Important ! Le système doit comporter le Service Pack 1 ou 2.

Téléchargez le Service Pack 1 pour Windows Vista :

<http://www.microsoft.com/ru-ru/download/details.aspx?id=910>

Téléchargez le Service Pack 2 pour Windows Vista (recommandé):

<http://www.microsoft.com/ru-ru/download/details.aspx?id=15278>

Les versions suivantes sont supportées :

- Windows Vista Business
- Windows Vista Entreprise
- Windows Vista Ultimate

Compte tenu du fait que le lancement de programmes à distance n'est pas pris en charge, les versions suivantes ne sont pas supportées :

- Windows Vista Starter
- Windows Vista Home Basic
- Windows Vista Home Premium

1. Si UAC (User Access Control) est activé, vous devez effectuer les étapes suivantes :

- Pressez les touches Windows + R. Dans la fenêtre qui s'ouvre, tapez « Regedit ». La fenêtre de l'éditeur de la base de registre Windows va s'ouvrir.
- Ouvrez la branche [HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Politiques \ System]
- Passez dans la partie droite de la fenêtre de l'éditeur de registre Windows, cliquez droit et dans le menu contextuel, sélectionnez l'option Créer □ Valeur DWORD de 32 bits. Etablissez le nom du paramètre LocalAccountTokenFilter-Policy.
- Double-cliquez sur la nouvelle clé avec le bouton gauche de la souris. La fenêtre Edition du paramètre DWORD apparaît. Etablissez la valeur sur 1, puis cliquez sur OK.
- Fermez l'éditeur de registre.

2. Configurez les paramètres du partage.

Cliquez sur le bouton « Démarrer » et allez dans le panneau de configuration → Réseau et Internet → Centre Réseau et partage → Partage et découverte. Activez les options « Découverte de réseau » et « Partage de fichiers ».

3. Activez le compte administrateur.

Cliquez sur le bouton « Démarrer » et sélectionnez Panneau de configuration → Système et maintenance → Outils d'administration → Gestion de l'ordinateur → Outils système, puis Utilisateurs et groupes locaux → Utilisateurs. D'autres

manipulations peuvent être effectuées en tant qu'administrateur, mais pour renforcer le niveau de sécurité, il est recommandé de créer un compte administrateur alternatif. Dans la fenêtre au milieu, cliquez droit et depuis le menu contextuel, sélectionnez l'élément « Nouvel utilisateur ».

- Entrez le nom d'utilisateur - DrWebCurenet
- Dans les champs Mot de passe et Confirmer le mot de passe, entrez un mot de passe complexe.
- Désactivez l'option Changer de mot de passe à la prochaine connexion.
- Activer l'option Mot de passe n'expire jamais.
- Cliquez sur Créer et puis sur Fermer.

Avec le bouton gauche de la souris double-cliquez sur le compte créé de DrWebCurenet et allez à l'onglet « Appartenance aux groupes ». Sélectionnez « Utilisateurs » et cliquez sur le bouton « Supprimer ». Puis cliquez sur le bouton « Ajouter » pour ouvrir la fenêtre « Sélection: Groupes ». Cliquez sur « Avancé » puis sur « Rechercher ». Dans les résultats de la recherche, cliquez sur « Administrateurs », puis cliquez sur OK. Dans la fenêtre « Sélection : Groupes », cliquez sur OK. Cliquez successivement sur « Appliquer », puis sur OK dans la fenêtre « Propriétés: DrWebCurenet ».

4. Configurez le pare-feu.

Si vous utilisez un pare-feu tiers, ouvrez les ports 139 et 445. Si vous utiliser le pare-feu Windows, procédez comme suit. Cliquez sur le bouton « Démarrer et passez dans le Panneau de configuration → Sécurité → Pare-feu Windows. Cliquez sur le lien « Autoriser un programme via le Pare-feu Windows ». Dans la fenêtre qui apparaît « Paramètre de Pare-feu Windows », cliquez sur l'onglet « Exceptions ». Activez l'option « Partage de fichiers et imprimantes » Cliquez sur le bouton OK.

5. Configurez les composants réseau.

Cliquez sur le bouton « Démarrer » et allez dans le panneau de configuration → Réseau et Internet → Centre Réseau et partage → Gestionnaire de connexions. Placez votre curseur sur une connexion réseau et cliquez sur le bouton gauche de la souris. Dans le menu contextuel qui apparaît, sélectionnez l'élément « Propriétés ». Assurez-vous que les composants suivants sont activés :

- Client pour les réseaux Microsoft
- Service de partage de fichiers et d'imprimantes pour les réseaux Microsoft
- Protocole Internet en version 4

6. Configurez la stratégie de sécurité locale.

Cliquez sur le bouton « Démarrer », sur Panneau de configuration → Système et maintenance → Outils d'administration → Stratégie de sécurité locale → Stratégies locales → Options de sécurité. Sélectionnez avec le curseur la politiques « Accès réseau: modèle de partage pour les comptes locaux ». Double-cliquez dessus avec le bouton gauche de la souris. La fenêtre « Propriétés » va s'ouvrir. Sélectionnez l'élément « Standard », puis cliquez sur OK.

La configuration de Windows 7 (Windows 2008, Windows Server 2008 R2) comprend six étapes:

- Configuration du contrôle de comptes utilisateur
- Configuration du partage
- L'activation du compte administrateur.
- Configuration du pare-feu Windows
- La configuration des composants réseau.
- Configuration de la stratégie de sécurité locale

Important ! Les versions suivantes sont supportées :

- Windows 7 Professionnel
- Windows 7 Entreprise
- Windows 7 Ultimate

Compte tenu du fait que le lancement de programmes à distance n'est pas pris en charge, les versions suivantes ne sont pas supportées :

- Windows 7 Starter
- Windows 7 Édition Familiale Basique
- Windows 7 Édition Familiale Premium

Pour le système Windows 2008, le Service Pack 2 doit être installé.

Téléchargez le Service Pack 2 pour Windows 2008:

<http://www.microsoft.com/ru-ru/download/details.aspx?id=15278>

1. Si UAC (User Access Control) est activé, vous devez effectuer les étapes suivantes :

- Pressez les touches Windows + R. Dans la fenêtre qui s'ouvre, tapez « Regedit ». Une fenêtre de l'éditeur de la base de registre Windows va s'ouvrir.
- Ouvrez la branche [HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Politiques \ System]
- Passez dans la partie droite de la fenêtre de l'éditeur de registre Windows, cliquez droit et dans le menu contextuel, sélectionnez l'option Créer Valeur DWORD de 32 bits. Etablissez le nom du paramètre LocalAccountTokenFilterPolicy.
- Double-cliquez sur la nouvelle clé avec le bouton gauche de la souris. La fenêtre Edition du paramètre DWORD apparaît. Etablissez la valeur sur 1, puis cliquez sur OK.
- Fermez l'éditeur de registre.

2. Configurez les paramètres du partage.

Cliquez sur « Démarrer » et sélectionnez Panneau de configuration → Réseau et Internet → Le Centre Réseau et partage → Modifier les paramètres de partage avancés. Dans le profil réseau approprié, sélectionnez « Activer la découverte de réseau » et « Activer l'accès partagé aux fichiers et aux imprimantes ». Cliquez sur le bouton « Enregistrer les modifications ». Si vous configurez Windows 2008 ou Windows Server 2008 R2, laissez désactivée l'option « Activer la découverte de réseau ».

3. Activez le compte administrateur.

Cliquez sur le bouton « Démarrer » et sélectionnez Panneau de configuration → Système et sécurité → Outils d'administration → Gestion de l'ordinateur → Outils système, puis Utilisateurs et groupes locaux → Utilisateurs. D'autres manipulations peuvent être effectuées en tant qu'administrateur, mais pour renforcer le niveau de sécurité, il est recommandé de créer un compte administrateur alternatif. Dans la fenêtre au milieu, cliquez droit et depuis le menu contextuel, sélectionner l'élément « Nouvel utilisateur ».

Entrez le nom d'utilisateur - DrWebCurenet

- Dans les champs Mot de passe et Confirmer le mot de passe, entrez un mot de passe complexe.
- Désactivez l'option Changer de mot de passe à la prochaine connexion.
- Activer l'option Mot de passe n'expire jamais.
- Cliquez sur Créer et puis sur Fermer.

Avec le bouton gauche de la souris double-cliquez sur le compte créé de DrWebCurenet et allez à l'onglet « Appartenance aux groupes ». Sélectionnez l'élément « Utilisateurs » et cliquez sur le bouton « Supprimer ». Puis cliquez sur le bouton « Ajouter » pour ouvrir la fenêtre « Sélection: Groupes ». Cliquez sur « Avancé » et puis sur « Rechercher ». Dans les résultats de recherche, sélectionnez « Administrateurs » et cliquez sur OK. Dans la fenêtre « Sélection : Groupes », cliquez sur OK. Maintenant, dans la fenêtre « Propriétés: Dr.WebCurenet », cliquez successivement sur « Appliquer », puis sur OK.

4. Configurez le pare-feu.

Si vous utilisez un pare-feu tiers, ouvrez les ports 139 et 445. Si vous utiliser le pare-feu Windows, procédez comme suit. Cliquez sur le bouton « Démarrer », sur Panneau de configuration → Système et sécurité → Pare-feu Windows → Autoriser un programme ou une fonctionnalité via le Pare-feu Windows. Cliquez sur le bouton « Modifier les paramètres ». Activez l'option « Partage de fichiers et imprimantes », cliquez sur OK.

5. Configurez les composants réseau.

Cliquez sur le bouton « Démarrer » et allez dans le panneau de configuration □ Réseau et Internet □ Centre Réseau et partage □ Modifier les paramètres de la carte. Utilisez le curseur pour sélectionner la connexion réseau et cliquez sur le bouton droit de la souris. Dans le menu contextuel qui apparaît, sélectionnez l'élément « Propriétés ». Assurez-vous que les composants suivants sont activés :

- Client pour les réseaux Microsoft
- Service de partage de fichiers et d'imprimantes pour les réseaux Microsoft
- Protocole Internet en version 4 (TCP / IP v4)

6. Configurez la stratégie de sécurité locale.

Cliquez sur le bouton « Démarrer », sur Panneau de configuration → Système et sécurité → Outils d'administration → Stratégie de sécurité locale → Stratégies locales → Options de sécurité. Sélectionnez la politique d'accès au réseau: modèle de partage pour les comptes locaux. Double-cliquez dessus avec le bouton gauche de la souris. La fenêtre « Propriétés » va s'ouvrir. Sélectionnez l'élément « Standard », puis cliquez sur OK.

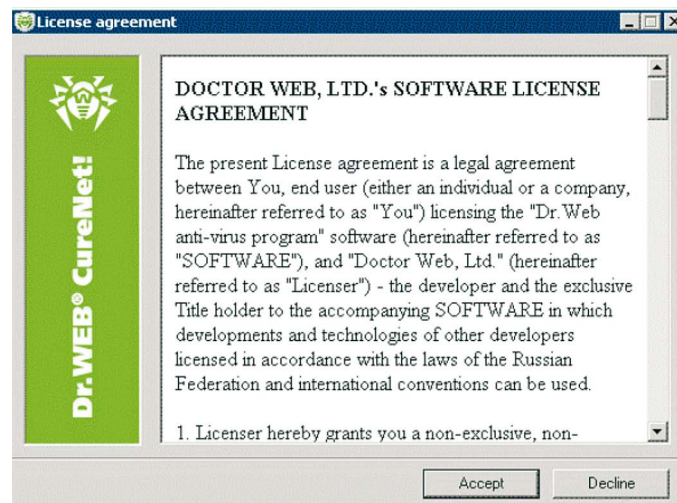
Lancement de Dr.Web CureNet!

1. Lancez le package `CureNet!.exe` que vous avez reçu.

Attention ! La marche à suivre pour les prochains lancements de Dr.Web CureNet! est décrite ci-dessous.

Attention ! Bien que Dr.Web CureNet! soit compatible avec les produits antivirus tiers, il est recommandé, afin d'accélérer le processus de scan, de stopper leur fonctionnement pendant l'activité de Dr.Web CureNet!

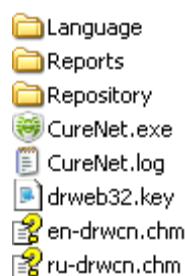
2. Veuillez lire et accepter le contrat de licence en cliquant sur « Accept ».



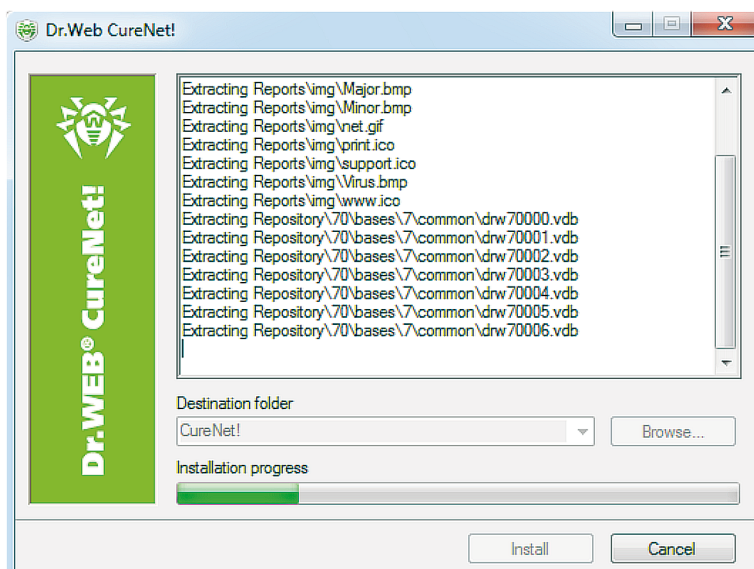
3. Si vous souhaitez enregistrer les fichiers Dr.Web CureNet! dans un autre emplacement que le dossier par défaut, sélectionnez le dossier voulu en cliquant sur « Browse ».


`CureNet!.exe` est une archive auto-extractible, ainsi, le produit ne nécessite pas d'installation. Il vous suffit de choisir l'emplacement vers lequel les fichiers seront extraits de l'archive. Le nom du dossier par défaut est CureNet!, mais vous pouvez spécifier un autre nom. Si vous décompressez le fichier sur une clé USB ou tout autre lecteur similaire, vous aurez toujours Dr.Web CureNet! à portée de main en cas d'urgence.

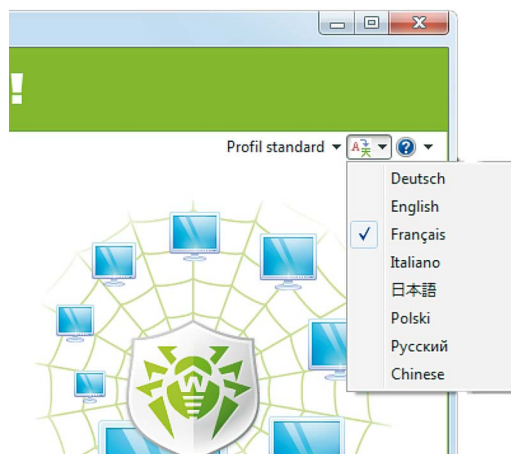
Le dossier créé lors de l'extraction contiendra les fichiers du dépôt de produit et le fichier clé.



Pour continuer l'installation, cliquez sur « Install ».

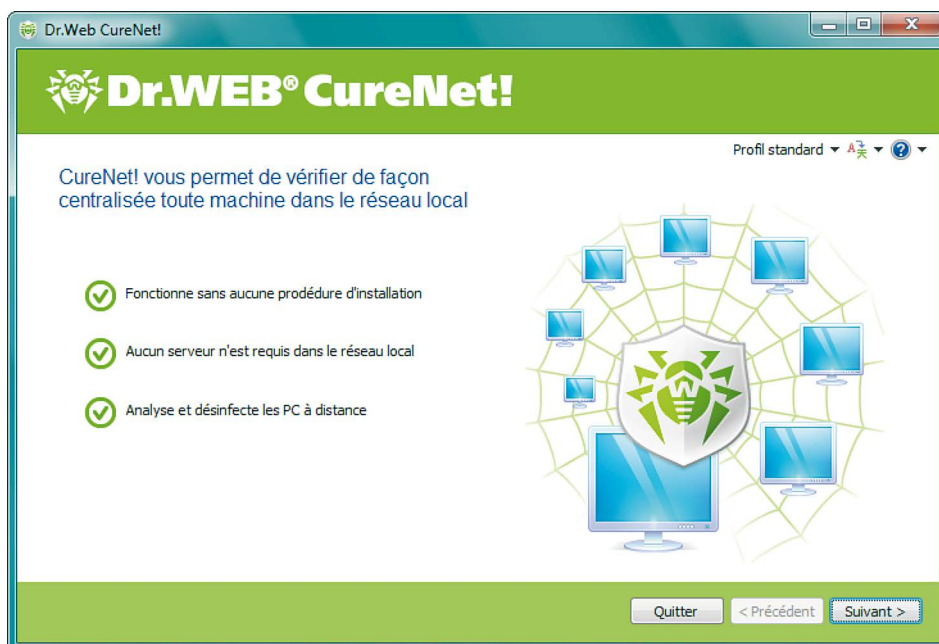



4. Dans la fenêtre qui s'ouvre, vous pouvez sélectionner la langue du logiciel, en appuyant sur  dans le coin supérieur droit.



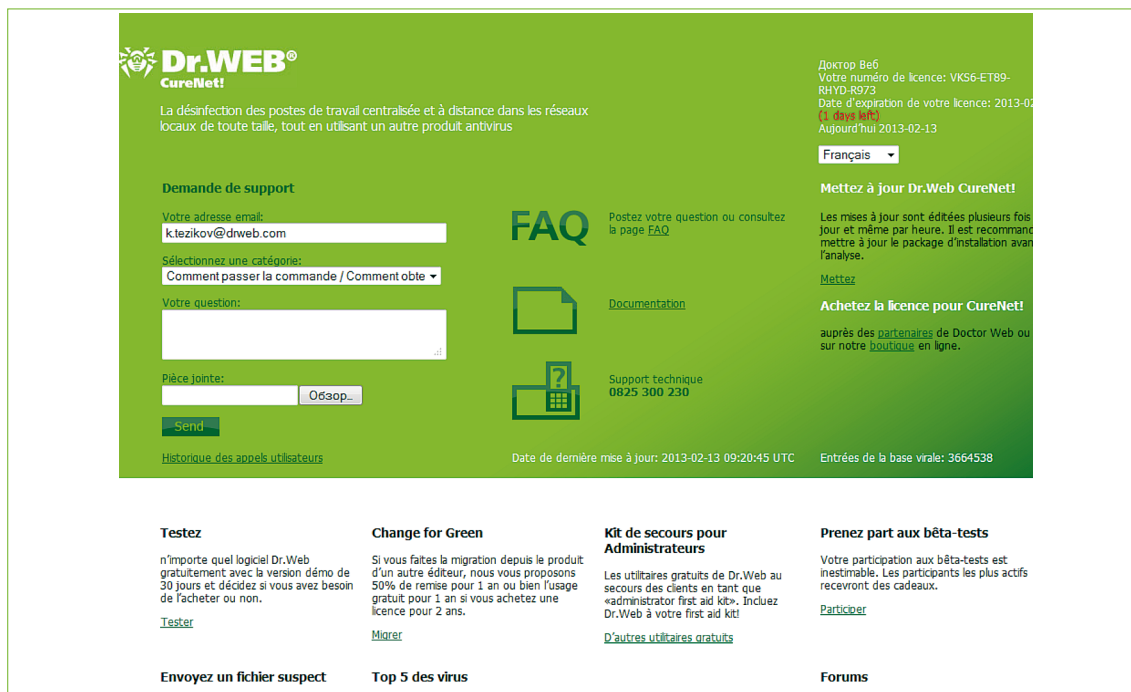
Attention ! Si vous utilisez une version russe du système d'exploitation, assurez-vous que tous les composants nécessaires pour l'affichage de caractères cyrilliques sont installés.

Dans le cas où vous avez précédemment enregistré les paramètres de scan, vous pouvez les télécharger en cliquant sur « Profil standard » dans le coin supérieur droit.



En cas de questions, cliquez sur . Sélectionnez « Aide » dans le menu contextuel si vous souhaitez consulter le Manuel Utilisateur. Si vous sélectionnez Mon Dr.Web, vous entrez dans votre espace personnel, où vous pouvez créer une requête auprès du support technique.

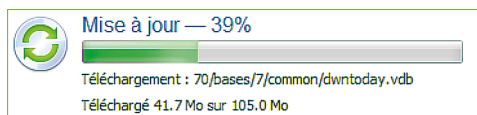
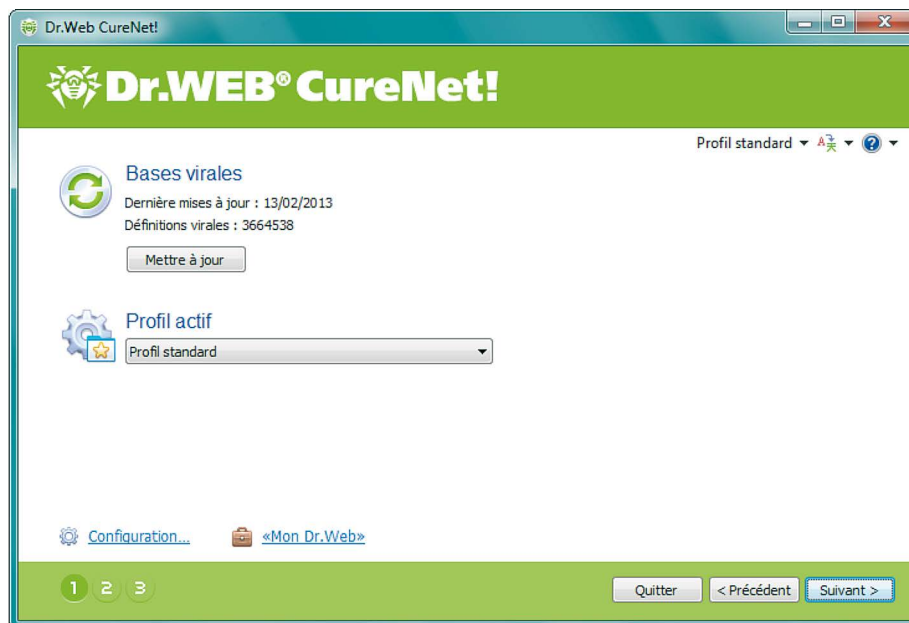
En outre, en cliquant sur « A propos du programme » depuis la même page, vous pouvez afficher des informations sur votre licence.



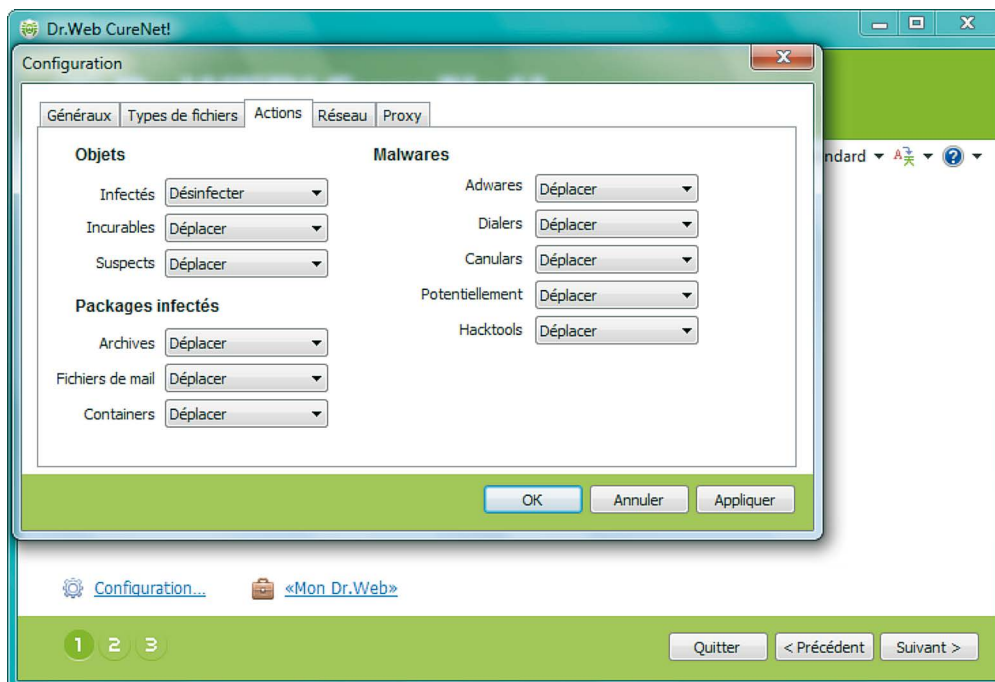
Pour continuer, cliquez sur « Suivant ».

Pour mettre à jour les bases virales, cliquez sur « Mettre à jour ».

Attention ! Le succès de la recherche et de la suppression des virus dépend de la pertinence des bases virales, de ce fait, il est recommandé de procéder à leur mise à jour à chaque démarrage.



Si vous souhaitez changer les paramètres par défaut, cliquez sur « Configuration ».

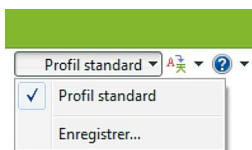


Dans l'onglet « Actions », vous pouvez sélectionner les actions qui seront appliquées à différents types d'objets malveillants. Par défaut, pour la plupart des types d'objets, l'action « Déplacer » est spécifiée.

Il est à noter que la liste d'actions disponibles est fonction du type d'objet. Par exemple, si pour les fichiers contaminés, les actions « Désinfecter », « Supprimer », « Renommer » et « Déplacer » sont applicables, l'action « Désinfecter » n'est pas applicable aux fichiers incurables.

Attention ! Le traitement de nombreux virus nécessite un redémarrage, cependant la case « Redémarrer le poste » n'est pas cochée puisque le redémarrage peut bousculer les utilisateurs. De ce fait, en cas de détection de virus dans le réseau local, il est recommandé d'effectuer son analyse complète et d'en avertir préalablement les utilisateurs.

Pour enregistrer les paramètres configurés, sélectionnez « Profil standard » et dans le menu qui apparaît, sélectionnez « Enregistrer ».



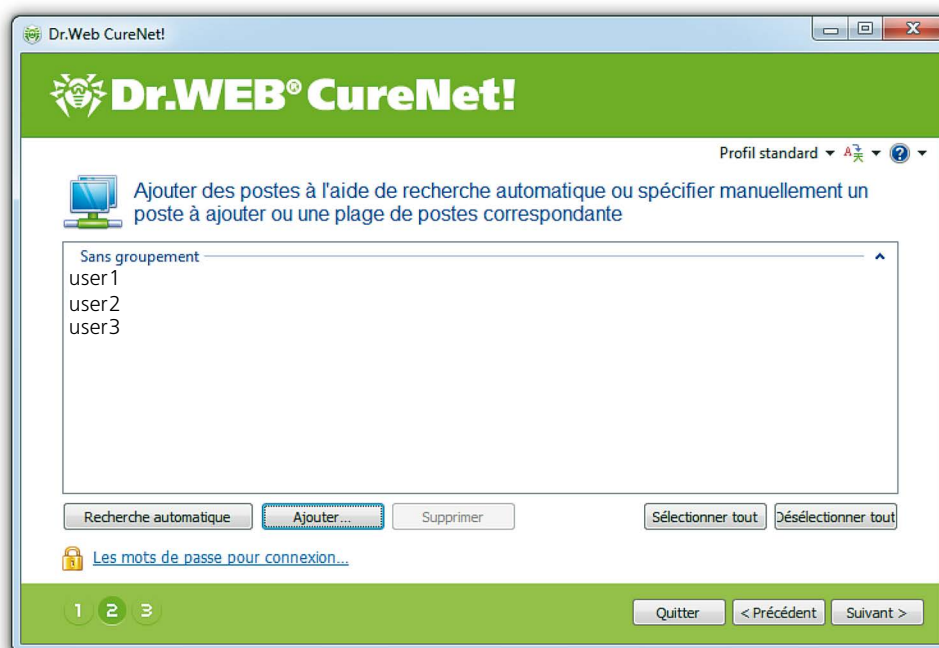
Attention ! Nous vous recommandons d'utiliser les paramètres par défaut, car tous les produits de Doctor Web sont fournis avec les paramètres optimisés pour une utilisation confortable.

Dans le cas où vous avez déjà des profils enregistrés, cliquez sur « Profil actif » et choisissez votre profil.

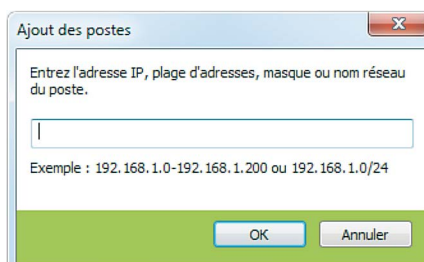


Pour continuer, cliquez sur « Suivant ».

5. Dans la fenêtre qui apparaît, créez une liste de postes sur lesquels vous souhaitez réaliser une analyse antivirus.



Pour rechercher des ordinateurs dans le réseau, cliquez sur « Recherche automatique ». Dans le cas où vous souhaitez créer une liste de manière manuelle, vous pouvez cliquer sur le bouton « Ajouter » et dans la fenêtre qui apparaît, saisissez l'adresse d'un ordinateur particulier ou une plage correspondant au réseau scanné.



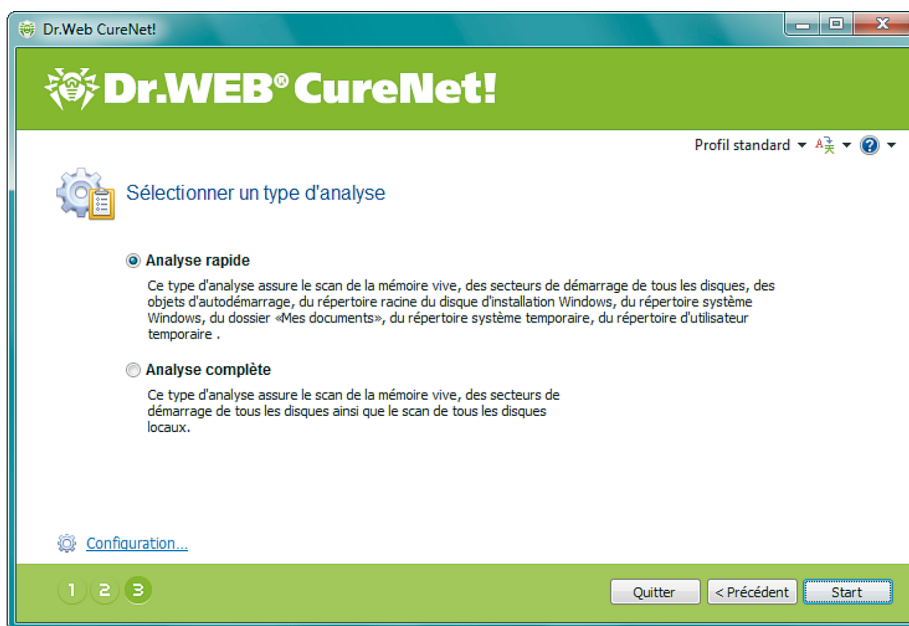
Dans le cas où le réseau scanné n'a pas de structure de domaine, cliquez sur le bouton « Mots de passe » pour vous connecter, puis dans la fenêtre qui apparaît, entrez les mots de passe pour accéder aux postes à scanner.



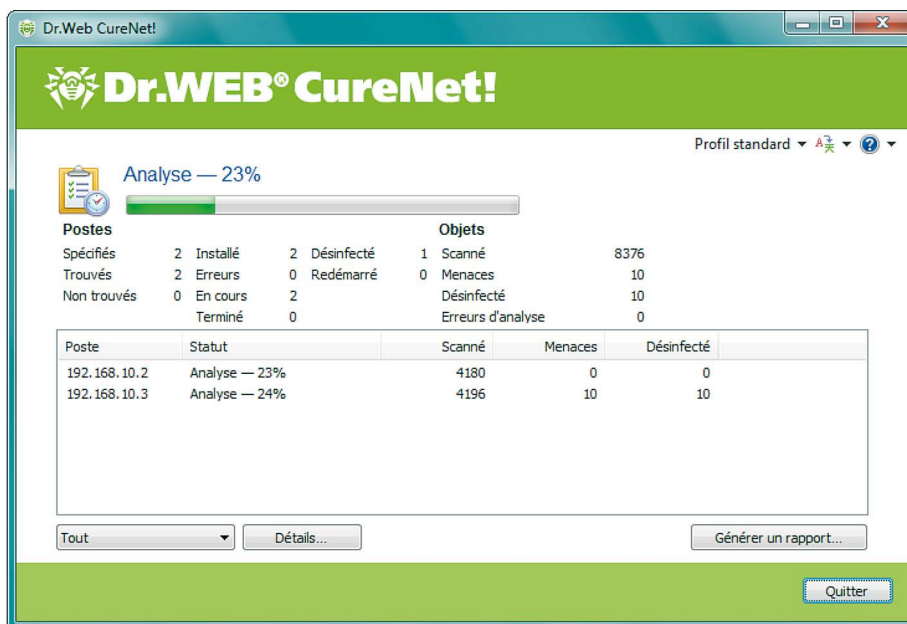
Pour continuer, cliquez sur « Suivant ».

Dans la fenêtre qui apparaît, sélectionnez le type d'analyse - Complète ou Rapide.

Attention ! Lors d'une analyse rapide, seuls les fichiers système et les processus en cours sont analysés, de ce fait, ce type d'analyse ne garantit pas un nettoyage complet de votre ordinateur. En particulier parce que les virus actifs peuvent infecter les fichiers déjà scannés (sains).



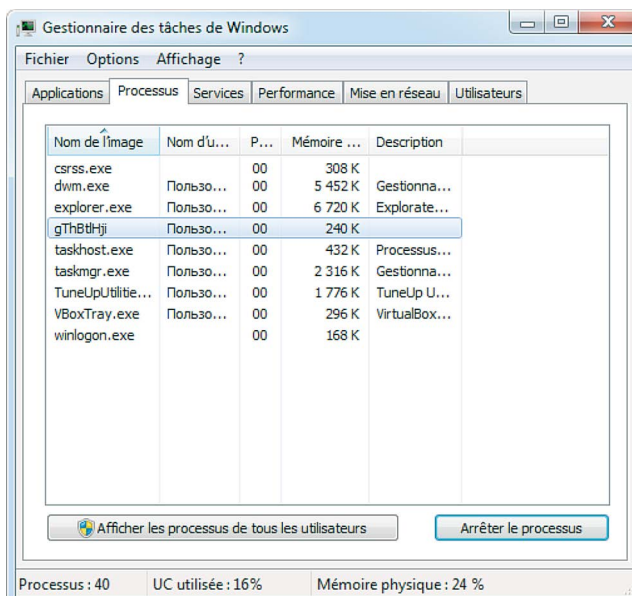
Pour continuer, cliquez sur « Start ».

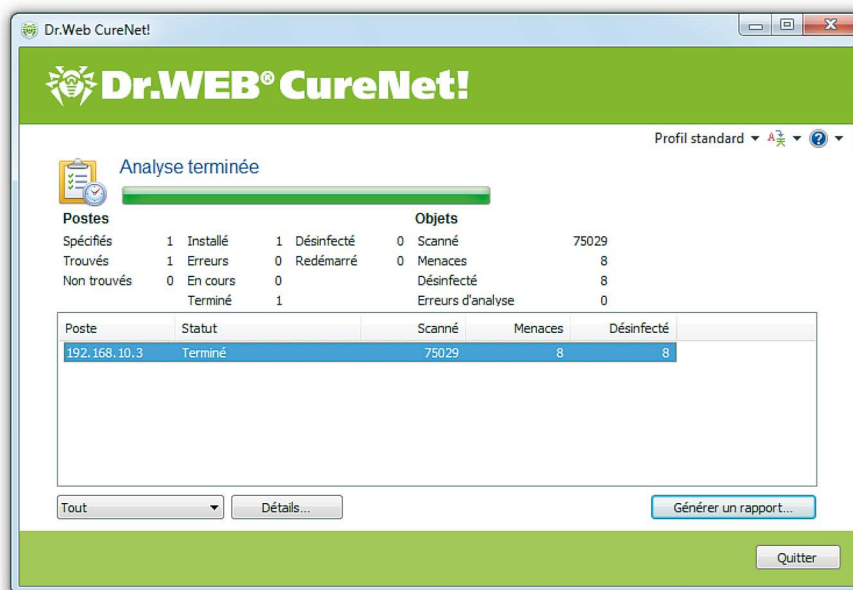


Cette page affiche l'état d'avancement et les résultats de l'analyse sur les ordinateurs distants au sein du réseau. Les statistiques fournies ne dépendent pas de la qualité de la connexion entre les ordinateurs. Même si la connexion est interrompue, Dr.Web CureNet! restaure les statistiques dès que la connexion est rétablie.


Attention ! Il n'est pas recommandé d'interrompre l'analyse.

Les processus en cours utilisent les mécanismes d'autoprotection contre les programmes malveillants.





Vous pouvez générer un rapport sur l'analyse du réseau en cliquant sur le bouton « Générer un rapport ».


[Doctor Web](#)
[Support technique](#)

Analyse rapide

	Scan lancé : 16:55:52 13/02/2013
	Scan arrêté : 17:05:05 13/02/2013

[Imprimer](#)

Postes	Objets
Spécifiés 2 Installé 2 Désinfecté 1 Scanné 8933	
Trouvés 2 Erreurs 0 Redémarré 0 Menaces 10	
Non trouvés 0 En cours 2 Désinfecté 10	
Terminé 0 Erreurs d'analyse 0	

192.168.10.2

192.168.10.3

Objets	Actions	Statistiques
Infectés 10	Désinfectés 1	Scanné 4470
Incurables 0	Supprimés 9	Volume de données (Ko) 1383854
Suspects 0	Déplacés 0	Durée de l'analyse 00:06:17
Adwares 0	Ignorés 0	
Dialers 0		
Canulars 0		
Potentiellement dangereux 0		
Hacktools 0		

Chemin	Objets	Action
C:\Windows\system32\cs-CZ\1.js	Trojan.Browseban.based.2	Désinfecté
C:\Windows\system32\cs-CZ\as.exe	Trojan.Winlock.4128	Désinfecté
C:\Windows\system32\cs-CZ\skype_05102012_image.exe	BackDoor.IRC.NgrBot.146	Désinfecté
C:\Windows\system32\cs-CZ\Trojan.Carberp.276.exe	Trojan.Carberp.276	Désinfecté
C:\Windows\system32\cs-CZ\Trojan.Carberp.30.dat	Trojan.Carberp.30	Désinfecté
C:\Windows\system32\cs-CZ\Trojan.Carberp.647.exe	Trojan.Carberp.647	Désinfecté

Pour terminer, cliquez sur « Quitter ».

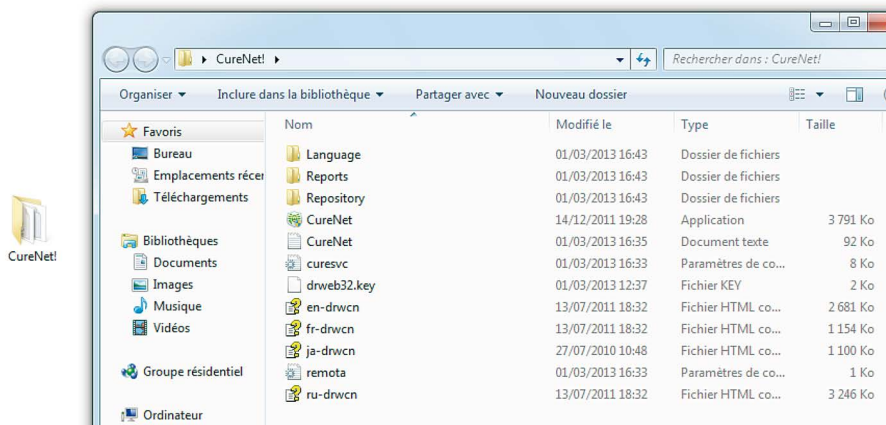
Pour les instructions détaillées sur l'utilisation du produit, les paramètres d'analyse, la création et maintenance de profils, consultez le [Manuel Administrateur Dr.Web CureNet!](#)

Utilisation de Dr.Web CureNet!

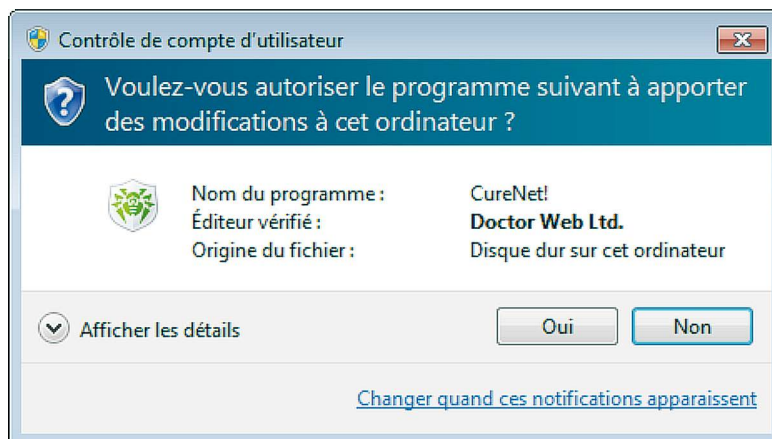
Il est recommandé de réaliser régulièrement une analyse antivirus du système, notamment parce que les fichiers analysés par le moniteur de fichiers et enregistrés sur le disque peuvent contenir des virus inconnus au moment de l'analyse.

Pour effectuer une analyse :

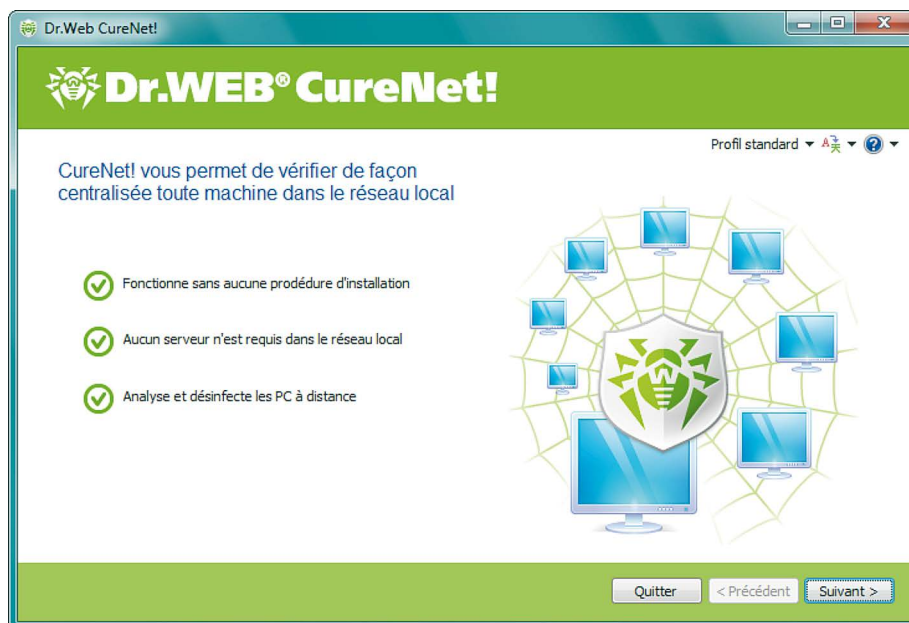
Ouvrez le dossier dans lequel, au cours du premier démarrage, les fichiers Dr.Web CureNet! ont été sauvegardés (par défaut, c'est le dossier CureNet! se trouvant sur le bureau) et lancez le fichier CureNet.



9. Si vous utilisez Windows 7, alors vous aurez à confirmer le lancement du programme en cliquant sur Oui.

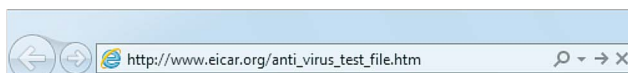


La suite de la procédure ne diffère pas de celle décrite ci-dessus.



Vérification du fonctionnement du produit

10. Pour obtenir un virus de test, ouvrez votre navigateur et allez à l'adresse



1. Sur la page qui s'ouvre, faites défiler vers le bas pour le texte

Download area using the standard protocol http			
eicar.com 68 Bytes	eicar.com.bt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

et sélectionnez l'une des variantes proposées pour télécharger, par exemple, la première – [eicar.com](#).

2. Enregistrez le fichier reçu sur le bureau de l'ordinateur scanné.

Attention ! Si vous utilisez Dr.Web CureNet! en plus des produits antivirus d'autres éditeurs, désactivez les produits tiers avant d'enregistrer le fichier de test.

3. Lancez Dr.Web CureNet! et réalisez une analyse antivirus.



© Doctor Web, 2003–2013



2-12A, 3 ulitsa Yamskogo polya, 125124, Moscou, Russie

Téléphone : +7 (495) 789-45-87 (multi-canal)

Fax : +7 (495) 789-45-97

www.drweb.com

www.freedrweb.com

www.av-desk.com

www.drweb-curenet.com