

Manuel abrégé de configuration et démarrage

0 0



Curenies:

Dru

CureNet!

Coreneer LEBo

Carl

ege votre univers



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 <u>http://products.drweb.com/register/</u>. Après la fin de l'enregistrement, un package d'installation personnalisé sera créé et disponible en téléchargement depuis votre Espace personnel.

Anti-virus	Products Solution	ıs Dr.Web AV-Desk	c Estore Do	ownloads S	Support	Partners	English 🔻
	Registrati	ON SUCCESSFU	or updated. Please,	eted wait a few secon	ıds.		
	Program:	Dr.Web CureNe	t				
	User:	Доктор Веб, k.t	tezikov@drweb.com				
	Status:	Status: building successfully completed (7 seconds elapsed)					
	File size:	109.24M (114,5	543,768b)				
	File MD5:	d8e3b9d075a0	1648b490723892c30	)21e			
	Download: (link valid for 24 ho	ours) CureNet!					
Company   News&Events   Send a	a virus   Online scanner   Privacy	r policy   Site map	More www-re www.av-desk.o www.freedrwel www.drweb-cu	esources: com p b.com e irenet.com	oda.drweb.co store.drweb.	Search .com	<b></b> ←
© Doctor Web 2003 — 2013	Doctor Web is a Russia market leader, Doctor V solutions for businesses international security sl evidence of the comple	n IT-security solutions vendor. I Web was the first vendor to offe s, government entities, and pers tandards. Doctor Web has recei te trust customers have in our p	Dr.Web anti-virus softw. er an anti-virus as a serv sonal use. We have a so ved numerous certificat products.	are has been develor vice in Russia. The o olid record of detect res and awards; our	oped since 19 company also ting malicious satisfied cus	92. The Russian IT offers proven anti- programs, and we tomers spanning th	security services virus and anti-spam adhere to all e globe are clear

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

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

Télécharger la mise à jour cumulative 1 pour Windows 2000 avec Service Pack 4: <u>http://www.microsoft.com/ru-ru/download/details.aspx?id=18997</u>

#### 1. Activez le compte administrateur.

Cliquez sur le bouton « Démarrer » et sélectionnez  $\rightarrow$  Panneau de configuration  $\rightarrow$  Outils d'administration  $\rightarrow$  Gestion de l'ordinateur  $\rightarrow$  Outils système, puis Utilisateurs et groupes locaux  $\rightarrow$  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 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.
- 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 DrWebCurenet et allez à l'onglet « Appartenance aux groupe »s. 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.WebCurenet », 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: <u>http://www.microsoft.com/ru-ru/download/details.aspx?id=28</u>

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): <u>http://www.microsoft.com/ru-ru/download/details.aspx?id=41</u>

#### 1. Activez le compte administrateur.

Cliquez sur le bouton « Démarrer » et sélectionnez Panneau de configuration  $\rightarrow$  Outils d'administration  $\rightarrow$  Gestion de l'ordinateur  $\rightarrow$  Outils système, puis Utilisateurs et groupes locaux  $\rightarrow$  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 sur le bouton OK dans la fenêtre « Sélection : Groupes ».

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

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 \ Policies \ System]
- 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  $\rightarrow$  Réseau et Internet  $\rightarrow$  Centre Réseau et partage  $\rightarrow$  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  $\rightarrow$  Système et maintenance  $\rightarrow$  Outils d'administration  $\rightarrow$  Gestion de l'ordinateur  $\rightarrow$  Outils système, puis Utilisateurs et groupes locaux  $\rightarrow$  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 \ Policies \ 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  $\rightarrow$  Système et sécurité  $\rightarrow$  Pare-feu Windows  $\rightarrow$  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 ».

🤴 Dr.Web CureN	et!		
<b>i</b>	Thank you for purchas CureNet! <sup>TM</sup>	sing Dr.Web®	
VEB® CureNet!	This product allows you to co scans of remote computers w software. Dr. Web CureNet! workstations and servers run Windows® operating system and size. Anti-virus solutions	onfigure and Start a rithout installing ant helps you to cure ning under Microso s in networks of ar of Doctor Web or	anti-virus i-virus off® ny topology other <del>_</del>
5	CureNet!	•	Browse
			biowse
-	Installation progress		
		Install	Cancel
🎯 Dr.Web CureN	et!		
EB® CureNet! 颇	Edracting Reports\img\Major.bmp Extracting Reports\img\Minor.bmp Extracting Reports\img\vint.ico Extracting Reports\img\vint.ico Extracting Reports\img\vinus.bmp Extracting Reports\img\vinus.bmp Extracting Reports\img\vinus.bmp Extracting Repositony\70\bases\7con Extracting Repositony\70\bases\7con Extracting Repositony\70\bases\7con Extracting Repositony\70\bases\7con Extracting Repositony\70\bases\7con Extracting Repositony\70\bases\7con Extracting Repositony\70\bases\7con Extracting Repositony\70\bases\7con	imon\drw70000.vdb imon\drw70001.vdb imon\drw70002.vdb imon\drw70003.vdb imon\drw70005.vdb imon\drw70005.vdb	E
Ň	Destination folder		
	CureNet!	<b></b>	Browse
-	Installation progress		
		Install	Cancel

4. Dans la fenêtre qui s'ouvre, vous pouvez sélectionner la langue du logiciel, en appuyant sur 4 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.

👼 Dr.Web CureNet!	
Or.WEB®CureNet!	
CureNet! vous permet de vérifier de façon centralisée toute machine dans le réseau local Fonctionne sans aucune prodédure d'installation Aucun serveur n'est requis dans le réseau local Analyse et désinfecte les PC à distance	Profil standard * A * * (2) *
	Quitter < Précédent Suivant >

En cas de questions, cliquez sur ② . 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.

et a distance dans les reseaux		Date d'expliation de votre licence, 2013
produit antivirus		(1 days left) Aujourd'hui 2013-02-13
		Français • Mettez à jour Dr.Web CureNet!
FAQ	Postez votre question ou consultez la page <u>FAQ</u>	Les mises à jour sont éditées plusieurs f jour et même par heure. Il est recomm mettre à jour le package d'installation av l'anaixse.
•	Documentation	Mettez
		auprès des <u>partenaires</u> de Doctor Web sur notre <u>boutique</u> en ligne.
?	Support technique 0825 300 230	
Data da damière	mico 3 jour 2012 02 12 00:20:45 UTC	Entráns do hinso visilos 2664529
for Green	Kit de secours pour Administrateurs	Prenez part aux bêta-tests
es la migration depuis le produit éditeur, nous vous proposons mise pour 1 an ou bien l'usage rr 1 an si vous achetez une	Les utilitaires gratuits de Dr.Web au secours des clients en tant que cadministrator first aid kits. Induez	Votre participation aux bêta-tests est inestimable. Les participants les plus acti recevront des cadeaux.
ır 2 ans.	Dr.Web à votre first aid kit!	Participer
	FAQ FAQ Determition Determition for Green to a use pays le produt diffetur, nous schetz une mis pour 1 an ou bien l'usage ri 1 an si vous schetz une ri 2 ans.	FACO       Postez votre question ou consulte page FAO         Image: Postez votre question ou consulte page FAO       Documentation         Image: Postez votre question ou consulte page FAO       Documentation         Image: Postez votre question ou consulte page FAO       Documentation         Image: Postez votre question ou consulte page FAO       Documentation         Image: Postez votre question ou consulte page FAO       Documentation         Image: Postez votre question ou consulte page FAO       Documentation         Image: Postez votre question ou consulte page FAO       Documentation         Image: Postez votre question ou consulte page FAO       Documentation         Image: Postez votre question ou consulte page FAO       Documentation         Image: Postez votre question ou consulte page FAO       Documentation         Image: Postez votre question ou consulte page FAO       Documentation         Image: Postez votre question ou consulte page FAO       Documentation         Image: Postez votre question ou consulte page FAO       Documentation         Image: Postez votre question ou consulte page FAO       Documentation         Image: Postez votre question ou consulte page FAO       Documentation         Image: Postez votre question ou consulte page FAO       Documentation         Image: Postez votre question ou consulte page FAO       Documentation         <

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.



👼 Dr.Web CureNet!	
😻 Dr.WEB° CureNet!	
Bases virales Dernière mises à jour : 13/02/2013 Définitions virales : 3664538	Profil standard ▼ 🐴 ▼ 🕢 ▼
Mettre à jour Profil actif	
🔅 Carfourting - 🚔 allas Dellaha	
	Quitter < Précédent Suivant >
Mico à jour 20%	

Téléchargement : 70/bases/7/common/dwntoday.vdb

Téléchargé 41.7 Mo sur 105.0 Mo

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

👼 Dr.Web CureNe	ti se	_ <b>X</b>
Configuration		
Généraux Type	s de fichiers Actions Réseau Proxy	
Objets	Malwares	ndard 🔻 👫 👻 🕜 👻
Infectés	Désinfecter   Adwares Déplacer	
Incurables	Déplacer	
Suspects	Déplacer   Canulars Déplacer	
Packages i	nfectés Potentiellement Déplacer	
Archives	Déplacer	
Fichiers de mail	Déplacer 🔻	
Containers	Déplacer 🔻	
	OK Annuler Appliquer	
L		J
Orfigura	Etion 🧧 «Mon Dr.Web»	
123	Quitter	écédent Suivant >

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 ».

	Profil standard 🔻 ≩ 🔻 🕜 🔻
$\checkmark$	Profil standard
	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.

São.	Profil actif	
2	Profil standard 🔹	
	Profil standard	i

Pour continuer, cliquez sur « Suivant ».

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

😽 Dr.Web CureNet!
🔅 Dr.WEB° CureNet!
Profil standard 🔻 🐴 👻 🔞 💌
Ajouter des postes à l'aide de recherche automatique ou spécifier manuellement un poste à ajouter ou une plage de postes correspondante
Sans groupement
user I user 2
user3
Recherche automatique         Ajouter         Supprimer         Sélectionner tout         Désélectionner tout
Es mots de passe pour connexion
1 2 3 Quitter < Précédent Suivant >

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.

jout des postes
Entrez l'adresse IP, plage d'adresses, masque ou nom réseau du poste.
Exemple : 192.168.1.0-192.168.1.200 ou 192.168.1.0/24
OK Annuler

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.



Comptes et mots de passe
Spécifier le login/mot de passe administrateur pour accéder aux postes distants
Nom d'utilisateur :
Mot de passe :
Afficher le mot de passe Ajouter Modifier Supprimer
Fermer

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).

Ø Dr.Web CureNet!	
🎯 Dr.WEB° CureNet!	
	Profil standard 🔻 🥀 👻 🕐 👻
Sélectionner un type d'analyse	
Analyse rapide     Analy	
Ce type d'analyse assure le scan de la mémoire vive, des secteurs de démarrage objets d'autodémarrage, du répertoire racine du disque d'installation Windows, du Windows, du dossier «Mes documents», du répertoire système temporaire, du ré temporaire .	de tous les disques, des u répertoire système pertoire d'utilisateur
Analyse complète	
Ce type d'analyse assure le scan de la mémoire vive, des secteurs de démarrage de tous les disques ainsi que le scan de tous les disques locaux.	
<u>Configuration</u>	
123	Quitter < Précédent Start

Pour continuer, cliquez sur « Start ».



Ana	lyse	e — 23%							
Postes						Objets			
Spécifiés	2	Installé	2	Désinfecté	1	Scanné		8376	
Irouvés	2	Erreurs	0	Redémarré	0	Menaces		10	
von trouves	0	En cours Terminé	0			Erreurs d'anal	vse	10	
Poste		Statut				Scanné	Menaces	Désinfecté	
192.168.10.2		Analyse — 2	3%			4180	0	0	
192.168.10.3		Analyse - 2	4%			4196	10	10	
92.168.10.3		Analyse — 2	4%			4196	10	10	

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.

plications Proce	ssus Services	Per	formance	Mise	en réseau	Utilisateurs	
Nom de l'image	Nom d'u	P	Mémoire .		Description		
csrss.exe dwm.exe	Пользо	00	308 5 452	K K	Gestionna		
explorer.exe	Пользо	00	6 720	к	Explorate		
gThBtlHji	Пользо	00	240	к			
taskhost.exe	Пользо	00	432	К	Processus		
taskmgr.exe	Пользо	00	2 316	К	Gestionna		
TuneUpUtilitie	Пользо	00	1 776	К	TuneUp U		
VBoxTray.exe	Пользо	00	296	К	VirtualBox		
winlogon.exe		00	168	К			
Afficher I	es processus de	tous	les utilisate	urs		Arrêter le p	processus



	Aly St	, termines			_					
Postes						Objets				
Spécifiés	1	Installé	1	Désinfecté	0	Scanné		75029		
Trouves	1	Erreurs	0	Redemarre	0	Menaces		8		
Non trouves	U	En cours Terminé	1			Erreurs d'analys	•	8		
Poste		Statut	-			Scanné	Menaces	D	ésinfecté	
192 168 10 3		Terminé				75029	8		8	
192110011010		- Contribution				10020				

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



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 <u>Manuel Administrateur Dr.Web CureNet!</u>



## **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.

	CureNet! > +				
Organiser 👻	Inclure dans la bibliothèque 👻 🛛 Partage	er avec 🔻 Nouveau dossier	000		
🔶 Favoris	Nom	Modifié le	Туре	Taille	
📃 Bureau	🔒 Language	01/03/2013 16:43	Dossier de fichiers		
🔛 Emplacen	nents récer 🛛 🔒 Reports	01/03/2013 16:43	Dossier de fichiers		
🚺 Télécharg	ements 🔒 Repository	01/03/2013 16:43	Dossier de fichiers		
	🛞 CureNet	14/12/2011 19:28	Application	3 791	
🔚 Bibliothèqu	es CureNet	01/03/2013 16:35	Document texte	92	
Documen	ts 🖉 curesvc	01/03/2013 16:33	Paramètres de co	8	
🔚 Images	drweb32.key	01/03/2013 12:37	Fichier KEY	2	
a) Musique	😭 en-drwcn	13/07/2011 18:32	Fichier HTML co	2 681	
Vidéos	😭 fr-drwcn	13/07/2011 18:32	Fichier HTML co	1 154	
	👔 ja-drwcn	27/07/2010 10:48	Fichier HTML co	1 100	
🔣 Groupe rési	dentiel 👔 remota	01/03/2013 16:33	Paramètres de co	1	
	😵 ru-drwcn	13/07/2011 18:32	Fichier HTML co	3 246	

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

🛞 Contrôle de d	compte d'utilisateur	<b>×</b>				
Voule des m	z-vous autoriser le pro odifications à cet ordin	ogramme suivant à apporter nateur ?				
<b>*</b>	Nom du programme : Éditeur vérifié : Origine du fichier :	CureNet! <b>Doctor Web Ltd.</b> Disque dur sur cet ordinateur				
Afficher le	s détails	Oui Non				
	Changer quand ces notifications apparaissent					

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



© Dr.Web CureNet!	
CureNet! vous permet de vérifier de façon centralisée toute machine dans le réseau local	Profil standard * A <sup>*</sup> <sub>A</sub> * @ *
	Quitter < Précédent Sulvant >

#### Vérification du fonctionnement du produit

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

(	Attp://www.eicar.org/anti virus test file.htm	$Q \rightarrow X$
	· · · · · · · · · · · · · · · · · · ·	*

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

	Download area usi	ng the standard protocol http	1
<u>eicar.com</u>	eicar.com.txt	<u>eicar_com.zip</u>	eicarcom2.zip
68 Bytes	68 Bytes	184 Bytes	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

www.drweb-curenet.com



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