



Dr.WEB®

CureNet!

Proteggi ciò che crei

Guida all'avvio rapido

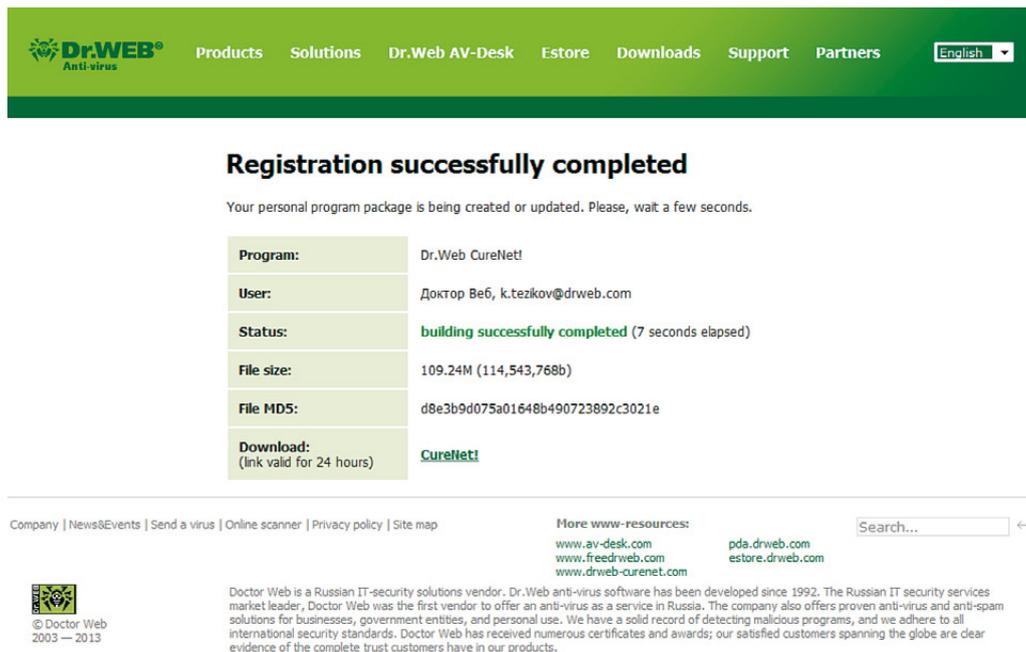


Tramite Dr.Web CureNet! si possono eseguire scansioni antivirali centralizzate di una rete locale senza installare il programma sui computer da controllare. Dr.Web CureNet! può scansionare postazioni e server Microsoft Windows nelle reti locali di qualsiasi topologia.

Attenzione! Dr.Web CureNet! non è progettato per una protezione continua della rete locale o dei singoli computer poiché tra una scansione e un'altra, elaboratori potrebbero essere infettati da vari programmi malevoli. Per proteggere computer della rete locale in modo sicuro, si consiglia di utilizzare Dr.Web Security Space Pro o Dr.Web Enterprise Security Suite.

Ricevere una copia di Dr.Web CureNet!

Per ricevere una copia del programma, è necessario registrare un numero di serie sulla pagina <http://products.drweb.com/register/>. Portata a termine la registrazione, viene generata una copia individuale del programma che può essere scaricata dall'Area personale dell'utente.



The screenshot shows the Dr.Web website navigation bar with links for Products, Solutions, Dr.Web AV-Desk, Estore, Downloads, Support, and Partners. Below the navigation bar, a green banner displays the message "Registration successfully completed". A table provides registration 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), and Download (CureNet! link valid for 24 hours). The footer contains company information, a search bar, and a disclaimer about Dr.Web's history and security standards.

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!

Si può accedere all'Area personale dal programma o sulla pagina <http://support.drweb.com/get+cabinet+link/> dopo aver inserito il numero di serie.

Se il numero di serie di Dr.Web CureNet! è già stato registrato, tutto quello che si deve fare è entrare nell'Area personale e scaricare la versione attuale di Dr.Web CureNet!

Requisiti di sistema

Per scansionare computer remoti tramite Dr.Web CureNet!, è necessario osservare i seguenti requisiti:

- i computer da scansionare devono essere accessibili via rete;
- l'account utilizzato dal programma Dr.Web CureNet! per connettersi ai computer da scansionare deve esistere e possedere privilegi di amministratore necessari;
- sui computer da scansionare devono essere aperte le porte 139 e 445.

Per eseguire una scansione con l'utility antivirale Dr.Web CureNet!, è necessario avere privilegi di amministratore sulle workstation e sui server da scansionare. La scansione remota non richiede alcuna configurazione aggiuntiva dei computer se essi fanno parte del dominio e se su di essi si usa l'account di amministratore di dominio. In caso di alcune versioni di Windows, è necessaria una configurazione aggiuntiva della macchina remota da scansionare, se essa non fa parte del dominio o se su di essa si usa un account locale. La descrizione dettagliata delle impostazioni del sistema operativo Windows è riportata nella sezione "Requisiti di sistema" di questa guida. Inoltre, si possono guardare i video tutorial.

Le impostazioni necessarie per la scansione remota potrebbero abbassare il livello di sicurezza del computer remoto. Pertanto, prima di apportare modifiche alla configurazione, si raccomanda vivamente di informarsi sullo scopo delle suddette impostazioni o di non usare la scansione remota e di eseguire invece un controllo antivirale direttamente sulla macchina remota fuori dominio o con utilizzo dell'account locale.

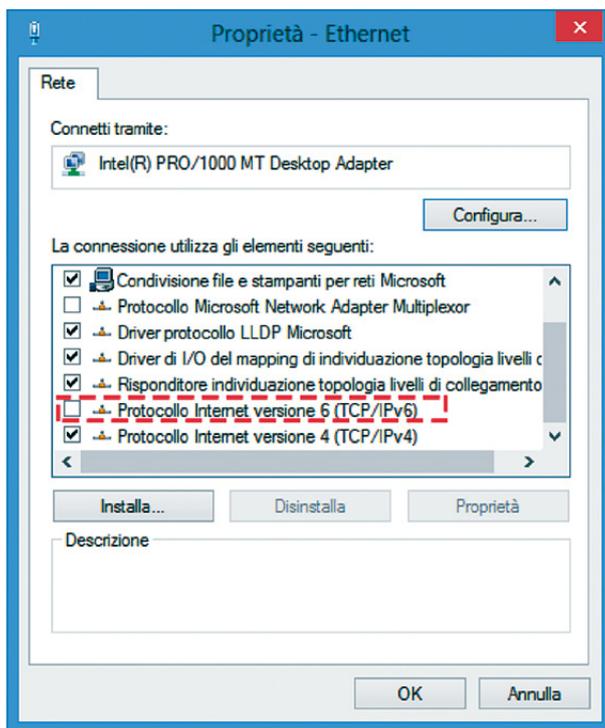
Configurare Windows per avviare la Procedura guidata

La Procedura guidata che fa parte del programma Dr.Web CureNet! può funzionare nelle seguenti versioni del sistema operativo Windows:

- Windows 2000 (Professional, Server, Advanced Server, Datacenter Server)
- Windows XP (Starter, Professional, Home Edition, Media Center Edition)
- Windows Server 2003 (Standard Edition, Enterprise Edition, 64-Bit Enterprise Edition, Datacenter Edition)
- Windows Vista (Starter, Home Basic, Home Premium, Business, Ultimate, Enterprise)
- Windows Server 2008 (Standard Edition, Enterprise Edition, Datacenter Edition)
- Windows 7 (Starter, Home Basic, Home Premium, Professional, Ultimate, Enterprise)
- Windows Server 2008 R2 (Standard, Enterprise, Datacenter)
- Windows 8, Windows 8 Professional
- Windows Server 2012 (Foundation, Essential, Standard, Datacenter)

Per il normale funzionamento della Procedura guidata, sono necessarie due condizioni:

1. Assenza dei caratteri dell'alfabeto nazionale nel percorso alla directory di Dr.Web CureNet!
2. Se la Procedura guidata viene avviata in Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, è necessario disattivare il protocollo IPv6 nelle impostazioni della scheda di rete. Per fare questo, cliccare sul pulsante Start e selezionare dal menu la voce **Pannello di controllo** → **Rete e Internet** → **Centro connessioni di rete e condivisione** → **Modifica impostazioni scheda**. Con il cursore, selezionare la connessione di rete e premere il pulsante destro del mouse. Si apre un menu contestuale da cui selezionare la voce **Proprietà**. Deselezionare il flag accanto a **"Protocollo Internet versione 6"**.

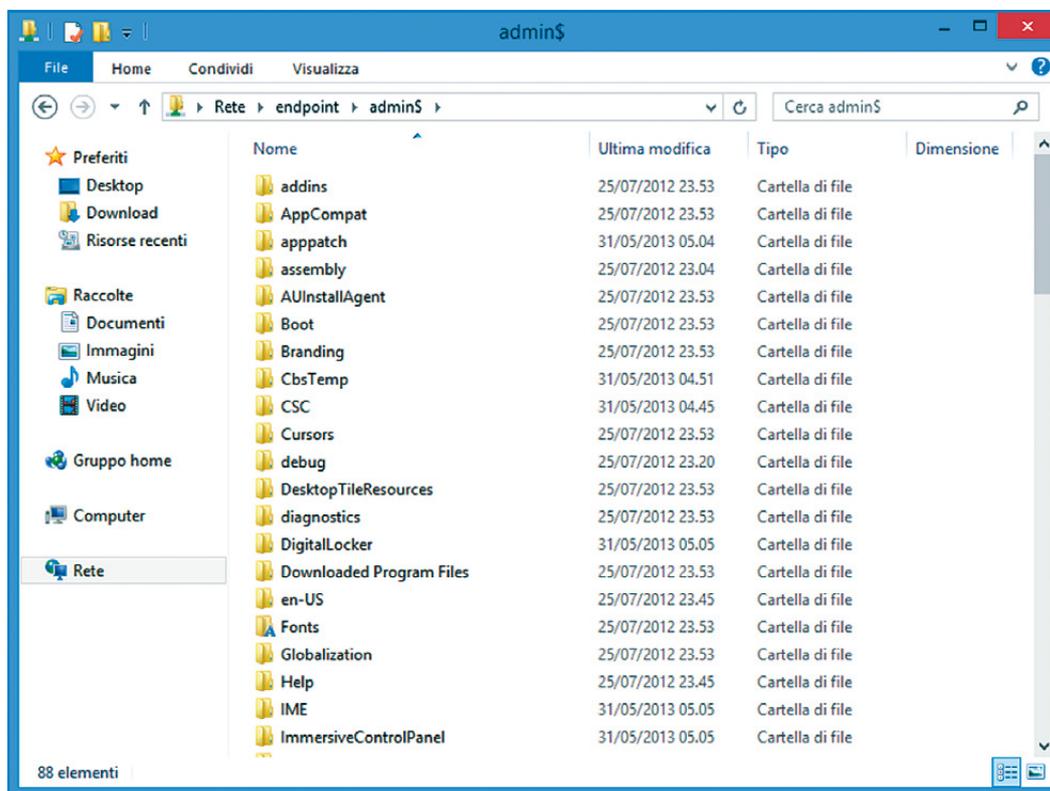


Cliccare sul pulsante **OK**.

Configurare Windows per avviare Scanner Dr.Web su remoto

Impostazioni generali per Windows 2000 – 8, Windows Server 2003/2008/2012

Assicurarsi che sul computer siano accessibili le risorse di amministrazione generali. Per fare questo, andare alla cartella condivisa admin\$ sul computer remoto. A seconda delle impostazioni di Windows, potrebbe essere necessario inserire login e password per l'autorizzazione come amministratore. Di conseguenza dovrebbe aprirsi la cartella di rete (vedi figura sotto).



Se le risorse di amministrazione generali non sono accessibili, fare le seguenti impostazioni sul computer. Aprire l'editor del registro di sistema, poi aprire il ramo

```
[HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\LANMANSERVER\PARAMETERS]
```

Creare un valore **DWORD (32 bit) AutoShareWks**, impostare uno nel campo **Dati valore**. Riavviare il computer. Le risorse di amministrazione generali diventeranno attive.

Configurare Windows 2000

1. Attivare l'account di amministratore.
2. Configurare i componenti di rete.

Importante! Il sistema operativo deve contenere il Service Pack 4 con il pacchetto cumulativo di aggiornamenti 1.

Il Service Pack 4 per Windows 2000 si può scaricare da:

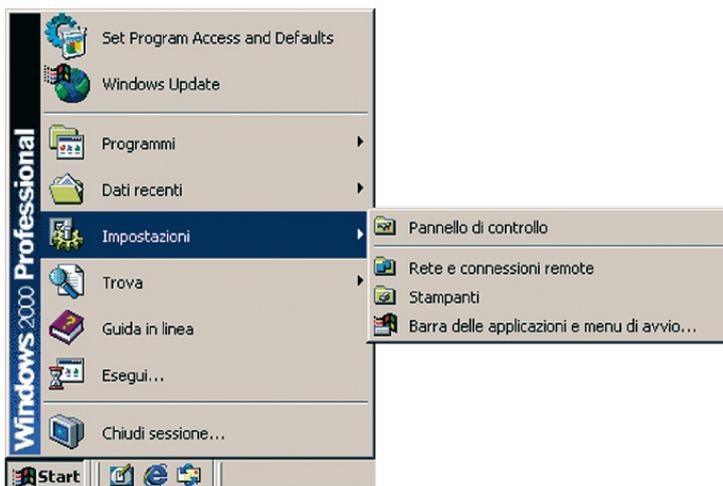
<http://www.microsoft.com/ru-ru/download/details.aspx?id=4127>

Il pacchetto cumulativo di aggiornamenti 1 per Windows 2000 con il Service Pack 4 si può scaricare da:

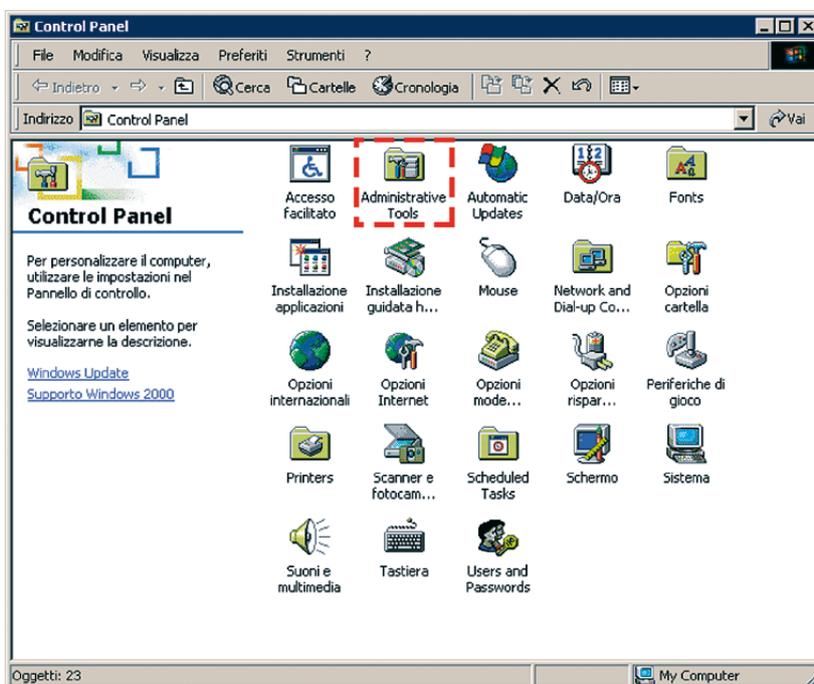
<http://www.microsoft.com/ru-ru/download/details.aspx?id=18997>

1. Attivare l'account di amministratore.

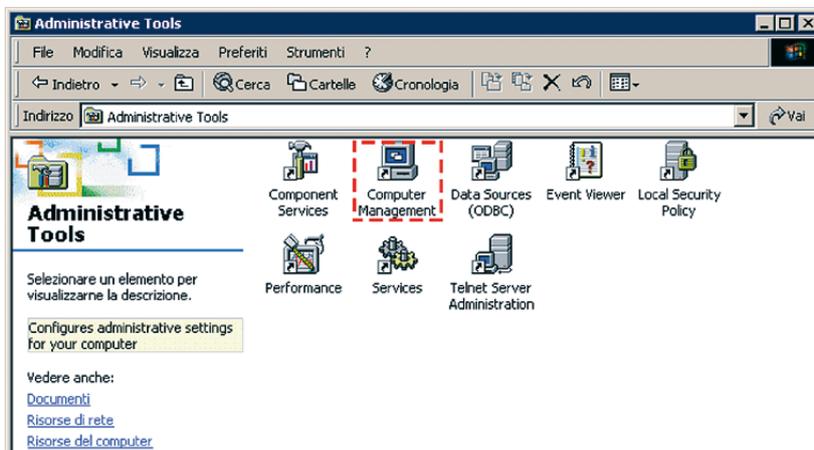
Cliccare sul pulsante Start e passare nel menu a **Impostazioni** → **Pannello di controllo**



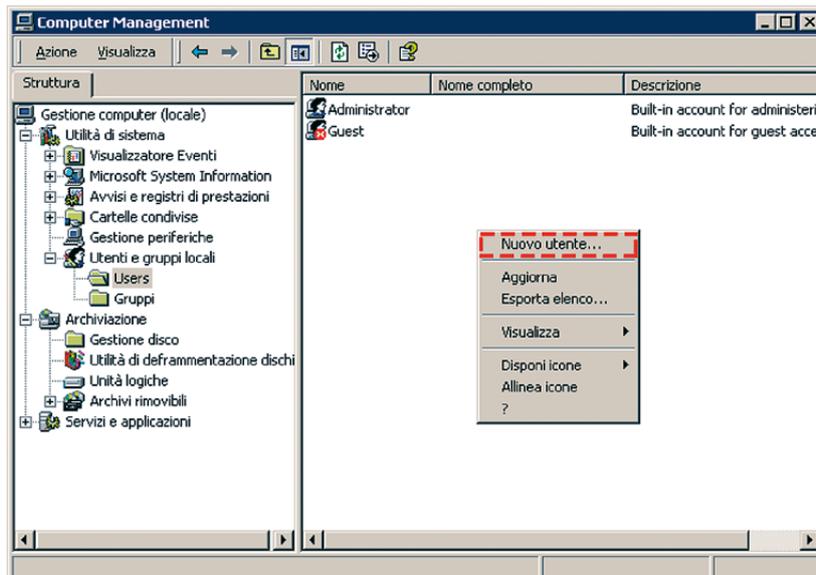
→ Amministrative tools



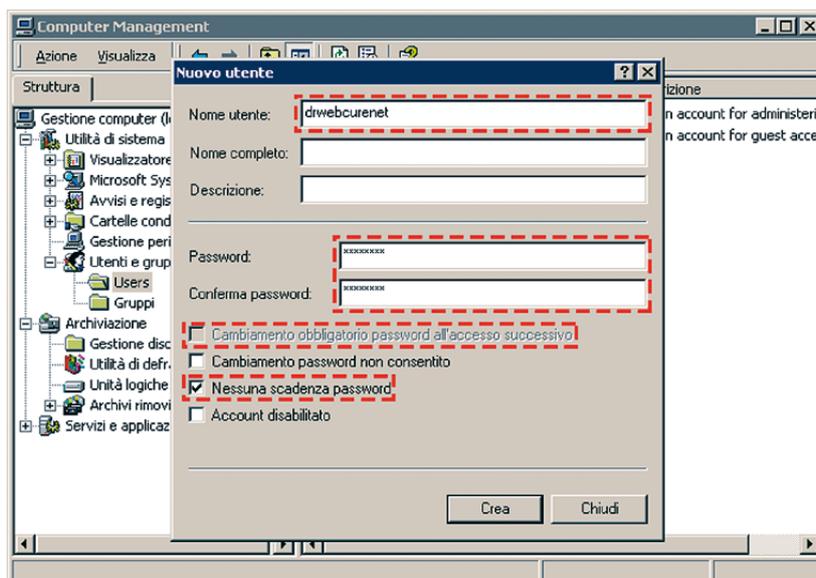
→ Computer Management



→ **Utenti e gruppi locali** → **Users**. Le azioni successive si possono eseguire anche utilizzando l'account Amministratore predefinito, ma al fine di aumentare la riservatezza, si consiglia di creare un altro account di amministratore. Per fare questo, nella finestra destra, premere il tasto destro del mouse e selezionare la voce **Nuovo utente** dal menu contestuale.

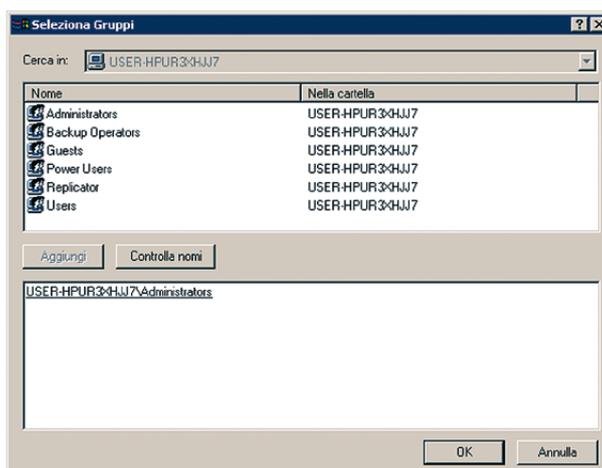


Nel campo **Nome utente** digitare DrWebCurenent. Nei campi **Password** e **Conferma password** impostare una password complessa. Disabilitare l'opzione **Cambiamento obbligatorio password all'accesso successivo**. Abilitare l'opzione **Nessuna scadenza password**.



Cliccare consecutivamente sui pulsanti **Crea** e **Chiudi**. Con il tasto sinistro del mouse fare doppio clic sull'account **DrWeb-Curenent** creato e andare alla scheda **Membro di**. Selezionare **Users** e cliccare su **Rimuovi**.

Quindi cliccare sul pulsante **Aggiungi**. Si apre la finestra **Seleziona gruppi**, nella parte superiore della quale, selezionare con il cursore del mouse la voce **Administrators** e cliccare sul pulsante **Aggiungi**, quindi sul pulsante **OK**.

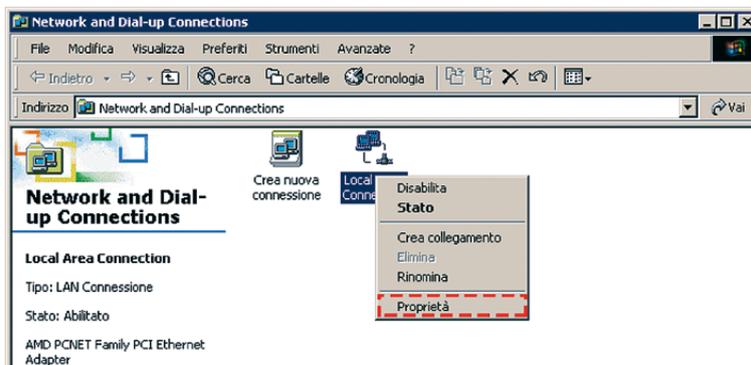


Nella finestra **Proprietà — DrWebCurenet**, cliccare consecutivamente su **Applica** e **OK**. Chiudere lo snap-in **Computer Management**.

2. Configurare i componenti di rete.

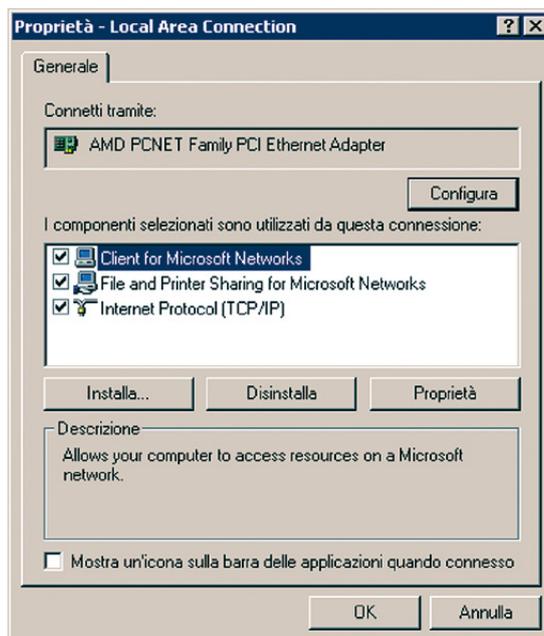
Cliccare sul pulsante **Start** e andare a **Impostazioni → Network e Dial-up Connections**.

Selezionare con il cursore del mouse la connessione di rete e premere il tasto destro del mouse. Viene visualizzato un menu contestuale da cui selezionare **Proprietà**.



Assicurarsi che siano attivati i seguenti componenti:

- Client for Microsoft Networks
- File and Printer Sharing for Microsoft Networks
- Internet Protocol (TCP/IP)



Fare clic sul pulsante **OK**. Se si usa il firewall, aprire le porte 139 e 445.

Configurare Windows XP e Windows Server 2003

1. Attivare l'account di amministratore
2. Configurare la condivisione di file (non è richiesto in caso di Windows 2003)
3. Configurare criteri di protezione locali
4. Configurare il firewall di Windows
5. Configurare i componenti di rete

Importante! Il sistema operativo Windows XP deve contenere i Service Pack 2 o 3.

Il Service Pack 2 per Windows XP si può scaricare da:
<http://www.microsoft.com/ru-ru/download/details.aspx?id=28>

Il Service Pack 3 per Windows XP (consigliato) si può scaricare da:
<http://www.microsoft.com/ru-ru/download/details.aspx?id=24>

Edizioni supportate:

- Windows XP Professional

Edizioni non supportate:

- Windows XP Starter
- Windows XP Home Edition

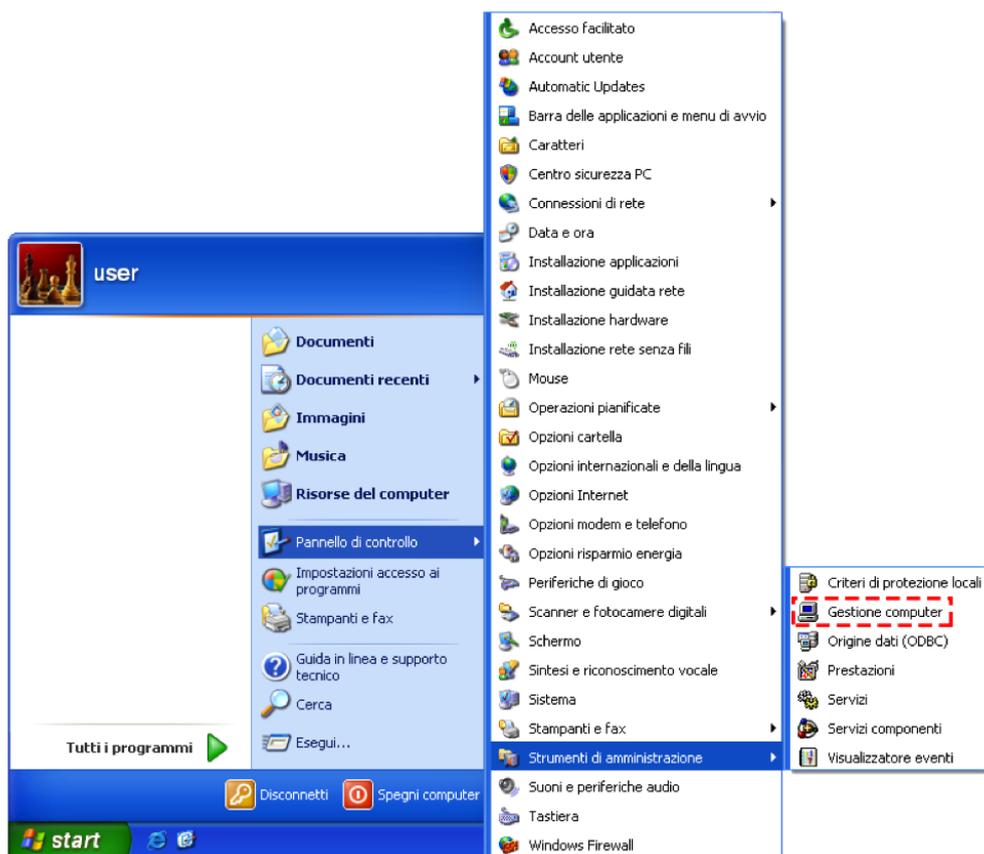
Il sistema operativo Windows 2003 deve contenere i Service Pack 1 o 2.

Il Service Pack 1 per Windows 2003 si può scaricare da:
<http://www.microsoft.com/ru-ru/download/details.aspx?id=11435>

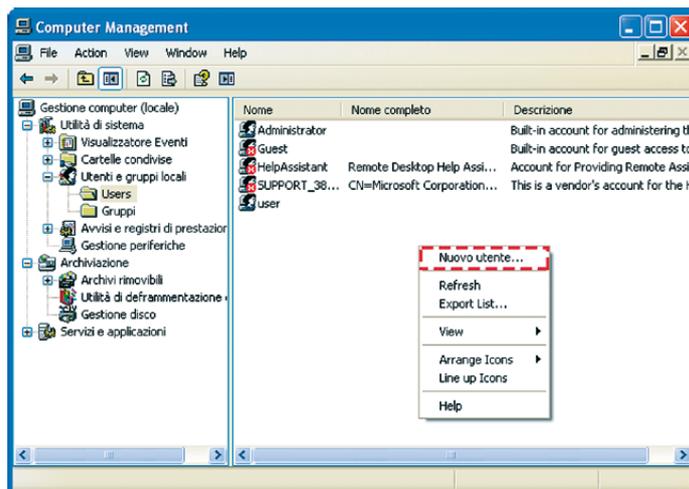
Il Service Pack 2 per Windows 2003 (consigliato) si può scaricare da:
<http://www.microsoft.com/ru-ru/download/details.aspx?id=41>

1. Attivare l'account di amministratore.

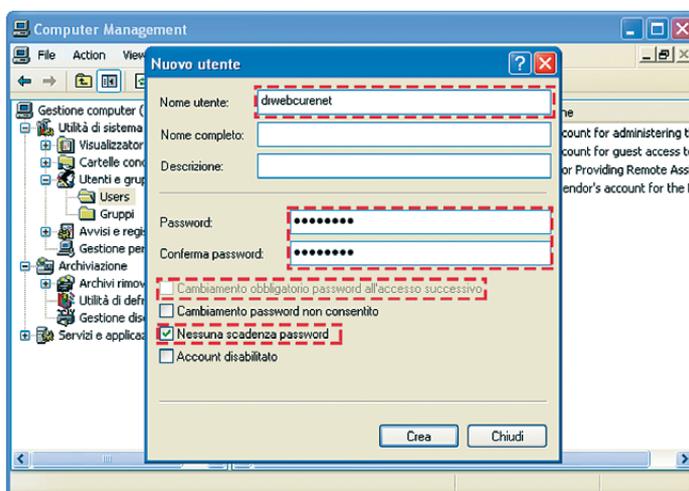
Cliccare sul pulsante **Start** e passare nel menu a **Pannello di controllo** → **Strumenti di amministrazione** → **Gestione computer** → **Utenti e gruppi locali** → **Utenti**.



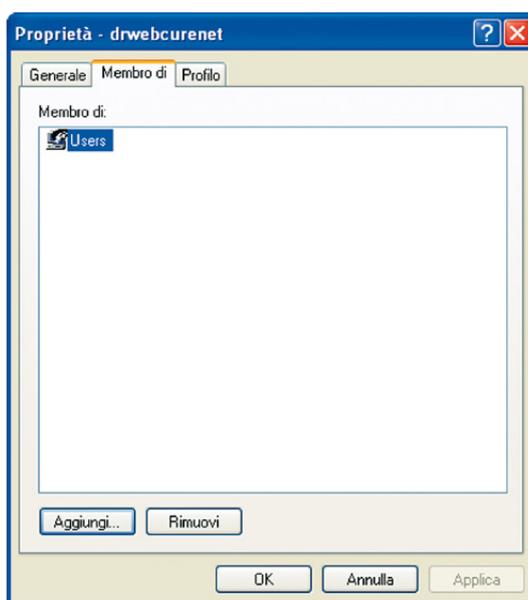
Le azioni successive si possono eseguire anche utilizzando l'account **Amministratore** predefinito, ma al fine di aumentare la riservatezza, si consiglia di creare un altro account di amministratore. Per fare questo, nella parte destra della finestra, premere il tasto destro del mouse. Quindi selezionare la voce **Nuovo utente** dal menu contestuale.



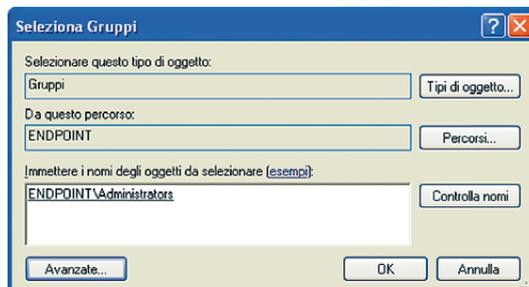
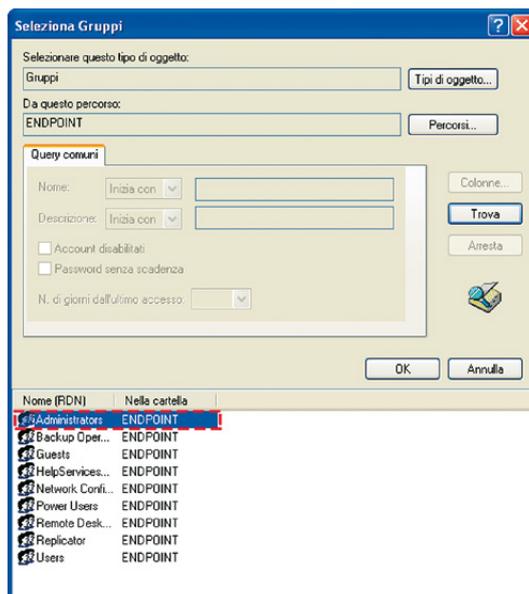
Nel campo **Nome utente** digitare **DrWebCurenet**, nei campi **Password** e **Conferma password** impostare una password complessa. Disabilitare l'opzione **Cambiamento obbligatorio password all'accesso successivo**. Abilitare l'opzione **Nessuna scadenza password**. Cliccare su **Crea** e poi su **Chiudi**.



Fare doppio clic sull'account **DrWebCurenet** creato. Si apre la finestra **Proprietà — DrWebCurenet**. Aprire la scheda **Membro di**.



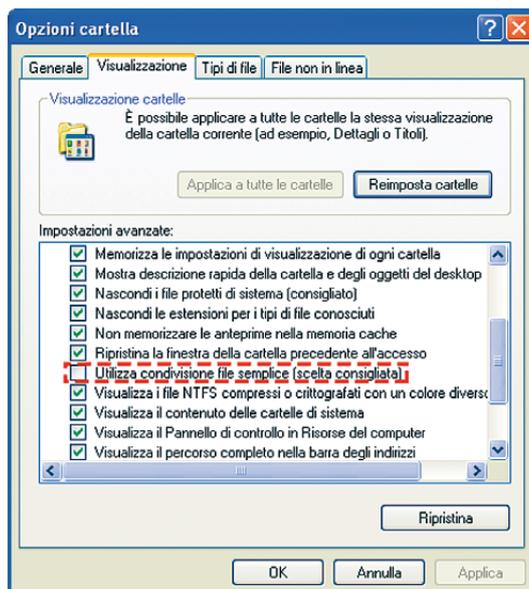
Nella finestra **Membro di**, selezionare **Users** e fare clic su **Rimuovi**. Quindi cliccare su **Aggiungi**. Si apre la finestra **Selezione gruppi**. Cliccare su **Avanzate** e poi su **Trova**. Si genera un elenco da cui selezionare **Administrators** e cliccare su **OK**, e quindi cliccare su **OK** nella finestra **Selezione gruppi**.



Nella finestra **Proprietà** — DrWebCurenet, cliccare prima su **Applica** e poi su **OK**.

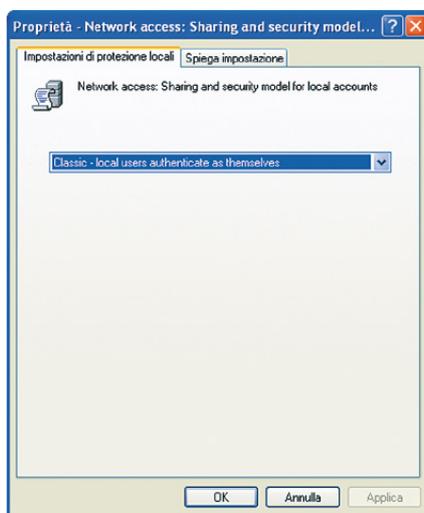
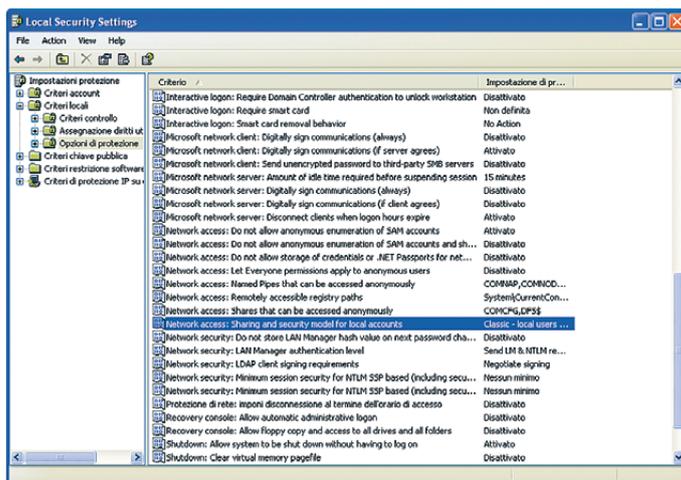
2. Configurare la condivisione di file.

Cliccare sul pulsante **Start** e andare a **Pannello di controllo** → **Visualizzazione classica** → **Opzioni cartella**. Si apre la finestra **Opzioni cartella**. Fare clic sulla scheda **Visualizzazione**. Disabilitare l'opzione **Utilizza condivisione file semplice**. Cliccare sul pulsante **Applica** e poi su **OK**.



3. Configurare criteri di protezione locali.

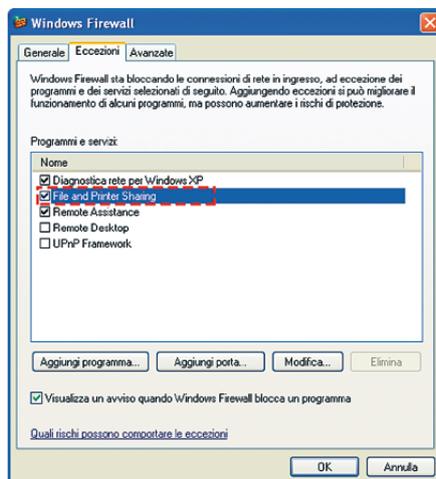
Aprire **Pannello di controllo** → **Strumenti di amministrazione** → **Local security settings** → **Criteri locali** → **Opzioni di protezione**. Mettere il mouse sopra il criterio **Network access: Sharing and security model for local accounts** e fare doppio clic con il tasto sinistro del mouse. Si apre la finestra **Proprietà**. Selezionare l'opzione **Classic**.



Cliccare prima su **Applica** e poi su **OK**. Chiudere lo snap-in **Local security settings**.

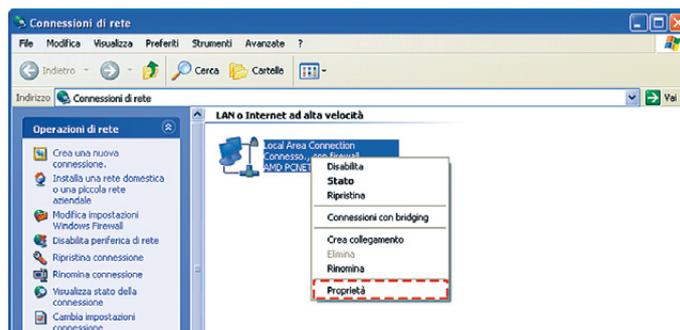
4. Configurare il firewall.

Se si usa un firewall dei terzi, aprire le porte 139 e 445. Se si usa il firewall di Windows, configurarlo nel seguente modo. Cliccare sul pulsante **Start** e selezionare **Pannello di controllo** → **Windows Firewall**. Si apre la finestra **Windows Firewall**. Aprire la scheda **Eccezioni**. Abilitare l'opzione **File and Printer Sharing**. Cliccare su **OK**.



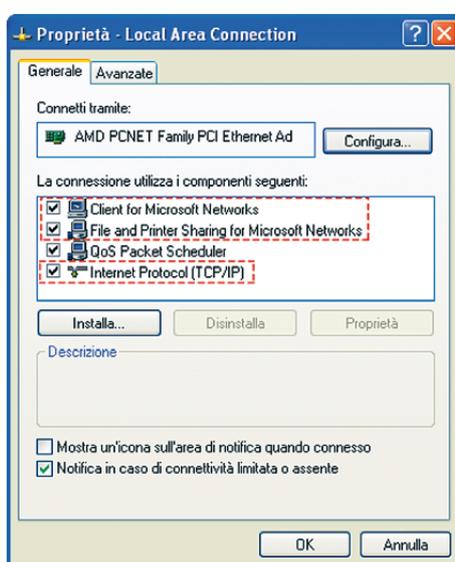
5. Configurare i componenti di rete.

Cliccare sul pulsante **Start** e selezionare la voce **Pannello di controllo** → **Connessioni di rete**. Selezionare con il cursore del mouse la connessione di rete e premere il pulsante destro del mouse. Viene visualizzato un menu contestuale in cui cliccare sulla voce **Proprietà**. Si apre la finestra di configurazione della connessione di rete.



Fare clic sulla scheda **Generali**. Assicurarsi che siano attivati i seguenti componenti:

- Client for Microsoft Networks
- File and Printer Sharing for Microsoft Networks
- Internet Protocol (TCP/IP)



Fare clic su **OK**.

Configurare Windows Vista e Windows Server 2008

1. Configurare il Controllo account utente (l'UAC) (in Windows Vista)
2. Configurare la condivisione di file
3. Attivare l'account di amministratore
4. Configurare il firewall di Windows
5. Configurare i componenti di rete
6. Configurare criteri di protezione locali

Importante! Il sistema operativo deve contenere:

- In caso di Windows Vista – i Service Pack 1 o 2.
- In caso di Windows Server 2008 – il Service Pack 2.

Il Service Pack 1 per Windows Vista si può scaricare da:

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

Il Service Pack 2 per Windows Vista (consigliato) si può scaricare da:

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

Il Service Pack 2 per Windows Server 2008 si può scaricare da:
<http://www.microsoft.com/ru-ru/download/details.aspx?id=15278>

Edizioni supportate:

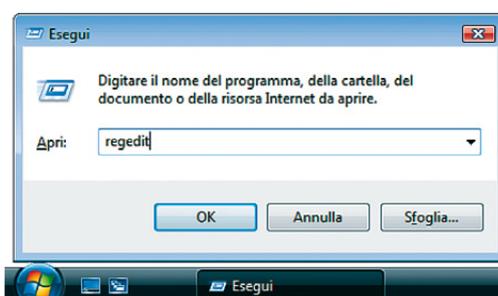
- Windows Vista Business
- Windows Vista Enterprise
- Windows Vista Ultimate

Edizioni non supportate:

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

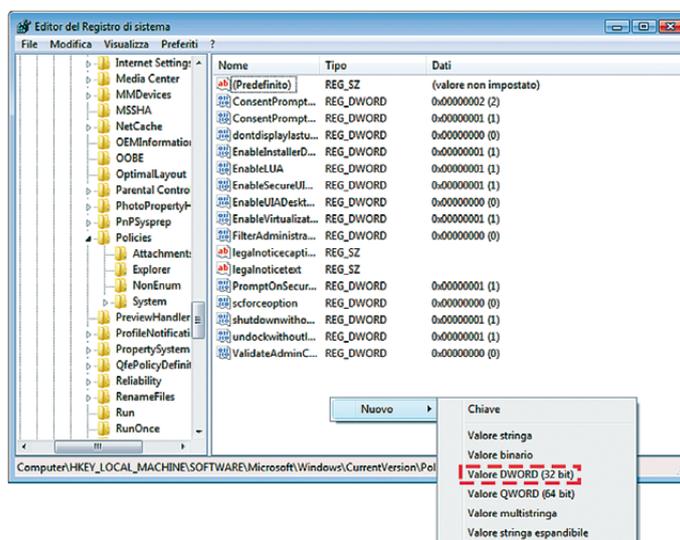
1. Configurare il Controllo account utente (User Account Control) (in Windows Vista).

Premere sui tasti **Windows + R**.

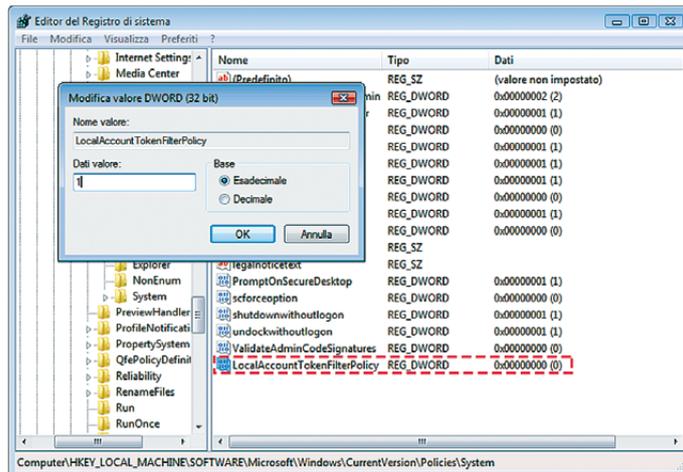


Nella finestra che si apre, digitare **Regedit**. Si apre l'editor del registro di Windows. Aprire il ramo [HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM]

Spostare il cursore del mouse alla parte destra della finestra dell'editor del registro di Windows, premere il tasto destro del mouse e dal menu contestuale che si apre selezionare **Nuovo — Valore DWORD (32 bit)**.



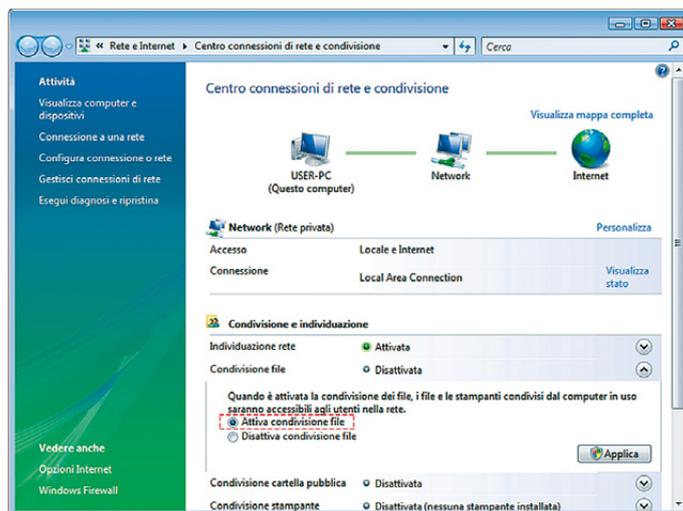
Impostare il nome del valore **LocalAccountTokenFilterPolicy**. Fare doppio clic sul valore creato con il tasto sinistro del mouse. Si apre la finestra **Modifica valore DWORD (32 bit)**. Impostare uno nel campo **Dati valore** e cliccare su **OK**.



Chiudere l'editor del registro di Windows. Eseguire le altre impostazioni (delle voci 2 – 6) e riavviare il computer.

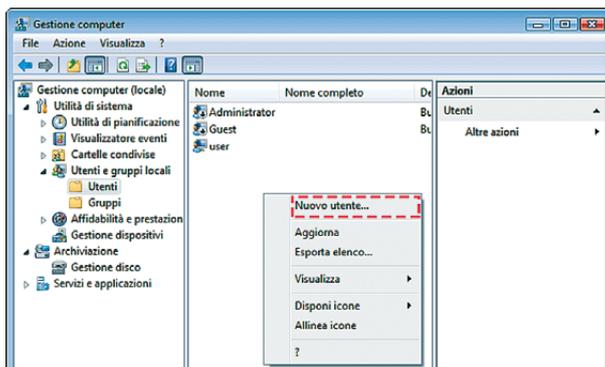
2. Configurare la condivisione di file.

Cliccare sul pulsante **Start** e passare a **Pannello di controllo** → **Rete e Internet** → **Centro connessioni di rete e condivisione**. Nella sezione **Condivisione e individuazione**, spuntare il flag **Attiva condivisione file**. Fare clic sul pulsante **Applica**.

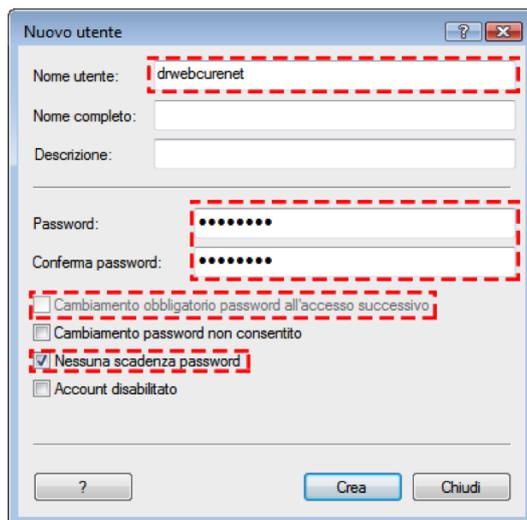


3. Attivare l'account di amministratore.

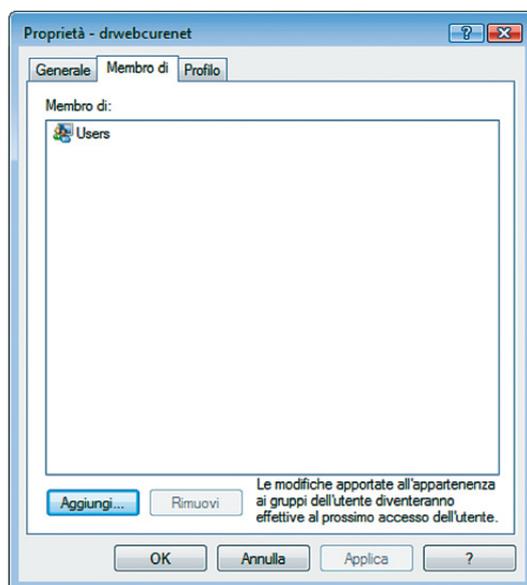
Cliccare su **Start** e andare a **Pannello di controllo** → **Sistema e manutenzione** → **Strumenti di amministrazione** → **Gestione computer** → **Utenti e gruppi locali** → **Utenti**. Le azioni successive si possono eseguire anche utilizzando l'account **Amministratore** predefinito, ma al fine di aumentare la riservatezza, si consiglia di creare un altro account di amministratore. Spostando il cursore alla parte media della finestra, premere il tasto destro del mouse e dal menu contestuale selezionare la voce **Nuovo utente**.



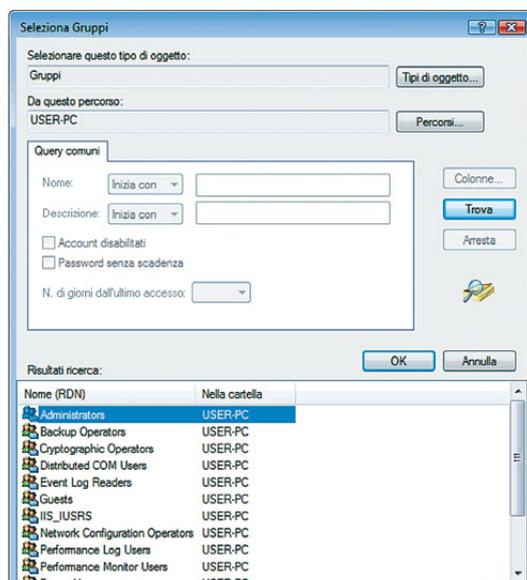
Nel campo **Nome utente** digitare **DrWebCurenet**. Nei campi **Password** e **Conferma password** impostare una password complessa. Disabilitare l'opzione **Cambiamento obbligatorio password all'accesso successivo**. Abilitare l'opzione **Nessuna scadenza password**.



Cliccare su **Crea** e poi su **Chiudi**. Con il pulsante sinistro del mouse fare doppio clic sull'account **DrWebCurennet** creato e nelle proprietà andare alla scheda **Membro di**.



Selezionare **Users** e fare clic su **Rimuovi**. Quindi cliccare su **Aggiungi**. Si apre la finestra **Seleziona gruppi**. Cliccare su **Avanzate** e poi su **Trova**. Si genera un elenco da cui selezionare **Administrators** e cliccare su **OK**.



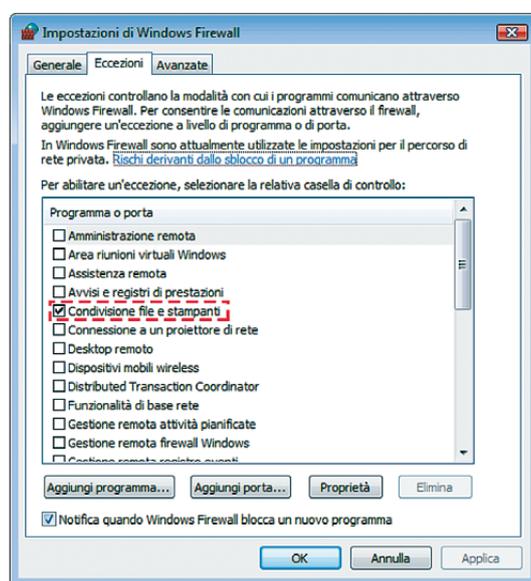
Quindi cliccare su **OK** anche nella finestra **Seleziona gruppi**.



Cliccare consecutivamente su **Applica** e **OK** nella finestra **Proprietà — DrWebCurenet**.

4. Configurare il firewall.

Se si usa un firewall dei terzi, aprire le porte 139 e 445. Se si usa il firewall di Windows, configurarlo nel seguente modo. Cliccare sul pulsante **Start** e selezionare **Pannello di controllo** → **Sicurezza** → **Windows Firewall**. Cliccare sul collegamento **Consenti programma con Windows Firewall**. Nella finestra **Impostazioni di Windows Firewall**, fare clic sulla scheda **Eccezioni**. Spuntare il flag **Condivisione file e stampanti**.

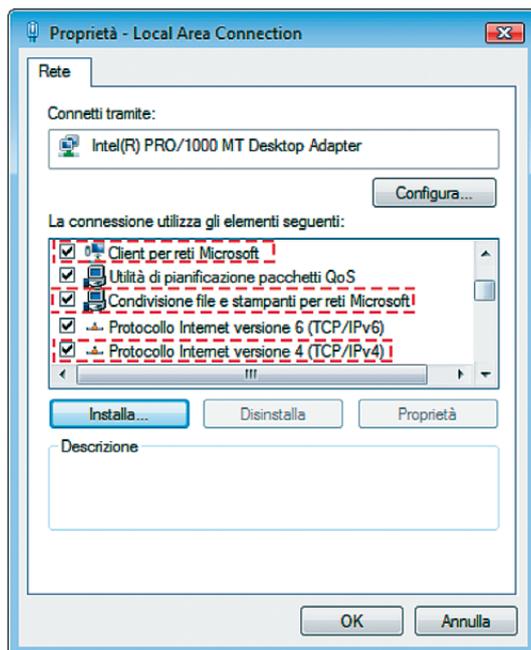


Cliccare su **OK**.

5. Configurare i componenti di rete.

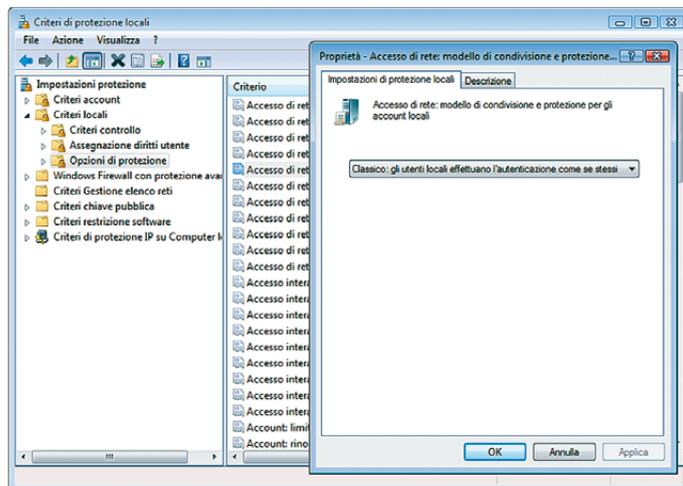
Cliccare sul pulsante **Start** e andare a **Pannello di controllo** → **Rete e Internet** → **Centro connessioni di rete e condivisione** → **Gestisci connessioni di rete**. Mettere il cursore del mouse sopra la connessione di rete e premere il tasto destro del mouse. Si apre un menu contestuale da cui selezionare la voce **Proprietà**. Assicurarsi che siano attivati i seguenti componenti:

- Client per reti Microsoft
- Condivisione file e stampanti per reti Microsoft
- Protocollo Internet versione 4 (TCP/IPv4)



6. Configurare criteri di protezione locali.

Fare clic su **Start** e andare a **Pannello di controllo** → **Sistema e manutenzione** → **Strumenti di amministrazione** → **Criteri di protezione locali** → **Criteri locali** → **Opzioni di protezione**. Selezionare con il cursore del mouse il criterio **Accesso di rete: modello di condivisione e protezione per gli account locali**. Fare doppio clic con il tasto sinistro del mouse. Si apre la finestra **Proprietà**. Selezionare la voce **Classico** e poi cliccare su **OK**.



Configurare Windows 7, Windows 2008 R2

1. Configurare il Controllo account utente (l'UAC) (in Windows 7)
2. Configurare la condivisione di file
3. Attivare l'account di amministratore
4. Configurare il firewall di Windows
5. Configurare i componenti di rete
6. Configurare criteri di protezione locali

Importante! Edizioni supportate:

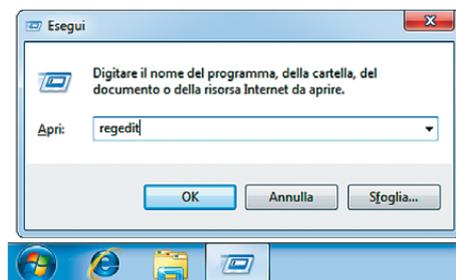
- Windows 7 Professional
- Windows 7 Enterprise
- Windows 7 Ultimate

Edizioni non supportate:

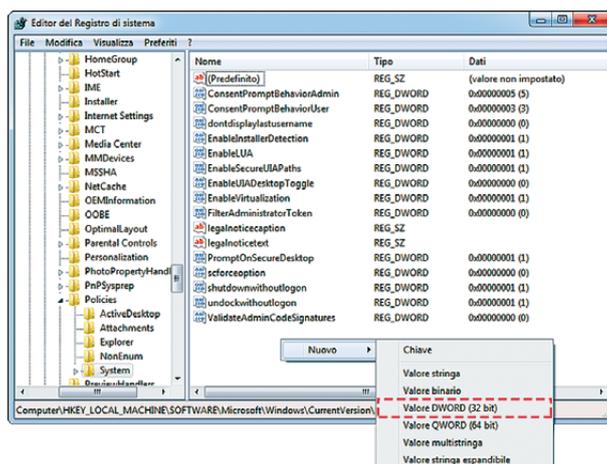
- Windows 7 Starter
- Windows 7 Home Basic
- Windows 7 Home Premium

1. Configurare il Controllo account utente (User Account Control)

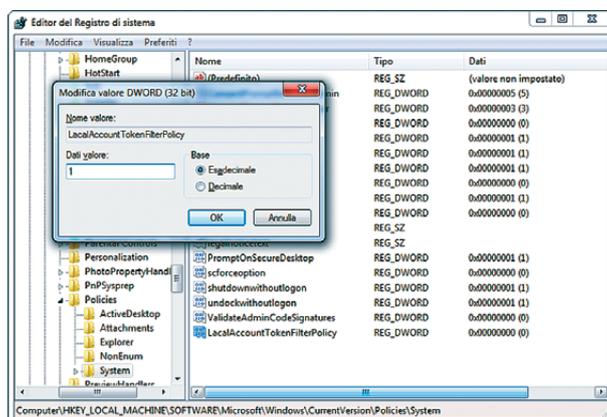
Premere sui tasti **Windows + R**.



Nella finestra che si apre, digitare **Regedit**. Si apre l'editor del registro di Windows. Aprire il ramo [HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM] Spostare il cursore del mouse alla parte destra della finestra dell'editor del registro di Windows, premere il tasto destro del mouse e dal menu contestuale che si apre selezionare **Nuovo** e quindi creare un **Valore DWORD (32 bit)**.



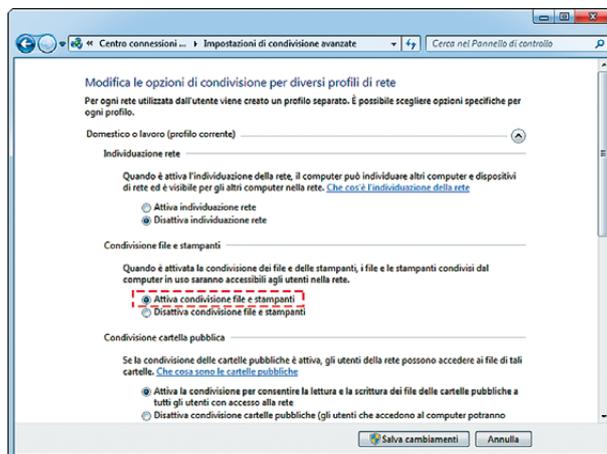
Impostare il nome del valore **LocalAccountTokenFilterPolicy**. Fare doppio clic sul valore creato con il tasto sinistro del mouse. Si apre la finestra **Modifica valore DWORD (32 bit)**. Impostare uno nel campo **Dati valore** e cliccare su **OK**.



Chiudere l'editor del registro di Windows. Eseguire le altre impostazioni (delle voci 2 – 6) e riavviare il computer.

2. Configurare la condivisione di file.

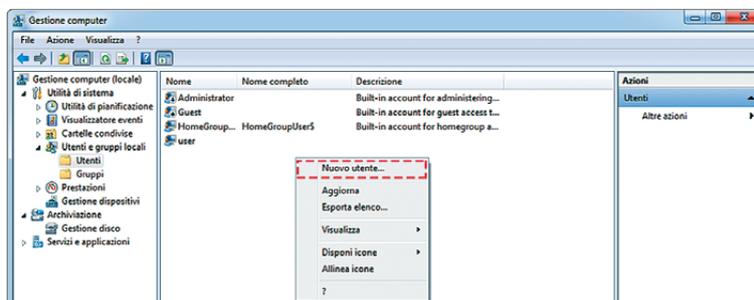
Cliccare sul pulsante **Start** e passare nel menu a **Pannello di controllo** → **Rete e Internet** → **Centro connessioni di rete e condivisione** → **Modificare le impostazioni di condivisione avanzate**. Nel profilo di rete generale, abilitare l'opzione **Attiva condivisione file e stampanti**.



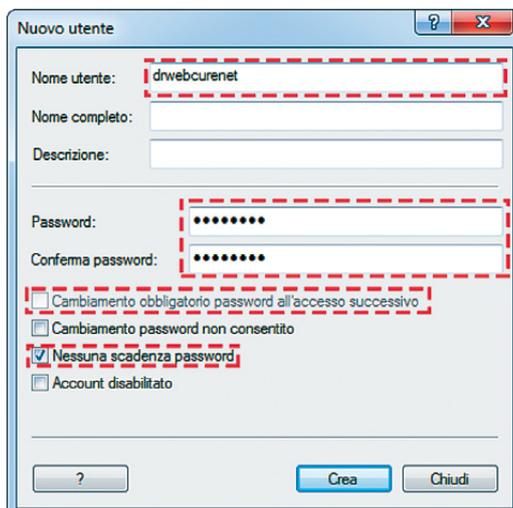
Fare clic sul pulsante **Salva cambiamenti**.

3. Attivare l'account di amministratore.

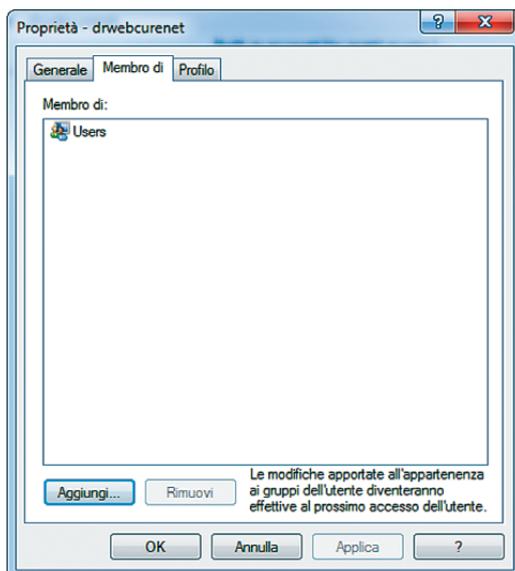
Cliccare sul pulsante **Start** e passare nel menu a **Pannello di controllo** → **Sistema e sicurezza** → **Strumenti di amministrazione** → **Gestione computer** → **Utenti e gruppi locali** → **Utenti**. Le azioni successive si possono eseguire anche utilizzando l'account **Amministratore** predefinito, ma al fine di aumentare la riservatezza, si consiglia di creare un altro account di amministratore. Spostando il cursore alla parte media della finestra, premere il tasto destro del mouse e dal menu contestuale selezionare la voce **Nuovo utente**.



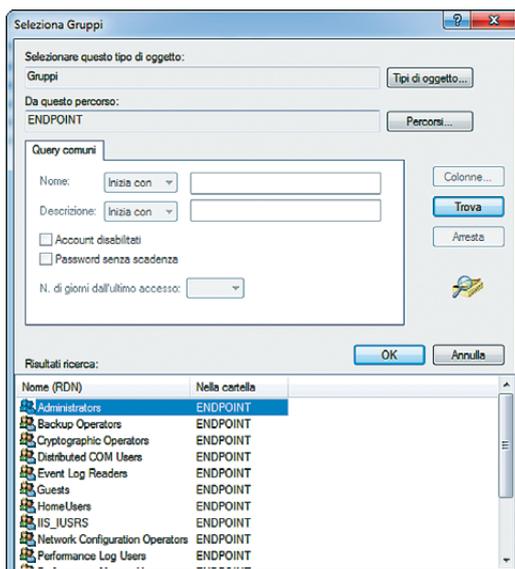
Nel campo **Nome utente** digitare **DrWebCurenet**. Nei campi **Password** e **Conferma password** impostare una password complessa. Disabilitare l'opzione **Cambiamento obbligatorio password all'accesso successivo**. Abilitare l'opzione **Nessuna scadenza password**. Cliccare su **Crea** e poi su **Chiudi**.



Con il pulsante sinistro del mouse fare doppio clic sull'account **DrWebCurenet** creato e nelle proprietà andare alla scheda **Membro di**. Selezionare **Users** e fare clic su **Rimuovi**.



Quindi cliccare sul pulsante **Aggiungi**. Si apre la finestra **Seleziona gruppi**. Cliccare sul pulsante **Avanzate** e poi su **Trova**. Si genera un elenco da cui selezionare **Administrators** e cliccare su **OK**.



Quindi cliccare su **OK** anche nella finestra **Seleziona gruppi**.

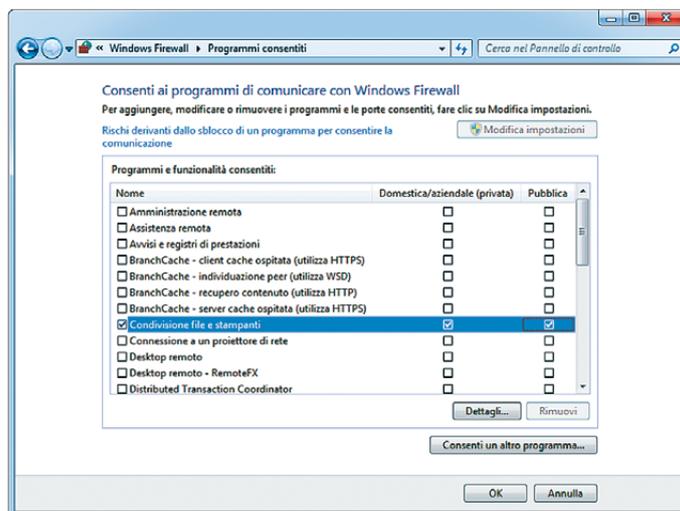


Adesso cliccare consecutivamente su **Applica** e **OK** nella finestra **Proprietà — DrWebCurenet**.

4. Configurare il firewall.

Se si usa un firewall dei terzi, aprire le porte 139 e 445. Se si usa il firewall di Windows, configurarlo nel seguente modo. Cliccare sul pulsante **Start** e andare a **Pannello di controllo** → **Sistema e sicurezza** → **Windows Firewall** →

Consenti programma o funzionalità con Windows Firewall. Cliccare sul pulsante **Modifica impostazioni**. Spuntare il flag **Condivisione file e stampanti**.

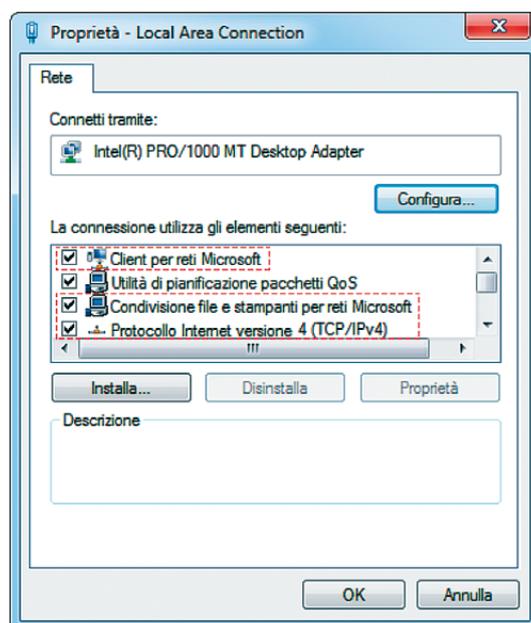


Cliccare su **OK**.

5. Configurare i componenti di rete.

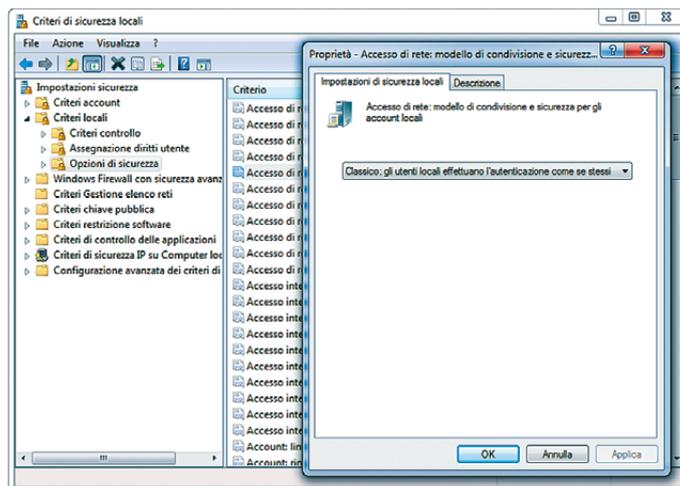
Cliccare sul pulsante **Start** e andare a **Pannello di controllo** → **Rete e Internet** → **Centro connessioni di rete e condivisione** → **Cambiare le impostazioni della scheda**. Mettere il cursore del mouse sopra la connessione di rete e premere il tasto destro del mouse. Si apre un menu contestuale da cui selezionare la voce **Proprietà**. Assicurarsi che siano attivati i seguenti componenti:

- Client per reti Microsoft
- Condivisione file e stampanti per reti Microsoft
- Protocollo Internet versione 4 (TCP/IPv4)



6. Configurare criteri di protezione locali.

Cliccare sul pulsante **Start** e andare a **Pannello di controllo** → **Sistema e sicurezza** → **Strumenti di amministrazione** → **Criteri di sicurezza locali** → **Criteri locali** → **Opzioni di sicurezza**. Selezionare il criterio **Accesso di rete: modello di condivisione e sicurezza per gli account locali**. Fare doppio clic con il tasto sinistro del mouse. Si apre la finestra **Proprietà**. Selezionare la voce **Classico** e poi cliccare su **OK**.

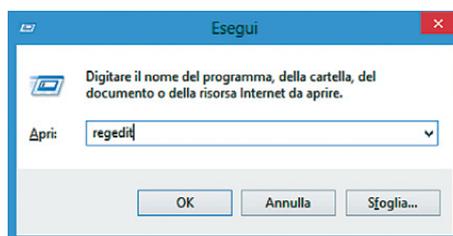


Configurare Windows 8, Windows Server 2012

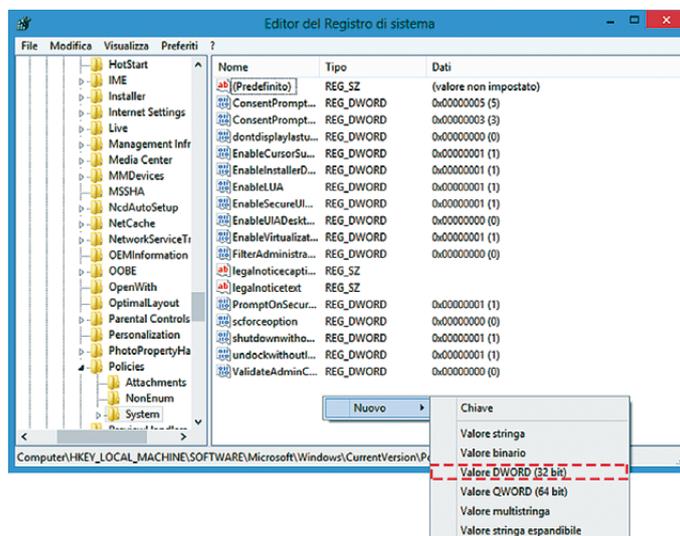
1. Configurare il Controllo account utente (l'UAC)
2. Configurare la condivisione di file
3. Attivare l'account di amministratore
4. Configurare il firewall di Windows
5. Configurare i componenti di rete
6. Configurare criteri di protezione locali

1. Configurare il Controllo account utente (l'UAC)

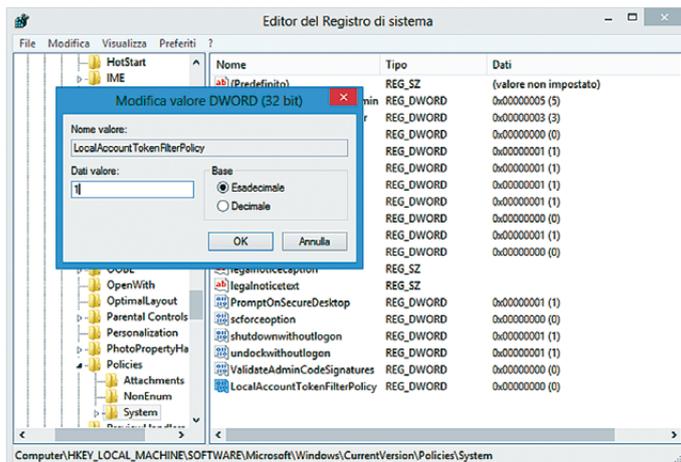
Premere sui tasti **Windows + R**.



Nella finestra che si apre, digitare **Regedit**. Si apre l'editor del registro di Windows. Aprire il ramo [HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM] Spostare il cursore del mouse alla parte destra della finestra dell'editor del registro di Windows, premere il tasto destro del mouse e dal menu contestuale che si apre selezionare **Nuovo** e quindi creare un **Valore DWORD (32 bit)**.



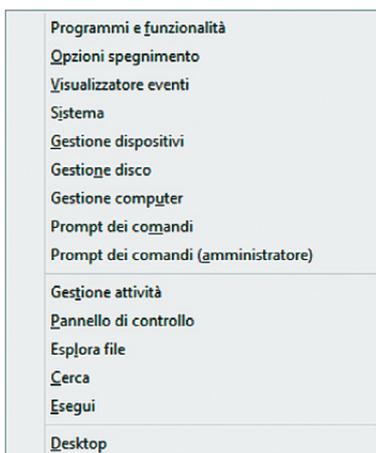
Impostare il nome del valore **LocalAccountTokenFilterPolicy**. Fare doppio clic sul valore creato con il tasto sinistro del mouse. Si apre la finestra **Modifica valore DWORD (32 bit)**. Impostare uno nel campo **Dati valore** e cliccare su **OK**.



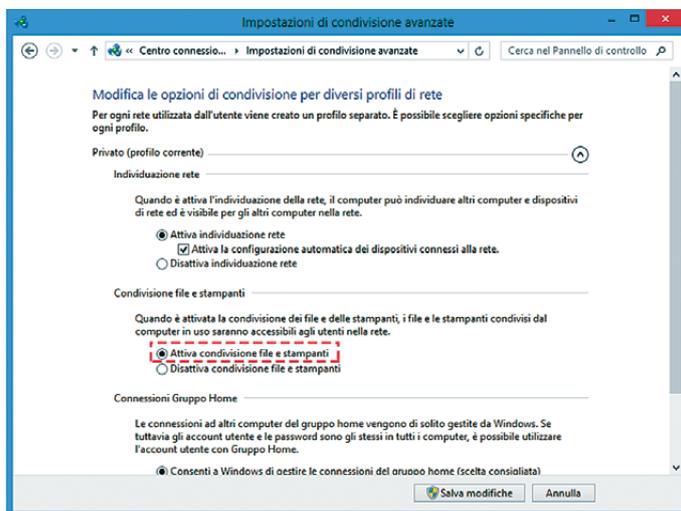
Chiudere l'editor del registro di Windows. Eseguire le altre impostazioni (voci 2 – 6) e riavviare il computer.

2. Configurare la condivisione di file.

Premere sui tasti **Windows + X**.



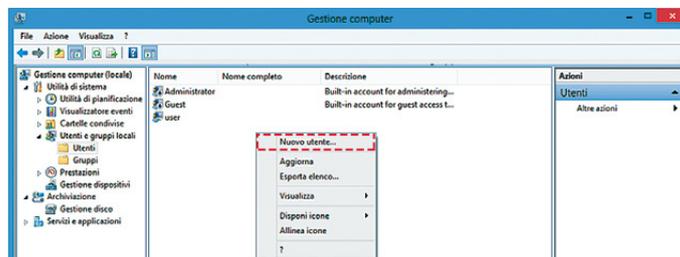
Dal menu contestuale che si apre selezionare la voce **Pannello di controllo** → **Rete e Internet** → **Centro connessioni di rete e condivisione** → **Modificare le impostazioni di condivisione avanzate**. Nel profilo di rete generale, abilitare l'opzione **Attiva condivisione file e stampanti**.



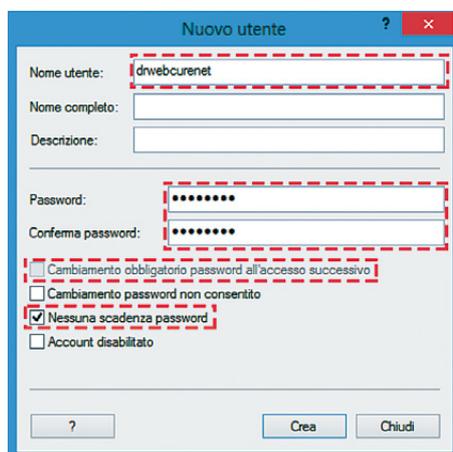
Cliccare sul pulsante **Salva modifiche**.

3. Attivare l'account di amministratore.

Premere sui tasti **Windows + X**. Nel menu contestuale che si apre andare a **Pannello di controllo** → **Sistema e sicurezza** → **Strumenti di amministrazione** → **Gestione computer** → **Utenti e gruppi locali** → **Utenti**. Le azioni successive si possono eseguire anche utilizzando l'account **Amministratore** predefinito, ma al fine di aumentare la riservatezza, si consiglia di creare un altro account di amministratore. Spostando il cursore alla parte media della finestra, premere il tasto destro del mouse e dal menu contestuale selezionare la voce **Nuovo utente**.

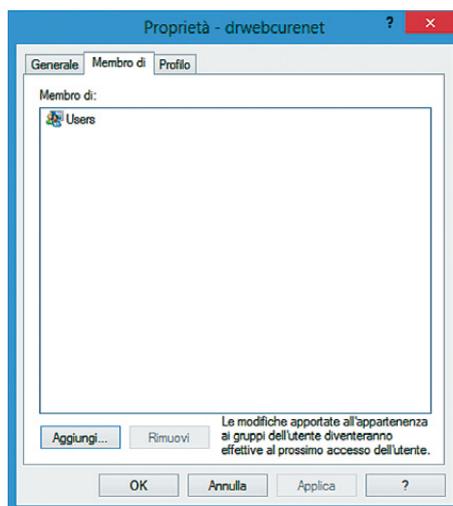


Nel campo **Nome utente** digitare **DrWebCurenet**. Nei campi **Password** e **Conferma password** impostare una password complessa. Disabilitare l'opzione **Cambiamento obbligatorio password all'accesso successivo**. Abilitare l'opzione **Nessuna scadenza password**.



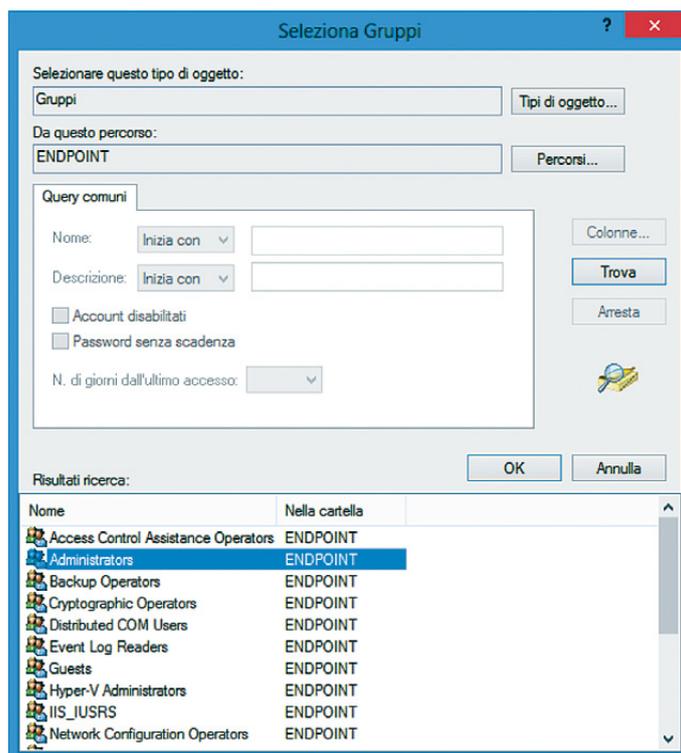
Cliccare su **Crea** e poi su **Chiudi**.

Con il pulsante sinistro del mouse fare doppio clic sull'account **DrWebCurenet** creato e nelle proprietà andare alla scheda **Membro di**.



Selezionare la voce **Users** e fare clic sul pulsante **Rimuovi**.

Quindi cliccare sul pulsante **Aggiungi**. Si apre la finestra **Seleziona gruppi**. Cliccare sul pulsante **Avanzate** e poi su **Trova**. Si genera un elenco da cui selezionare la voce **Administrators** e cliccare su **OK**.



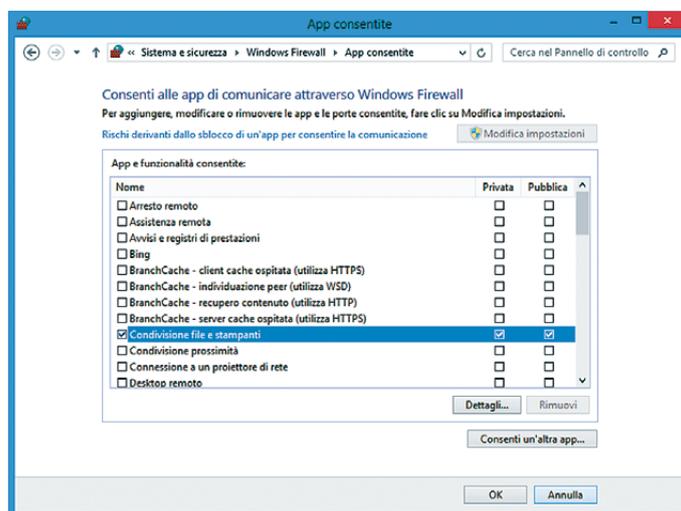
Quindi cliccare su **OK** anche nella finestra **Seleziona gruppi**.



Adesso cliccare consecutivamente su **Applica** e su **OK** nella finestra **Proprietà — DrWebCurenet**.

4. Configurare il firewall.

Se si usa un firewall dei terzi, aprire le porte 139 e 445. Se si usa il firewall di Windows, configurarlo nel seguente modo. Premere sui tasti **Windows + X**. Nel menu contestuale che si apre andare a **Pannello di controllo** → **Sistema e sicurezza** → **Windows Firewall** → **Consenti programma o funzionalità con Windows Firewall**. Cliccare sul pulsante **Modifica impostazioni**. Spuntare il flag **Condivisione file e stampanti**.



Cliccare su **OK**.

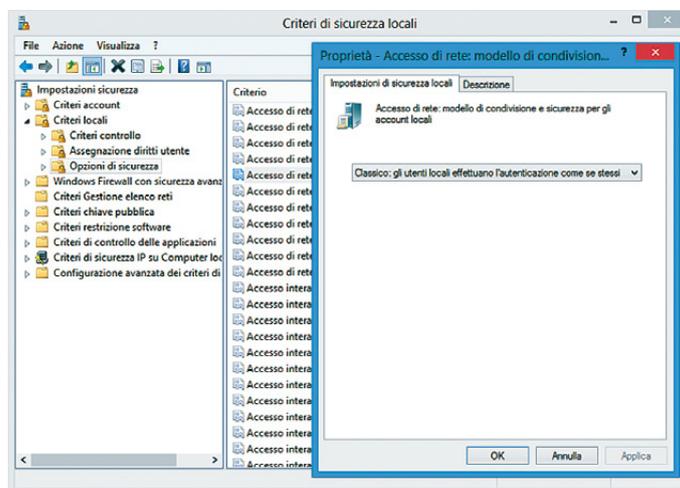
5. Configurare i componenti di rete.

Premere sui tasti **Windows + X**. Nel menu contestuale che si apre andare a **Pannello di controllo** → **Rete e Internet** → **Centro connessioni di rete e condivisione** → **Cambiare le impostazioni della scheda**. Mettere il cursore del mouse sopra la connessione di rete e premere il tasto destro del mouse. Si apre un menu contestuale da cui selezionare la voce **Proprietà**. Assicurarsi che siano attivati i seguenti componenti:

- Client per reti Microsoft
- Condivisione file e stampanti per reti Microsoft
- Protocollo Internet versione 4 (TCP/IPv4)

6. Configurare criteri di protezione locali.

Premere sui tasti **Windows + X**. Nel menu contestuale che si apre andare a **Pannello di controllo** → **Sistema e sicurezza** → **Strumenti di amministrazione** → **Criteri di sicurezza locali** → **Criteri locali** → **Opzioni di sicurezza**. Selezionare il criterio **Accesso di rete: modello di condivisione e sicurezza per gli account locali**. Fare doppio clic con il tasto sinistro del mouse. Si apre la finestra **Proprietà**. Selezionare l'opzione **Classico** e poi cliccare su **OK**.



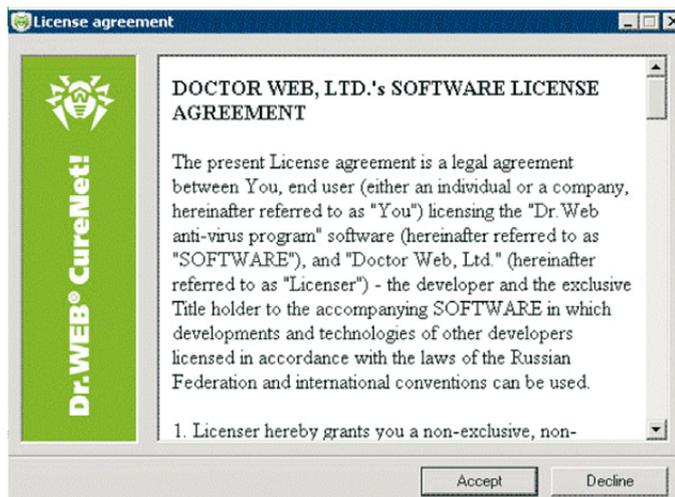
Avvio di Dr.Web CureNet!

1. Avviare la copia ricevuta del programma CureNet!.exe.

Attenzione! Gli avvisi successivi di Dr.Web CureNet! verranno descritti più avanti.

Attenzione! Sebbene Dr.Web CureNet! sia compatibile con programmi antivirus di altri produttori, per accelerare il processo di scansione, si raccomanda di disabilitare gli antivirus dei terzi per il tempo di esecuzione di Dr.Web CureNet!.

2. Per continuare, fare clic sul pulsante **Accept**.



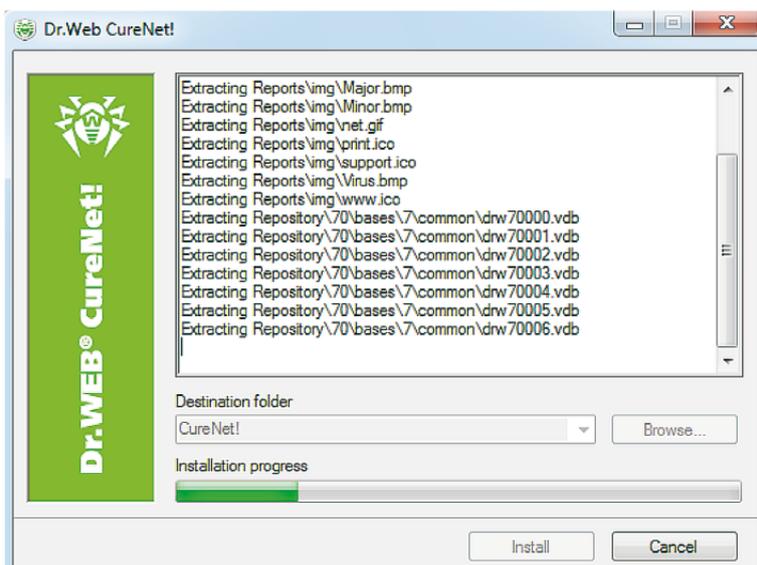
3. Se si vuole salvare i file di Dr.Web CureNet! in una cartella diversa dalla cartella predefinita, fare clic sul pulsante **Browse** e selezionare una cartella.

CureNet!.exe è un archivio autoestraente perciò il programma non richiede di essere installato. Per procedere, è necessario selezionare una cartella in cui verranno memorizzati i file estratti da quest'archivio. Il nome della cartella di default è CureNet!, ma si può scegliere un nome diverso. Se l'archivio viene decompresso su un dispositivo USB o su un dispositivo simile, si avrà l'utility Dr.Web CureNet! sempre a portata di mano per utilizzarla in eventuali casi di emergenza nella rete locale.

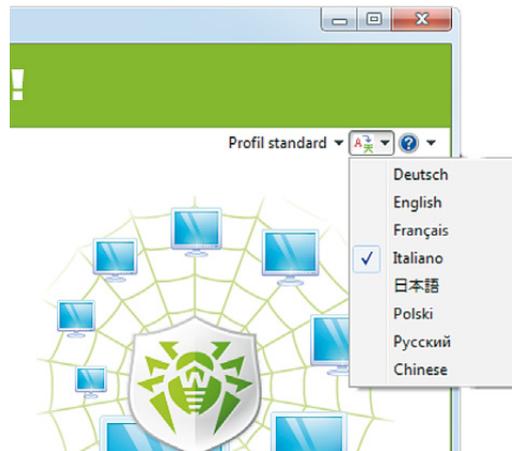
La cartella creata nel corso della decompressione dell'archivio contiene i file del repository del programma e il file della chiave.



Per continuare l'installazione, fare clic sul pulsante **Install**.



4. Nella finestra apertasi, si può scegliere la lingua della localizzazione utilizzando il pulsante  che si trova nell'angolo superiore destro.

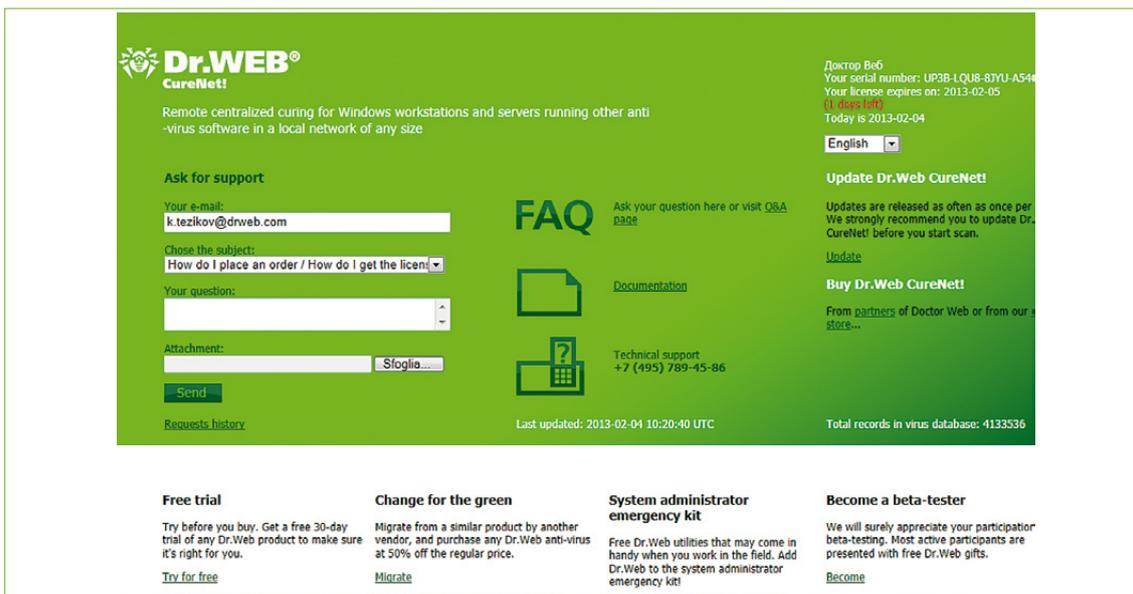


Se in precedenza sono state memorizzate le impostazioni di scansione, è possibile caricarle utilizzando il pulsante Profilo standard che si trova nell'angolo superiore destro.



Se si hanno domande, fare clic su . Selezionando la voce Aiuto dal menu contestuale si può consultare il Manuale dell'utente. Selezionando la voce Il mio Dr.Web si apre l'Area personale dell'utente da cui è possibile inviare una domanda al servizio di supporto tecnico.

Inoltre, l'opzione Sul programma sulla stessa pagina visualizza le informazioni della licenza.



Dr.WEB® CureNet!
 Remote centralized curing for Windows workstations and servers running other anti-virus software in a local network of any size.

Ask for support
 Your e-mail:
 Choose the subject: **How do I place an order / How do I get the license?**
 Your question:
 Attachment:

FAQ Ask your question here or visit [Q&A page](#)

Дoктop Beб
 Your serial number: UP3B-LQU8-8YU-A546
 Your license expires on: 2013-02-05
 (1989216)
 Today is 2013-02-04

Update Dr.Web CureNet!
 Updates are released as often as once per...
 We strongly recommend you to update Dr. CureNet! before you start scan.

Buy Dr.Web CureNet!
 From [partners](#) of Doctor Web or from our [store](#)...

Last updated: 2013-02-04 10:20:40 UTC
 Total records in virus database: 4133536

Free trial
 Try before you buy. Get a free 30-day trial of any Dr.Web product to make sure it's right for you.
[Try for free](#)

Change for the green
 Migrate from a similar product by another vendor, and purchase any Dr.Web anti-virus at 50% off the regular price.
[Migrate](#)

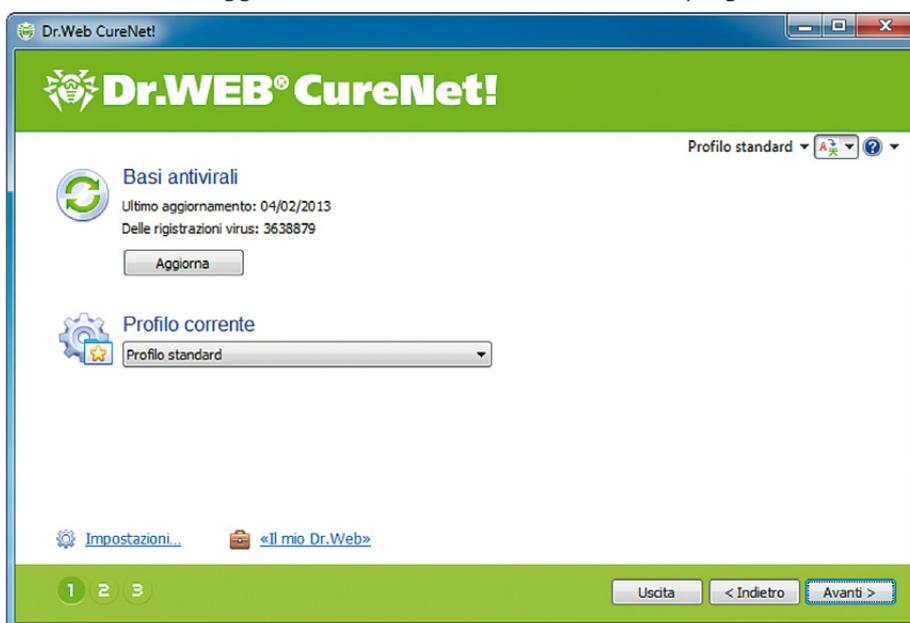
System administrator emergency kit
 Free Dr.Web utilities that may come in handy when you work in the field. Add Dr.Web to the system administrator emergency kit!

Become a beta-tester
 We will surely appreciate your participation beta-testing. Most active participants are presented with free Dr.Web gifts.
[Become](#)

Per continuare, cliccare su **Avanti**.

Per aggiornare i database dei virus, cliccare su **Aggiorna**.

Attenzione! Il successo della ricerca e della neutralizzazione dei virus dipende in gran parte dallo stato dei database antivirali, dunque si raccomanda di aggiornare i database a ciascun avvio del programma.



Dr.WEB® CureNet!
 Profilo standard

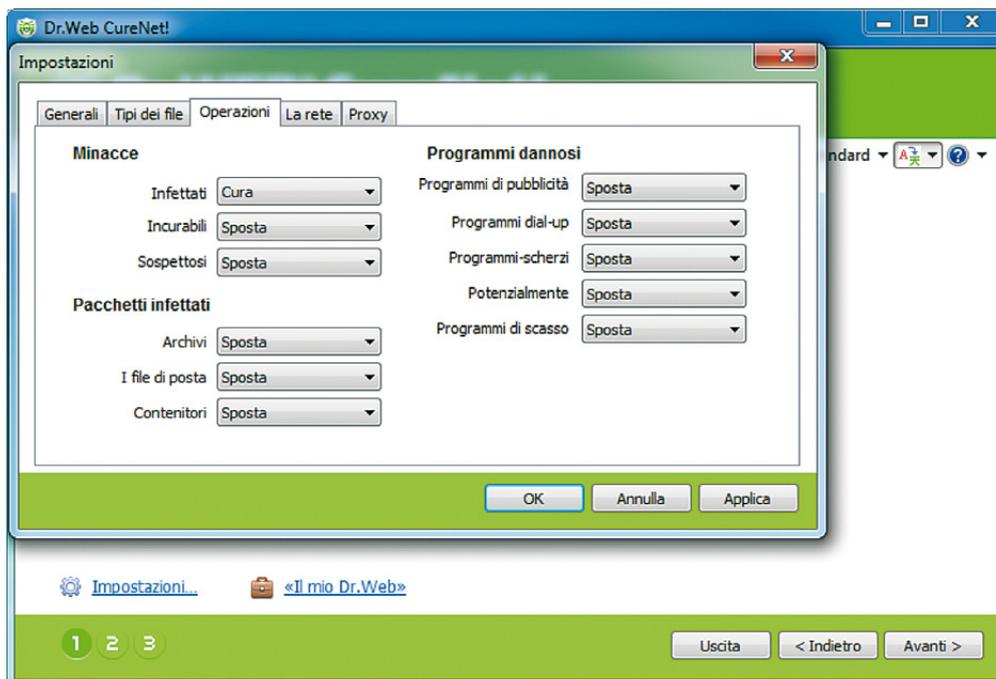
Basi antivirali
 Ultimo aggiornamento: 04/02/2013
 Delle registrazioni virus: 3638879

Profilo corrente



Aggiornamento — 49%
 Delle registrazioni virus: 7686724
 Scaricato 54.7 MB di 111.1 MB

Se si vuole modificare le impostazioni predefinite, cliccare su **Impostazioni**.



Nella scheda **Operazioni**, si possono selezionare le operazioni da applicare a oggetti malevoli di vari tipi. Di default, l'operazione **Sposta** è selezionata per più tipi di malware.

Va notato che l'elenco delle operazioni disponibili è diverso secondo il tipo di malware. Così, a file infetti si possono applicare le operazioni **Cura**, **Rimuovi**, **Rinomina** e **Sposta**, mentre per oggetti incurabili l'azione **Cura** non è disponibile.

Attenzione! La cura di alcuni virus richiede il riavvio del computer. Tuttavia, di default, l'opzione **Riavviare la stazione** nella scheda **Generali** non è selezionata perché un riavvio non aspettato del computer potrebbe disturbare l'utenza. Pertanto, se sono stati trovati virus nella rete locale, si raccomanda di eseguire una scansione completa della rete locale preavvisandone gli utenti.

Per memorizzare le impostazioni modificate, selezionare **Profilo standard** e dal menu apertosi selezionare **Salvare**.



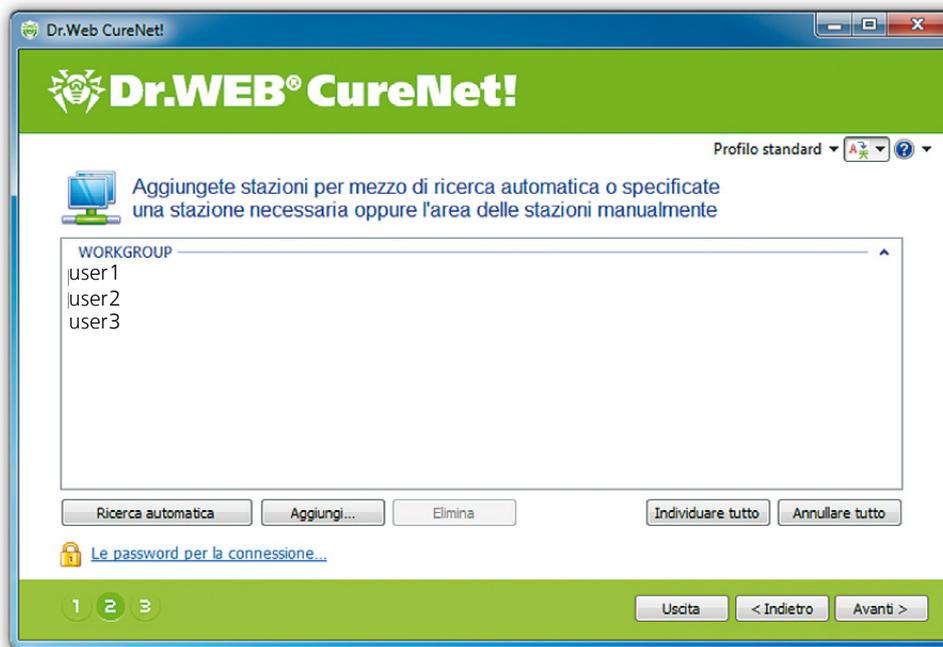
Attenzione! Si raccomanda di utilizzare le impostazioni predefinite poiché tutti i prodotti dell'azienda Doctor Web vengono forniti con le impostazioni ottimali che permettono il miglior funzionamento.

Se si hanno profili salvati, cliccare su **Profilo corrente** e scegliere il profilo desiderato.

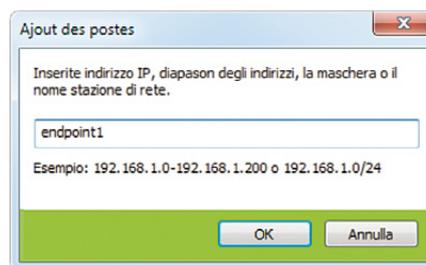


Per continuare, cliccare su **Avanti**.

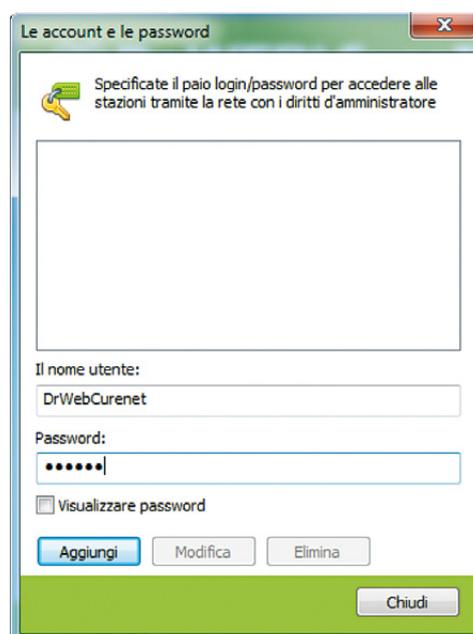
5. Nella finestra apertasi, creare un elenco delle postazioni della rete su cui si vuole eseguire il controllo antivirale.



Per cercare postazioni nella rete, premere sul tasto **Ricerca automatica**. Se si vuole creare un elenco in modo manuale, premere sul tasto **Aggiungi** e nella finestra **Aggiungere stazioni**, inserire l'indirizzo di un singolo computer o un intervallo di indirizzi.



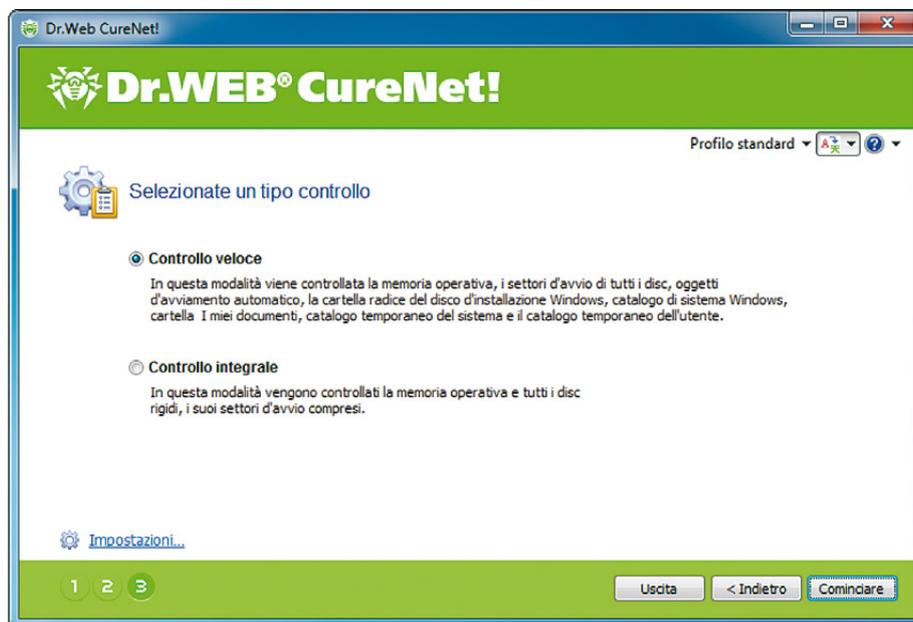
Se la rete da scansione non ha una struttura di dominio, fare clic sulle **Password per la connessione** e nella finestra apertasi inserire le password per accedere ai computer da scansione.



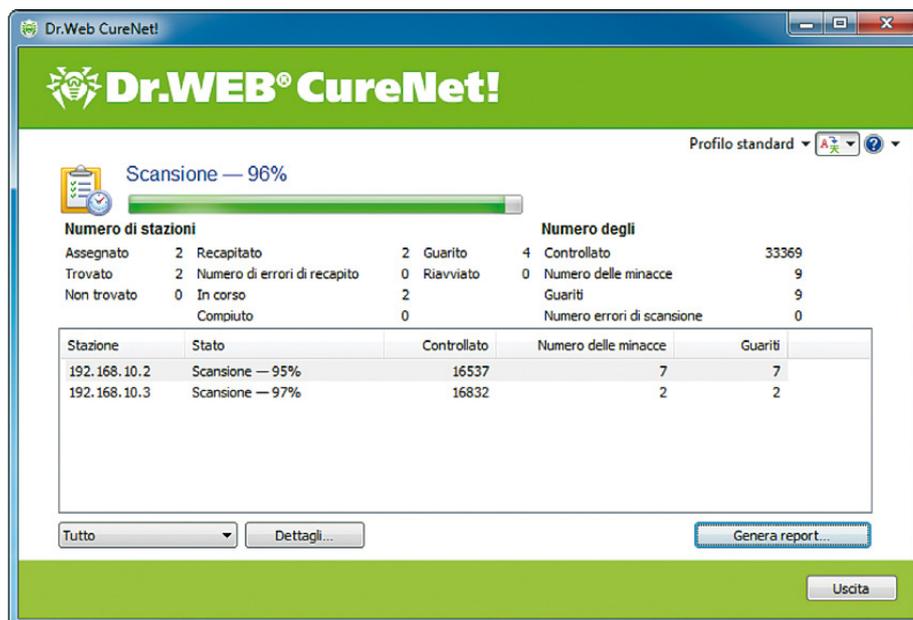
Per continuare, cliccare su **Avanti**.

Nella finestra apertasi, scegliere il tipo di scansione – **Veloce** o **Integrale**.

Attenzione! La scansione del tipo veloce controlla sole aree di sistema e processi in esecuzione. Di conseguenza, tale scansione non garantisce che i computer verranno completamente ripuliti dai virus, anche perché virus attivi potrebbero reinfectare file già controllati e ripuliti.



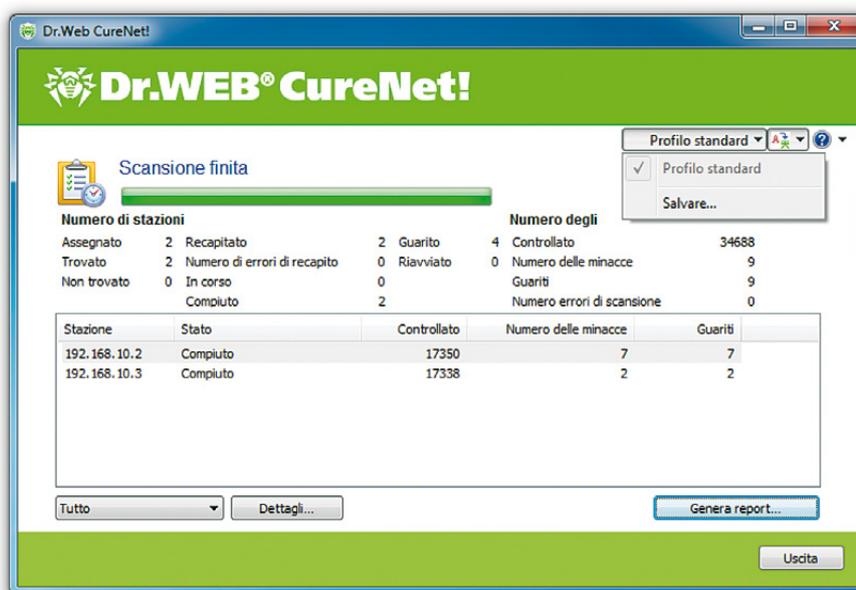
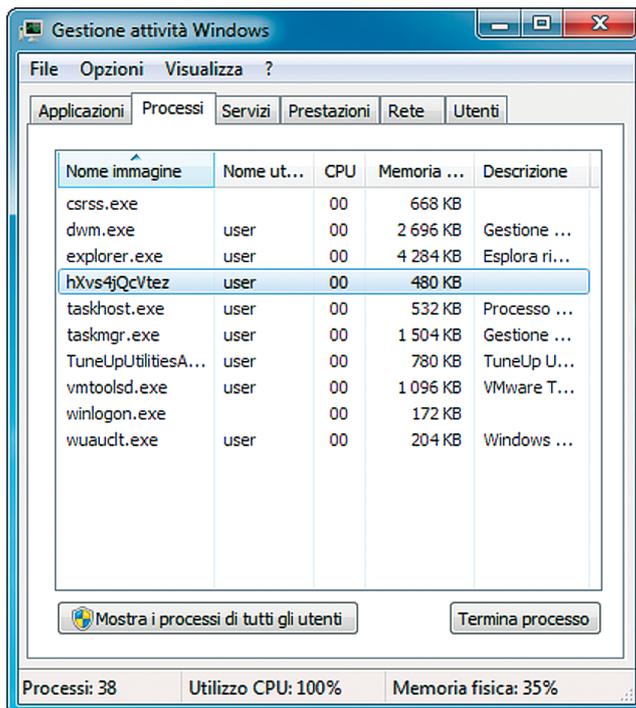
Per procedere con la scansione, cliccare su **Cominciare**.



Questa pagina visualizza lo stato di avanzamento e i risultati della scansione che si esegue sui computer remoti della rete locale. La ricezione delle informazioni statistiche non dipende dalla qualità della connessione tra i computer. Se la connessione si interrompe, l'utility Dr.Web CureNet! aggiorna le informazioni statistiche appena la connessione si riprende.

Attenzione! Non è consigliabile interrompere la scansione prima del completamento.

I processi di scansione in esecuzione utilizzano meccanismi di autodifesa per proteggersi contro i programmi malevoli.



Si può generare un report con i risultati della scansione della rete utilizzando il pulsante **Genera report**.

Controllo veloce

 L'inizio: 16:37:48
 04/02/2013
 La fine: 16:55:49
 04/02/2013

 [Stampa](#)
Numero di stazioni

 Assegnato 2
 Trovato 2
 Non trovato 0

 Recapitato 2
 Numero di errori di recapito 0
 In corso 0
 Compiuto 2

 Guarito 2
 Riavviato 0
 0
 2

Numero degli oggetti

 Controllato 34688
 Numero delle minacce 9
 Guariti 9
 Numero errori di scansione 0

192.168.10.2
Minacce

 Infettati 7
 Incurabili 0
 Sospettosi 0
 Programmi di pubblicità 0
 Programmi dial-up 0
 Programmi-scherzi 0
 Potenzialmente pericolosi 0
 Programmi di scasso 0

Operazioni

 Curato 1
 Eliminato 6
 Spostato 0
 Ignorato 0

Statistica

 Scansionati 17350
 La quantità di dati(KB) 2926263
 Tempo di controllo 00:15:10

Percorso	Minacce	Operazione
C:\Trojan.Carberp.276.exe	 Trojan.Carberp.276	Curato
C:\Trojan.Carberp.30.dat	 Trojan.Carberp.30	Curato
C:\Trojan.Carberp.647.exe	 Trojan.Carberp.647	Curato

Per chiudere il programma, premere sul pulsante **Uscita**.

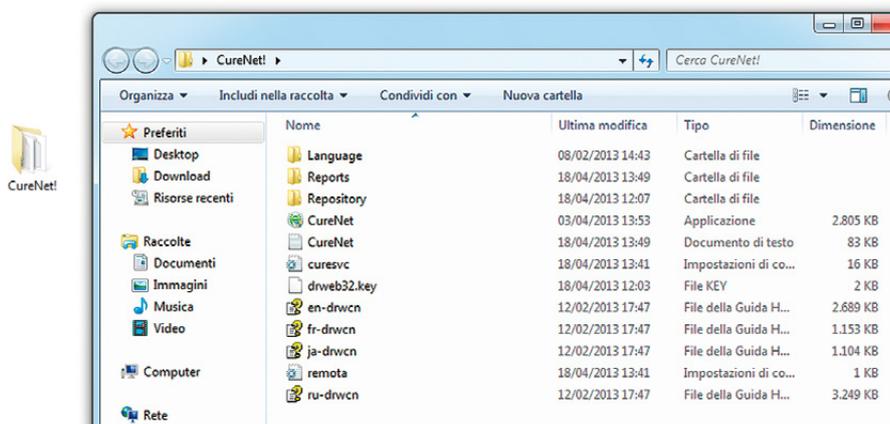
Le istruzioni dettagliate su come utilizzare il prodotto, impostare la scansione, creare e salvare profili sono disponibili nel [Manuale dell'amministratore di Dr.Web CureNet!](#)

Utilizzo di Dr.Web CureNet!

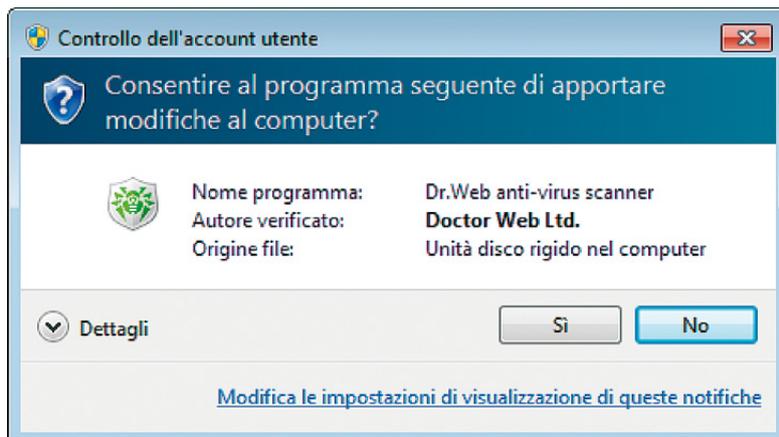
Le scansioni periodiche dei computer sono consigliabili. Una delle ragioni è perché file controllati dal file monitor e memorizzati sul disco potrebbero contenere virus sconosciuti al momento del controllo. Tali virus possono essere rivelati durante le successive scansioni.

Per eseguire una scansione, è necessario:

Aprire la cartella in cui sono stati salvati i file di Dr.Web CureNet! quando l'utility è stata avviata per la prima volta (di default, è la cartella **CureNet** sul desktop) e lanciare il file **CureNet**.



6. Se si usa Windows 7, di seguito sarà necessario confermare l'avvio del programma cliccando sul tasto **Yes**.



I passi successivi di utilizzo di Dr.Web CureNet! sono uguali a quelli descritti sopra.



Verificare l'operatività del prodotto

- Per ottenere un malware di test, aprire il browser e usare il seguente indirizzo



- Si apre una pagina web. Scorrerla fino al seguente testo

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

e poi scegliere una variante di download, per esempio, la prima eicar.com.

- Memorizzare il file scaricato sul desktop del computer da scansionare.

Attenzione! Se Dr.Web CureNet! si usa come programma complementare agli antivirus dei terzi, è necessario disattivare gli antivirus dei terzi prima del salvataggio del file di test.

- Avviare Dr.Web CureNet! ed eseguire una scansione antivirale.



Doctor Web, 2003–2013



Russia, 125124, Mosca, la 3° via Yamskogo polya, 2-12A,

Tel.: +7 (495) 789-45-87 (centralino)

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

www.drweb.com

www.freedrweb.com

www.av-desk.com

www.drweb-curenet.com