


Rescue CD User's Guide

When to Use the Rescue CD

There are two main situations when you should use the Rescue CD:

- The computer no longer starts, as the operating system has been corrupted by malware. In this case you can use the Rescue CD to scan the computer and quarantine the malware. This may allow the operating system to start properly again.
- If you suspect that your security software has been compromised by malware. You can use the Rescue CD to check this, as it is independent of the operating system.

If the computer cannot be recovered, you can also use Rescue CD and a USB drive to save important data. Note that if you copy data from the computer to the USB drive, this data may contain malware. The Rescue CD cannot scan encrypted disks. This includes for example, Windows Vista BitLocker disk encryption.

 *Using the Rescue CD on a working operating system may rename essential system files and so cause your operating system to no longer start. If this happens you can use your operating system repair disk to reinstall the operating system. Note that this may reinstall a fresh operating system and so remove any personal settings and files you have.*

System Requirements

To use the F-Secure Rescue CD, the computer must meet the following minimum requirements:

- x86 compatible
- at least 1024 MB of RAM
- startup from a CD or USB
- connected to the Internet or be able to use a USB drive

Using the Rescue CD

1. Place the F-Secure CD in your CD drive and switch the computer on. After a few seconds you should see a prompt that shows F-Secure Rescue CD.



If you do not see the F-Secure Rescue CD screen you should check that the computer can start from CD. To do so:

1. *Restart the computer.*
 2. *Hold the BIOS options key while the computer starts, usually this is one of F1, F2, F10, F12 or DELETE. If none of these work, consult the documentation for the computer.*
 3. *Change the option that determines which device the BIOS tries to find the operating system from, so that the CD drive is searched first.*
 4. *Save settings and restart the computer.*
2. Press ENTER within 15 seconds after you see the prompt to start Rescue CD.
 3. Use the arrow keys to select **Start scan** and press ENTER.



*If you connect to the Internet through a proxy, select **Proxy settings** before you start.*

4. Wait for the latest virus definition database to be downloaded from F-Secure. This is finished when you see the **End User License Agreement** window.
5. Press PAGEDOWN to read the agreement and then select **Next** and press ENTER.
6. Select **I Agree** and press ENTER if you agree to the terms.
7. Select which drives you want to scan.



The Master Boot Record is a small section at the start of a disk that can be used to hide malware. You should scan the Master Boot Records.

8. Select **Proceed to scan** and press ENTER.
9. When the scan is finished, press ENTER to see the scan report.
10. If any malware were found, you can see which files were renamed by the Rescue CD. Select **Next** and press ENTER when you are ready to continue.
11. Select **Restart** and press ENTER.
12. Wait for 5 seconds for the computer to switch off. The computer restarts.
13. If you see the same screen as you did in step 1, wait for 15 seconds for the computer to start normally.

Using a USB drive

You can download the Rescue CD updates to a USB drive using a healthy computer that has an Internet access. This USB drive must be more than 1024 MB and less than 16 GB in size for the Rescue CD to recognize it. In addition, the USB drive must have at least 400 MB of free space. You can use this USB drive to fix a computer that cannot connect to the Internet and so cannot download the Rescue CD updates.

Recommended method:

1. Create a new directory called *fsecure* to the USB drive.
2. Go to the *fsecure* directory and create a directory called *rescuecd* under the *fsecure* directory.
3. Start the Rescue CD while the USB drive is still connected to the computer. When the Rescue CD starts, it finds the USB drive you have configured for it.
4. Select **Next** when the Rescue CD notifies you that the memory stick has been found.
5. The Rescue CD starts to download the latest databases. The Rescue CD has finished downloading databases when the end-user license agreement appears.
6. The memory stick is ready and you can remove the CD and the memory stick.
7. Insert the memory stick to the computer you want to fix and use the Rescue CD to boot the computer.

Alternative method:

1. On a healthy computer with Internet access, Insert an empty USB drive.
2. Open <http://download.f-secure.com/latest/fsdbupdate9-packed.run> with your web browser. Your web browser asks you what you want to do with the file in the web site.
3. Choose to save the file to your computer.
4. After the web browser has finished downloading the file, go to the directory where you downloaded the *fsdbupdate9-packed.run* file and copy it to the USB drive.
5. Insert this USB drive in the computer on which you want to use the Rescue CD.
6. Follow the instructions in [Using the Rescue CD](#).

Automate the Scanning Process

You can set up a USB drive to make the Rescue CD process almost automatic. This drive must be 1024 MB or greater in size. You can:


- Preload virus definition database updates to the USB drive to fix a computer without Internet access.
- Define proxies that Rescue CD will use to download updates.
- Set Rescue CD to skip the wizard and automatically clean the computer.

To set up your USB drive:

1. Create a new directory called *fsecure* to the USB drive.
2. Go to the *fsecure* directory and create a directory called *rescuecd* under the *fsecure* directory.
3. Start the Rescue CD while the USB drive is still connected to the computer and run through the steps described in [Using the Rescue CD](#). This USB drive now contains a virus definition database and is ready to use.

Once you have completed the above steps you can also set up the USB drive so that it runs through the scan process automatically:

1. Open the file `fsecure/rescuecd/config` with a text editor.
2. Add the text `timeout=1` to the file. With this value, you have 1 second between each step of the Rescue CD process before the program selects the default option automatically.

 If you can access the Internet from the infected computer only through a proxy, you can define proxy settings in the same config file to download updates through the proxies you define. To define a proxy, add the following line to the config file:

```
http_proxies=http://user:password@address:port
```

Note that `http://`, `user`, `password` and `port` are optional and `address` is mandatory. For example, the following is a valid proxy setting:

```
http_proxies=sam:abc123@proxy.company.com:8090,http://sally@proxy.us.company.com,proxy.global.company.com
```

To use the USB drive, insert it into the infected computer and use Rescue CD as normal.

Making bootable USB drive

If you do not want to use the CD, you can make a bootable USB drive that has the whole rescue CD content. You need the UNetbootin application to make a bootable USB drive.

Using Unetbootin:

1. Download the Unetbootin application from its homepage (<http://unetbootin.sourceforge.net>).
2. Insert the memory stick that you want to use.
3. Run the Unetbootin application.
4. In the main window, choose *Diskimage* and then click "...“ to browse for the rescue-cd ISO image file.
5. Click OK to install files from the image file to the memory stick.
6. When the installation is complete, click **Exit**.
7. Download the Rescue CD updates to the USB drive to make a fully self-contained drive that does not require any network access. Follow the instructions in the previous section for more information.

You can remove the memory stick now and use it in a computer that you want to scan.

DISCLAIMER

"F-Secure" and the triangle symbol are registered trademarks of F-Secure Corporation and F-Secure product names and symbols/logos are either trademarks or registered trademarks of F-Secure Corporation. All product names referenced herein are trademarks or registered trademarks of their respective companies. F-Secure Corporation disclaims proprietary interest in the marks and names of others. Although F-Secure Corporation makes every effort to ensure that this information is accurate, F-Secure Corporation will not be liable for any errors or omission of facts contained herein. F-Secure Corporation reserves the right to modify specifications cited in this document without prior notice.

Companies, names and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of F-Secure Corporation.

This product may be covered by one or more F-Secure patents, including the following:

GB2353372, GB2366691, GB2366692, GB2366693, GB2367933, GB2368233, GB2374260

Copyright © 2013 F-Secure Corporation. All rights reserved

