****

**Reivers Service Desk Manual**

**Written by the staff of the service desk**

**Table of Contents**

**Mission Statement**

Our mission at the Reiver help desk is to deliver extensive support and to meet and exceed the expectations of our customers. The Reiver help desk prides itself on fulfilling the needs of others and delivering this service with a smile.

We will achieve this by:

* Laying out clearly defined expectations
* Offering extensive support at first contact
* Offering multiple points of contact
* Working to continually satisfy our customers

**Policy**

We have a clearly defined set of policies that our staff take pride in abiding by and fulfilling.

**Goals**

The goals of all our staff is to meet and exceed the expectations of our customers and to provide them with the services that they deserve.

**Purpose**

We are to be the single point of contact for all IT related incidents on campus.

**Procedures performed**

The following is some individual procedures performed by the service desk and detailed outlines on how they are done.

***Virus removal***

By far the most reported incident in the service desk is of a virus or some sort of malware on a client’s computer. The cause of a virus can vary, but asking the customer about his browsing habits can help in teaching them about prevention of future incidents. Remember that all data must be backed up before proceeding.

The standard procedure for virus removal goes as follows:

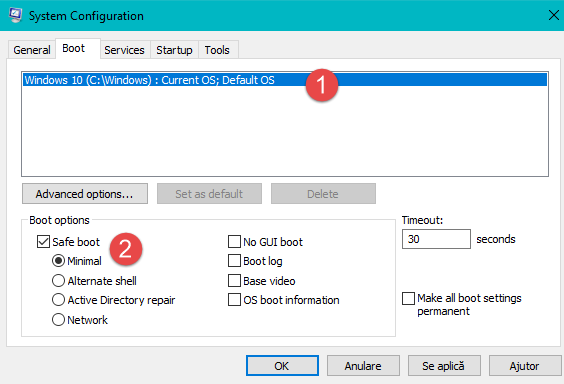
1. Download an antivirus executable onto a flash drive or other medium.



A popular antivirus tool that the help desk likes to use is MalwareBytes. Go to [www.malwarebytes.com](http://www.malwarebytes.com) and download the executable. Put the executable on a flash drive or other portable medium

1. Boot the problem computer into safe mode.

An easy method of going into safe mode is by running msconfig.exe and enabling safe mode on next boot followed by a restart into safe mode



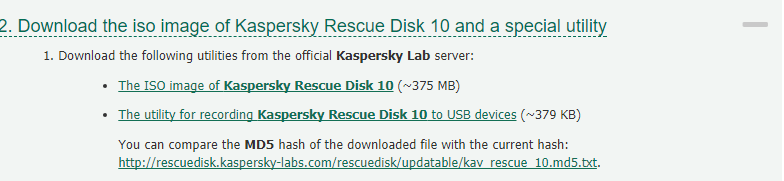
Another way of doing this is to hit restart while holding the shift key, which in turn will bring you to an option page.

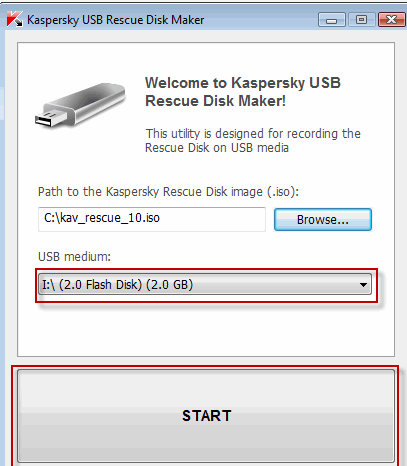
When on the option page follow this combination of settings: Troubleshoot🡪Advanced Options🡪Startup settings. You can then select the safe mode option which will be represented by a number. This will bring up safe mode on the next boot.

1. Once in safe mode plug in your removable media and install the antivirus. Run the antivirus while in safe mode and try to remove the virus. Be sure to restart and verify that the virus has been removed.

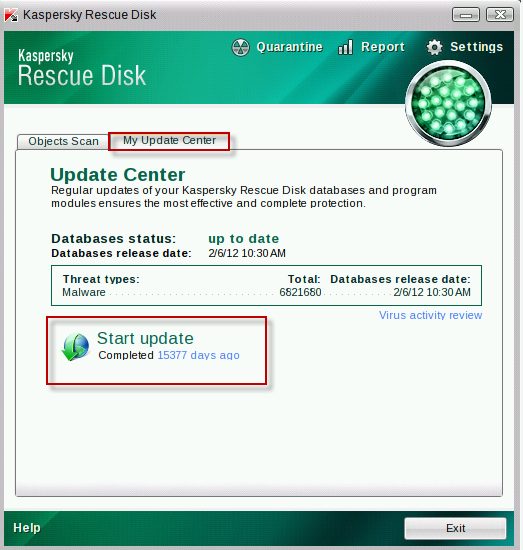
Sometimes a virus cannot be removed this way. And requires more intrusive methods. One such method is to install an AV live medium to a flash drive and boot into it. A favorite of the help desk is the Kaspersky live antivirus medium

1. To find the ISO image and the installer go to <https://support.kaspersky.com/8092#block2> and follow the instructions to the links in the manual.



1. After downloading both utilities you need to install the utility for recording the Kaspersky Rescue Disk 10 OS. Install the utility and open it.
2. 

First you click browse, find your ISO file, select your USB medium, and allow it to image the disk.

1. You must then restart the machine and enable boot from removable disk from the BIO’s or UEFI. Be sure to have the flash drive plugged in before the computer POSTs.
2. You will boot into Kaspersky Rescue Disk 10, which navigating shouldn’t be too difficult if you are familiar with Linux. Enable the GUI interface and open the rescue disk program preinstalled to the OS.

It is extremely important that you update the databases before proceeding with the scan.

1. Finally click on objects scan, select your Windows Partition and scan it for Malware. Remove the viruses and attempt to boot back into windows.

***Screen Repair***

Laptop screen repair