ESET Tech Center

Starting Full Disk Encryption (standalone)

Anish | ESET Nederland - 2018-03-07 - Comments (0) - ESET Endpoint Encryption

The following instructions are for encryption of system disks on standalone workstations. If your system is managed by an Enterprise Server please see this article instead: KB101 - How to encrypt a hard drive using a managed version of DESlock+?

To start encryption please follow the steps below:

Ensure you have a current backup of the disk, ideally a sector level backup, before initiating this process.
Ensure you have installed DESlock+ and setup a **Pro** licence, please see here for details: KB124 - How do I set up my version of DESlock+?
Right click the DESlock+ Icon next to the clock. Select the **Full Disk Encryption\Full Disk Encryption** menu.

In the DESlock+ Full Disk Encryption dialog click the **Manage Disks** button.

Click the **Finish** button to allow the system to restart and verify the system boots using Safe Start.

A warning will appear explaining Windows will restart. Ensure you have saved your work then click **OK** to allow the system to restart.

When the machine restarts you should see the Safe Start count down screen, you can either wait 60 seconds or press a key.

When Windows loads login to DESlock+.
Providing the safe start process was successful a dialog will appear explaining it was successful. Click **OK** to continue.

If you are using a tablet or other touch interface device you may receive a warning at this point that a USB keyboard will be required to start the machine once it is encrypted. Click **OK** to continue.
Select the Whole Disk or partition to encrypt. Then click the **Next** button.

A dialog will appear detailing that you should have a backup before proceeding. Click the checkbox **Check to confirm and continue**then click **Next**.

The admin password will be displayed on screen. It is vital that a backup of this password is taken. You will need this to manage or decrypt the system in the future and it can be useful as an extra emergency login should the normal passwords be forgotten.
Click the **Save to File** button to save a copy of the admin password. You will need to specify a storage location that is not on the system i.e. removable or network storage. You can also optionally print a copy of the admin password.
Once the password has been saved, enter the admin password into the **Confirm password** entry then click **Next**.

Enter your username and password to use with the system then click **Add** to add this to the user list. This information will be required to start the machine in the future so you should make certain you know what values are chosen.
You can also add further logins for other users with different passwords as required. Click **Next** once you are happy with the user list.

Set the check box labelled **Check to confirm the above information is correct**. Then click the **Next** button.

A progress bar will appear detailing the encryption progress.

The machine can be used while encryption is progressing. You can restart, shutdown etc. as normal and the encryption process will resume when Windows loads.
Once encryption has completed a notification will pop up indicating this.

Related Articles

KB247 - How to start a system that is Full Disk Encrypted

KB70 - How do I perform a full sector by sector backup of my hard drive?

KB177 - What is DESlock+ Full Disk Encryption Safe Start

KB164 - Why do I need an admin password?

KB234 - Safe Start has prevented Full Disk Encryption starting