ESET® Cybersecurity
Progress. Protected.

How do I backup my data?

Anish | ESET Nederland - 2018-02-16 - Reacties (0) - ESET Endpoint Encryption

This article will explain how to take backups of your data in the correct way while DESlock+ is installed. As with all backup plans, please ensure that you fully test your backup and restore process to ensure that everything is setup and working correctly before deploying to live data. Failure to do this may lead to permanent loss of data.

Encrypted or non-encrypted data backups

It is important to understand whether or not you want a backup of your data in an encrypted state or in a non-encrypted state.

Encrypted

You may want to backup your data in in an encrypted state to keep it protected. However, if you do this then you must make sure that you have access to DESlock+ with the correct key-file and Encryption Key or password, in order to regain access to the backed up data.

> **Important**
> You must **not** store key-file backups on encrypted media as this will prevent access to the Encryption Keys when they are required.

KB38 - Why should I make a Key-File backup?

KB58 - How do I backup my Key-File?

Non-encrypted

Having a non-encrypted backup of your data means that if you lose access to DESlock+ key-file, Encryption Key or password that protects your data, then your backup will still be accessible. If you want a non-encrypted backup of your data, then you must ensure that the data is in a non-encrypted state before carrying out the backup.

Different types of backup

File level backup

Most backup software will take backups of data on a file and folder level. This is designed to backup selected files and folders on your system. In order to have a backup of non-encrypted data, your backup software needs to be running under the correct Windows profile and be setup to backup the correct locations. If everything is set correctly and you are logged into DESlock+, your backup software will be able to backup data stored inside an Encrypted Folder or a Virtual Disk (this must be mounted in order for backup software to be able to copy the data). For more information on this please read this article:

[KB244 - Windows User context and encryption](#)

Sector level backup

Hard disks are made up of lots of sectors and each sector stores information. These sectors of data are what make up the contents of your hard disk. Taking a sector level backup will completely backup all of the sectors on your hard disk. This is a thorough backup and can take a long time, but the benefits of taking a backup in this way allows you to restore a machine to a specific state. With a sector-by-sector backup you can even restore changes made to your operating system.

Full Disk Encryption (FDE)

If you plan to FDE your machine, we recommend taking a sector level backup beforehand. This will allow you to restore your disk to its non-encrypted state in the event of losing access to your machine.

With backup software like Acronis, there are different ways of performing a sector level backup. While your machine is FDE, you should **not** run a sector-by-sector backup from within Windows itself. Instead you should create bootable media (CD) that takes a sector-by-sector backup outside of Windows. You must ensure that you include unused sectors in the backup, as these sectors are required due to the encryption. It is also worth noting that the backup will not compress due to the encryption. If you need to restore the image in the future, then you must make sure that the disk you restore to has the same amount of space or more as the image you are restoring from. You will not be able to resize

or modify the restored disk without first decrypting the disk. Due to these points it recommended that you take regular file level backups.

Please note, if you use both the FDE and file level encryption features of DESlock+, then ensure that you understand how to backup encrypted data correctly.

For more information on performing a sector level backup, please read this article:

[KB70 - How do I perform a full sector by sector backup of my hard drive?](#)

Enterprise Server backup

We recommend that you install your Enterprise Server within a Virtual Machine (VM). This makes the backup and migration of your Enterprise Server much easier. If you need to take a backup of your Enterprise Server, then please read this article:

[KB296 - Backing up the Enterprise Server, or migrating an Enterprise Server to a new host](#)

[KB278 - Using the Enterprise Server in a virtual machine environment](#)

---

keywords: backup, encrypted, data, file, level, sector-by-sector, key-file