ESET Tech Center

How to encrypt a hard drive using a managed version of DESlock+?

Anish | ESET Nederland - 2018-01-24 - Comments (0) - ESET Endpoint Encryption

If you are a managed user

If you are using DESlock+ in a managed environment (i.e. DESlock+ on the workstation is under the control of a DESlock+ Enterprise Server) and you have a Professional licence, your workstation is able to receive a Full Disk Encryption command.

Request that your Enterprise Server admin issues a full disk encryption command to your workstation.

If you are a DESlock+ Enterprise Server administrator

To issue a full disk encryption command to a workstation, you will need to select the user associated with the workstation (the user will need to have been issued a Professional licence) and double click on the user to open a new window called the 'User Card'.

When this this window opens, click on the 'Workstation' tab. at which point, you will see all of the workstations with which the user is associated. You will also be able to see the Full Disk Encryption status of the workstation under the 'FDE status' column.

Click the appropriate Workstation to which you wish to send a Full Disk Encryption command and then click the 'Full Disk Encrypt' button. This will start the Full Disk Encryption wizard as seen below.

If you do not wish to see the initial FDE wizard window when sending a Full Disk Encryption command, put a tick in the box next to 'Don't show this page again' and click the 'Next' button.

You will now be shown the Compatibility Checks stage of the FDE wizard. This stage will inform you if there are any incompatibilities on the workstation to which you are about to send the command.

Select the appropriate start mode depending on the compatibility checks. i.e. if no incompatibilities have been reported (you have a green topped panel) you can select the 'Normal Start Mode'. If you have possible incompatibilities, it is advisable for you to select the 'Safe Start Mode'. For more information on Safe Start, please see our relevant kb article. Once you have selected the appropriate start mode, click 'Next'.

In the next stage of the FDE wizard, you will be able to set the FDE login details for the user such as their Username, password etc. It is at this point that you can set whether the user's password is set to Single Sign-On. Please click here for more information regarding Single Sign-On. Once you have set your preferences for the user, click 'Next'.

If this is the first Full Disk Encryption command that you are sending from the Enterprise Server then you will be prompted to set the FDE admin username and password. The FDE admin username and password is 'sticky' and therefore will be remembered for each subsequent FDE command you send. When setting your FDE admin username and password, it is not advisable for it to be the same as the Enterprise Server admin username and password, as doing so would compromise the security if someone were to discover what the FDE admin username and password is. click the 'Next' button.

The next stage of the FDE wizard will give you the option of either encrypting the whole of the drive or encrypting a partition of the drive. The screenshot above depicts that the whole of the drive will be encrypted and that the drive consists of two partitions. Select your preference and click the 'Next' button.

At this point, all that is left to do is click the 'Start Encryption' button. In doing so, the Full Disk Encryption command will be sent to the workstation. This will be apparent by the workstation icon being orange and also under the 'FDE status' the status will be set as 'Start FDE Pending'

For the Full Disk Encryption command to be picked up by the workstation, you can do one of 4 things:

1. You can wait for the background check period to elapse (this is set by default to take place every 60 minutes)

2. You can double click the DESlock+ Icon in the Notification Area to log out and then double click to log back in. Each time a user logs in to DESlock+ it will perform a background check to see is any updates have been posted while the user was logged off.

3. You can right click the DESlock+ icon in the Notification Area and then click 'Enterprise Sync' from the context menu which will force a background check.

4. You can double click the Enterprise Deployment Client icon from the Notification Area which will perform the same action as number 3.

Once the FDE command has been processed, the machine will either restart the system or start the Full Disk Encryption process depending on the start mode selected.

Keywords: Full Disk Encryption start initiate hard drive whole