

ESET Tech Center

Knowledgebase > ESET Endpoint Encryption > How to initiate Single Sign On.

How to initiate Single Sign On.

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

Single sign on is a feature in DESlock+ which is only applicable when either a client machine is to have a Full Disk Encryption command sent to it or if the client machine is already Full Disk Encrypted.

Sending a new Full Disk Encryption command with Single Sign-On activated

At the point of sending a Full Disk Encryption command to a client machine from the Enterprise Server, you will have the following Full Disk Encryption user interface appear



You can check the box next to 'Don't show this page again' if you wish then click 'Next' to see the Compatibility Checks page. Select the relevant start method and click 'Next'.



You will now need to set your preferences for the user's account and then click 'Next', **Please note that the Single Sign-On (SSO) username will be what is in the username text box and will not be the same as the user's Active Directory username, unless you set it to be the same in the FDE Username text box as shown below.**

At this point, if you want to enable Single sign-on, you will need to put a tick in the box next to 'Single Sign-On', click 'Next'.



At this point, if this is the first time of issuing a Full Disk Encryption command, you will be prompted to set the FDE Admin Username, Password and number of password attempts. This is sticky and therefore once set, will be applied to all subsequent FDE commands sent. Click 'Next', the following page will prompt you for your choice of either encrypting the entire disk or a partition. Select your preference or if wishing to encrypt the entire disk, leave the settings as

they are and click 'Next'. The final window will require you to click the 'Start Encryption' button as shown below.



From the client machine, at the point of the Full Disk Encryption command being applied to the machine, the following window will appear



At this point the user will need to enter their network password, click 'Verify' and then if all is correct, click the 'OK' button. When the user is presented with the bootloader screen at boot up, their password will be the same as their username will be as displayed in the box and their password will be the same as their network password.

Sending a Single Sign-On update to a user that is already Full Disk Encrypted

If a user already has their workstation Full Disk Encrypted, you can still send them the ability to enable Single Sign-On by performing the following steps;

Log into the Enterprise Server to or click 'Proxy Sync' to ensure that the user is up to date, double click the user to which you wish to send the Single Sign-On command and click on the 'FDE Logins' tab. Highlight the user and click the 'Change' button.



You will now be presented with the following user interface window. At this point you will need to change the setting from 'Normal login' to Single sign-on (SSO) login' and click the 'Post Change' button.



The post will now be sent to the client machine and when the client machine has either performed its background checks after the time period specified within the Enterprise Server, the user has logged out and back into DESlock or has performed an 'Enterprise Sync' by right clicking on the DESlock+ icon in the Notification Area (formally known as the system tray), the user will be presented with the following window.



At which point, they will be required to enter both their current Pre-boot

password and their Network Password, then click 'Verify' and if all is correct, click 'OK'.

The user's Pre-boot password will now be changed to their Network Password, the user will now be able to continue working normally.

keywords: SSO single sign-on sign on network password domain