ESET Tech Center

How to remotely disable a workstation

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

It is possible to use settings and commands from the Enterprise Server to disable access to data on a workstation. This can be useful if a machine is lost or stolen.

These options are only available for Workstations that are under the management of an Enterprise Server.

Deletion of encryption keys (Deactivation)

The encryption keys within a users key-file provide access to granular encrypted data (e.g. Encrypted Files, Encrypted Folders, Encrypted Removable Media, Encrypted Emails etc.).

By using the deactivate command the users key-file will be deleted removing access to their copies of the encryption keys. In order for the command to be received the target machine must be connected to the Internet and logged in to the Windows profile that contains the users key-file.

To send a deactivate command follow the steps below:

Login to the Enterprise Server.
Select the **Users** branch or user sub team containing the user you wish to deactivate.
Select the user to deactivate in the list of users.
Click the **Details** button.
Select the **Workstations** tab.
Click the **Deactivate** button.

Set the check box next to the warning **Are you sure you want to deactivate this user?**
Click the **Deactivate** button.

The command will be posted to the DESlock+ cloud and processed by the client machine when it is connected to the Internet and the Windows user

profile of the user in question is logged in.
On receiving the command the user will be logged out of their key-file, their key-file reset and the activation dialog will appear again as if they were a new user.

It is possible to reactivate a machine in the future that has been deactivated to regain access to granular encrypted data if required.

Disabling of a full disk encrypted system (Disable)

If a machine is full disk encrypted then the FDE logins can be removed to prevent the machine from being able to be started using those credentials.

When removing the logins you can choose to leave the FDE admin login if required so that the login can still be used to start the machine.

This process also has the option to force the machine to reboot upon processing the command so any user currently using the system will be stopped from using the machine.

The disable command requires that the machine is connected to the Internet in order for the command to be received.

It is important to note that if a machine has been disabled and all FDE logins removed it will not be possible to access any of the data on that system again. It will note be possible to generate a recovery CD to decrypt the system.

To send a disable command follow the steps below:

Login to the Enterprise Server.
Select the **Workstations** branch or workstation sub team of the navigation tree containing the machine you wish to disable.
Select the machine in the list of Workstations.
Click the **Details** button.
Click the **Disable** button.

Select which FDE logins to remove and optionally set the option to **Reboot the workstation after processing command**.

Click the **OK** button.
Confirm your Enterprise Server login password to proceed with the action

then click the **OK** button.
If the option to reboot was chosen the system will show a blue screen on receipt of the command and the system will restart depending on the Startup and Recovery settings of the system.

If the option was set to delete all logins then the boot menu will no longer be shown and it will not be possible to start the system.

If the Enterprise Server receives a receipt of the command completing it will still show the encrypted workstation but there will be no FDE Logins tab displayed when viewing the workstations details.

Timed expiry

The Workstation Policy contains options to force the client to disable automatically if it is unable to contact the DESlock+ cloud for a specified period of time.

It is important to note that you should use these options with caution. If for some reason the machine is unable to access the cloud for the specified period of time the disable action will be performed. Therefore if you intend to use the options they should be set with an amount of leeway to allow for network problems, user vacations, machine repairs and other unexpected events that could delay connection to the cloud.

The settings that control this capability are within the **Server Communication Settings** section of Workstation Policy. The relevant options are detailed below:

Client disable warning period - When set to a non-zero value this is the amount of days that can pass before the user is displayed a warning that their DESlock+ will disable.
Client disable warning message - The warning text to display once the warning period has been reached to remind the user that they need to connect the machine to the Internet. This message can be customised as required.
Client disable period - When set to a non-zero value this is the amount of days that can pass before the expiry action is performed.
Client disable message - At the point of performing the expiry action this message will be displayed to the user explaining what has happened. This

message can be customised as required.
Expiry action to perform - This can either be set to deactivate the users key-file or to remove all user FDE logins. The FDE admin login will remain if this happens to allow the admin to recover access should it be required.

For details of the process to modify a workstation policy, please see this article:
How do I modify workstation policy?