ESET Tech Center

How DESlock+ Removable Media Encryption (RME) policies work

Anish | ESET Nederland - 2018-01-30 - Comments (0) - ESET Endpoint Encryption

DESlock+ Removable Media Encryption (RME) policy can be complex to configure correctly because of the interaction of both the Workstation Policies and the users' Key File policies.

In basic terms, Workstation Policy will control the default access to removable media, and the Key-File policy configured for the user will override or supersede these policies *when* the user is logged in. When the user logs out of DESlock+, the Workstation policy will come back into effect.

(RME) can be set to **File** or **FDE.** See our article here KB322 - What are the removable media encryption modes - (file / full disk)?

Note: Optical Media can only be **File** encrypted, if the policy being used is **Force Choice** Optical Media will automatically be **File** encrypted.

Key

Throughout this article the following indicators are used to describe access to removable devices

Designation	Meaning
R/W	The user has full read and write access to the device. There are no restrictions imposed by DESlock+.
R/O	The user only had read access. Write access is blocked by DESlock+.
Blocked	The device is inaccessible. DESlock+ will block all attempts to read from or write to the device. The device will still be visible.
Hidden	DESlock+ hides the non-encrypted data so it is still present but cannot be accessed. Only the encrypted area will be accessible meaning the user only has access to existing encrypted data and, when saving new data, can only save it to the encrypted area.

Workstation Policies

The basic three policies that control DESlock+ RME are defined in the Workstation Policy. These are **Open**, **Read-Only** and **Blocked**.

Workstation policy will be in effect:

> before the user has activated on a workstation; ***and***
> when an activated user logs out of DESlock+.

You should bear these two scenarios in mind when designing a policy configuration for your organisation.

RME Encryption Mode	RME Type	Workstation Policy Mode		
		Open	Read-Only	Blocked
Non-encrypted device	n/a	R/W	R/O	Blocked
Encrypted with RME FDE	n/a	Blocked	Blocked	Blocked
Encrypted with RME File	Encrypted area	Blocked	Blocked	Blocked
	Non-encrypted area	R/W	R/O	Blocked

Using DESlock+ Go when not logged in

If an RME file mode device is connected when the user is not logged into DESlock+ (either because they are not yet activated, or they have logged out) a policy can used to allow or deny access to the device using DESlock+ Go.

NB If this policy allows DESlock+ Go when not logged in, then after the user enters their password they will receive the same access as if they had plugged the device into a workstation without DESlock+. This means that no workstation policies will be applied and thus access via DESlock+ Go may be different than when accessing the device when logged into DESlock+ normally.

Deleting Files

A policy also exists which can allow access to delete or move files when the device is in a Read-Only mode. This can be used to move or delete files, such as in the case where the users wishes to move files from the non-encrypted area to the encrypted area so they can be modified. Or they may wish to simply remove files from the non-encrypted area to make some free space on the device to store more encrypted data.

Key-File Policies

The policies that control DESlock+ RME, defined by the Key-File, are much richer than just Workstation Policy because the Key-File has encryption abilities. Therefore Key-File policy shares the basic modes of **Open**, **Read-Only** and **Blocked**, but it can additionally force encryption in one of three ways: **Force FDE** = force RME FDE mode encryption; **Force file** = force RME File mode encryption; or **Force choice** = Force the user to choose a method of encryption.

DESlock+ group policy also has an additional policy which controls how a RME file mode encrypted device is handled. RME file mode works normally by creating a folder called Encrypted on the root of the stick. Everything in this folder is encrypted, and everything outside this folder is left not-encrypted. This can be useful in a BYOD scenario where you do not wish to encrypt users' personal documents that may already exist on the device, but you which to ensure while in the corporate environment they can securely store data on the device.

RME Encryption Mode	RME Type	Key-File Policy						
		Open		Read-Only		Blocked	Force (File, FDE, Choice)	
		Read all/write encrypted		Read all/write encrypted		Read all/write encrypted	Read all/write encrypted	
		On	Off	On	Off	n/a	On	Off
Non-encrypted device	n/a	R/W	R/W	R/O	R/O	Blocked	R/O	Blocked

Encrypted with RME FDE	n/a	R/W	R/W	R/O	R/O	Blocked	R/W	R/W
Encrypted with RME File	Encrypted area	R/W	R/W	R/O	R/O	Blocked	R/W	R/W
	Non-encrypted area	R/W	Hidden	R/O	Hidden	Blocked	R/O	Hidden