ESET Tech Center

Trusted Platform Module (TPM) FAQ

Anish | ESET Nederland - 2018-02-20 - Comments (0) - ESET Endpoint Encryption

Are there any restrictions?

None of the TPM modes allow Workstations to be adopted into an Enterprise Server. If a Workstation is deleted or a Workstation needs to be transferred from one Enterprise Server to another, they will have to be decrypted first. You will not be able to change authentication mode without fully decrypting the Workstation first. This also applies to encrypted Workstations that are not using a TPM mode that have been upgraded to the latest version of DESlock+.
TPM encryption is only available via an Enterprise Server, it is not supported on an unmanaged client.
If you 'Clear' the TPM, all the current encryption keys being stored will be lost and the Workstation will not be able to boot. If you 'Clear' the TPM after encryption you will need to use the recovery ISO from the Enterprise Server: KB346 - DESlock+ Full Disk Encryption Recovery Overview

Disaster recovery

In the event of a hardware or Windows fault, you will need to decrypt the disk using the FDE Recovery Image from the Enterprise Server: KB346 - DESlock+ Full Disk Encryption Recovery Overview
You can not move the disk to another physical Workstation and boot it, due to the TPM security.
In the event that your Enterprise Server host machine is inaccessible, you will lose the ability to create recovery ISO's in order to manually decrypt your TPM enabled Workstations.

Are there any things I need to be careful of?

You must be very careful with the TPM. If you Clear it, attempt to change the Owner password or have it changed due to hardware failure, you will be unable to correctly boot the Workstation and will need to decrypt the disk.

It is therefore important that you maintain backups of your Enterprise Server: KB296 - Backing up the Enterprise Server, or migrating an Enterprise Server to a new host

Is there anything I should do?

Keeping regular file level backups of your data is important. It is usually much faster and simpler to restore your back up files than it is to decrypt data, especially if the disk or data is damaged or partially corrupted.

This applies to both the encrypted Workstation as well as your Enterprise Server.

KB63 - How do I backup my data?

How many attempts do I get to log in?

DESlock+ TPM support uses Active Directory Group Policy settings.

The Default Workstation retries value varies from 32 to 31 (Windows 10 Creators edition) and could vary in other O/S updates, or in other environments.

The "interval" value is the number of times each retry stays active. (Default is 2 hours)

How this works is if you have an interval value of 2 hours and set the number of retries to 31 and use them all then it will take 2 hours to be able to have one more attempt, or wait 4 hours in order to have two more attempts.

This is fully reset by doing a TPM PIN/Password recovery: KB446 - TPM Recovery

Related Articles

KB442 - Starting Full Disk Encryption using a TPM (Trusted Platform Module)

KB430 - Trusted Platform Module (TPM) Support

Keywords: Full Disk Encryption start initiate hard drive whole tpm transparent pin