ESET Tech Center

Knowledgebase > ESET Endpoint Encryption > Trusted Platform Module (TPM) Support

Trusted Platform Module (TPM) Support

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

What is a Trusted Platform Module (TPM)?

The TPM is a form of hardware security that stores cryptographic information about the Workstation it's connected to.

What are the minimum requirements to use a TPM with DESlock+?

DESlock+ Full Disk Encryption supports TPM (Trusted Platform Module) in the following environments:

- Windows 10 and Windows 8.1
- Boots using UEFI
- Has a TPM version 2.0
- Using DESlock+ managed client version 4.8.17 or later
- Using DESlock+ Enterprise Server 2.9.0 or later

How can I tell if my computer is supported?

If you have activated the Workstation with an Enterprise Server, look at the **Workstation Details** page: [KB332 - How do I view Workstation Details?]

On the Workstation Details tab, you will see something similar to the following image, which represents a computer ready to use FDE with a TPM.

Boot Mode may say **Legacy BIOS**, this mode does not support TPM.

TPM Status may also say one of the following

- Trusted Platform Module (TPM) status is not available
  - This means your computer either has an older version TPM, or no TPM at all. You will not be able to use FDE with a TPM.

The Trusted Platform Module (TPM) is unavailable

> This means your computer has a supported TPM, but it requires some additional reconfiguration to work with DESlock+: KB442 - How to take ownership of the TPM (Trusted Platform Module)

TPM Version states the manufacturer and version of the TPM module, it is only shown if there is a TPM 2.0 module.

What do the different TPM FDE modes do?

Username and Password

This mode operates in exactly the same way as has previously been available, only it uses the TPM for storage of the encryption key.

KB101 - How to encrypt a hard drive using a managed version of DESlock+?

> If you require multiple distinct pre-boot users, then you should choose the **Username and Password** mode, either with or without TPM.
>
> It is also the only mode that supports Single Sign-On.

KB187 - What is Single Sign-On

PIN Code

This mode provides a single method of authentication, a numeric PIN. There is one PIN for all users of the computer.

> If you only require a user to be able to start the computer, as long as they know the PIN, you can choose **Pin Code** mode.
>
> This will allow anyone that knows the PIN to start the computer, however it does mean that any user that has access to that Workstation could change the PIN.

No Extra Authentication

This mode boots the computer without any pre-boot interaction, all security is handled at the Windows login and requires the user to have a Windows Password.

> If you just require the computer to be encrypted, for example in the case where the hard drive is stolen or removed, you could use **No Extra Authentication** mode.
> This mode moves the burden of security from the pre-boot loader phase to the Windows logon. As such it is good practice to ensure you have a strong password policy as well as a minimum level of Windows network security established.

Related Articles

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

KB439 - TPM FAQ

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