ESET Tech Center

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

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

In order to encrypt a Workstation's hard drive utilising the TPM, you may have to take ownership of the TPM.

Once you have taken ownership of the TPM, you can then proceed to FDE the hard drive and secure the Workstation with a Pin Code or Username and Password. It is also possible to initiate 'No Extra Authentication' which will provide no authentication in the pre-boot environment, allowing you to boot straight to the Windows login.

Important: Please check the TPM requirements articles below.

KB430 - Trusted Platform Module (TPM) Support

KB439 - TPM FAQ

Starting the Full Disk Encryption Process

To utilise the TPM please follow the steps below:

Login to the Enterprise Server.
Select the Workstation you wish to encrypt from the Workstations window.
Highlight the Workstation and click **Full Disk Encryption**.

Click the appropriate Workstation to which you wish to send a Full Disk Encryption command and then click the **Full Disk Encryption**button. This will start the Full Disk Encryption wizard as seen below.
You will now be shown the **Compatibility Checks** stage of the FDE wizard. This stage will inform you if there are any incompatibilities on the Workstation.

Configuring the TPM

You may be required to **Reconfigure** the TPM by sending a command to the target Workstation.

Note: If your TPM doesn't require reconfiguring, please skip to 'Choosing the TPM Security Mode'.

You will be asked to confirm the **Reconfigure TPM** process and authenticate the command from the Enterprise Server by entering your Administrator Password.

Once a synchronisation has occurred, the command will be received by the target Workstation and a restart will be needed to clear the TPM.

A manual sync can be made by following the article here: [KB195 - How do I manually synchronise the Enterprise Server and DESlock+ client?]

You will be warned on the target Workstation that a restart will need to take place.

Depending on the Workstation make / model / current settings, the restart may need to take place twice in order to configure the TPM correctly.

Note: When the restart takes place, a manufacturers pre-boot dialog will ask you to confirm the command. This is supplied by the manufacturer and may look different on various Workstation models / makes. The image below is taken from a Microsoft Surface Pro 3.

When the TPM has been cleared and a sync has been made between Enterprise Server and Client Workstation, you will be able to proceed with the Full Disk Encryption Wizard process.

Choosing the TPM Security Mode

Choose the **TPM Hardware** from the **Security Mode** options.

You will then have a choice of authentication modes:

Username and Password
Pin Code
No Extra Authentication

KB443 - TPM Mode Username / Password

KB444 - TPM Mode PIN

KB445 - TPM Mode No Extra Authentication

Related Articles

KB177 - What is DESlock+ Full Disk Encryption Safe Start

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