![ESET Cybersecurity Progress. Protected.]

Recovery on TPM systems with only UEFI boot mode

Recovery on TPM systems with only UEFI boot mode

To decrypt a managed PC using Ubuntu you will need to have two removable devices: one for transferring files and the other for booting Ubuntu. For the purposes of this article, we will assume two USB sticks will be used.

Note: ensure a full sector-by-sector backup of the existing hard drive has been taken before attempting recover.

See this article for details: KB70 - How do I perform a full sector by sector backup of my hard drive?

Before booting Ubuntu:

1. Download the recovery ISO from the Enterprise Server for the Workstation you want to recover. Make note of the password you set.

See the **Generating the Recovery Image** section of this article: KB210 - How do I decrypt a managed system that is unable to start Windows?

2. Extract or mount the Recovery ISO generated from step 1 and copy the **dlrecvr.dat** file to a USB stick for later use. This file is found in the **isolinux** folder inside the ISO.

Boot Ubuntu on the Workstation you want to decrypt:

1. Connect your USB stick and copy the **dlrecvr.dat** file to the desktop.

2. Follow the article below but do **NOT** enter the last command shown: **./dlprecovery -s**

[KB281 - How do I decrypt a system that only has UEFI boot mode?](#)

3. When you reach the final command do **NOT** type **sudo ./dlprecovery -s**, instead type **sudo ./dlprecovery -r:./Desktop/dlrecvr.dat**

Important: the command above is case sensitive and all punctuation must be correct.

Follow the on-screen prompts to begin the decryption, do **NOT** interrupt its progress.

Keywords: TPM, recovery, decrypt, trusted, platform, module, ubuntu