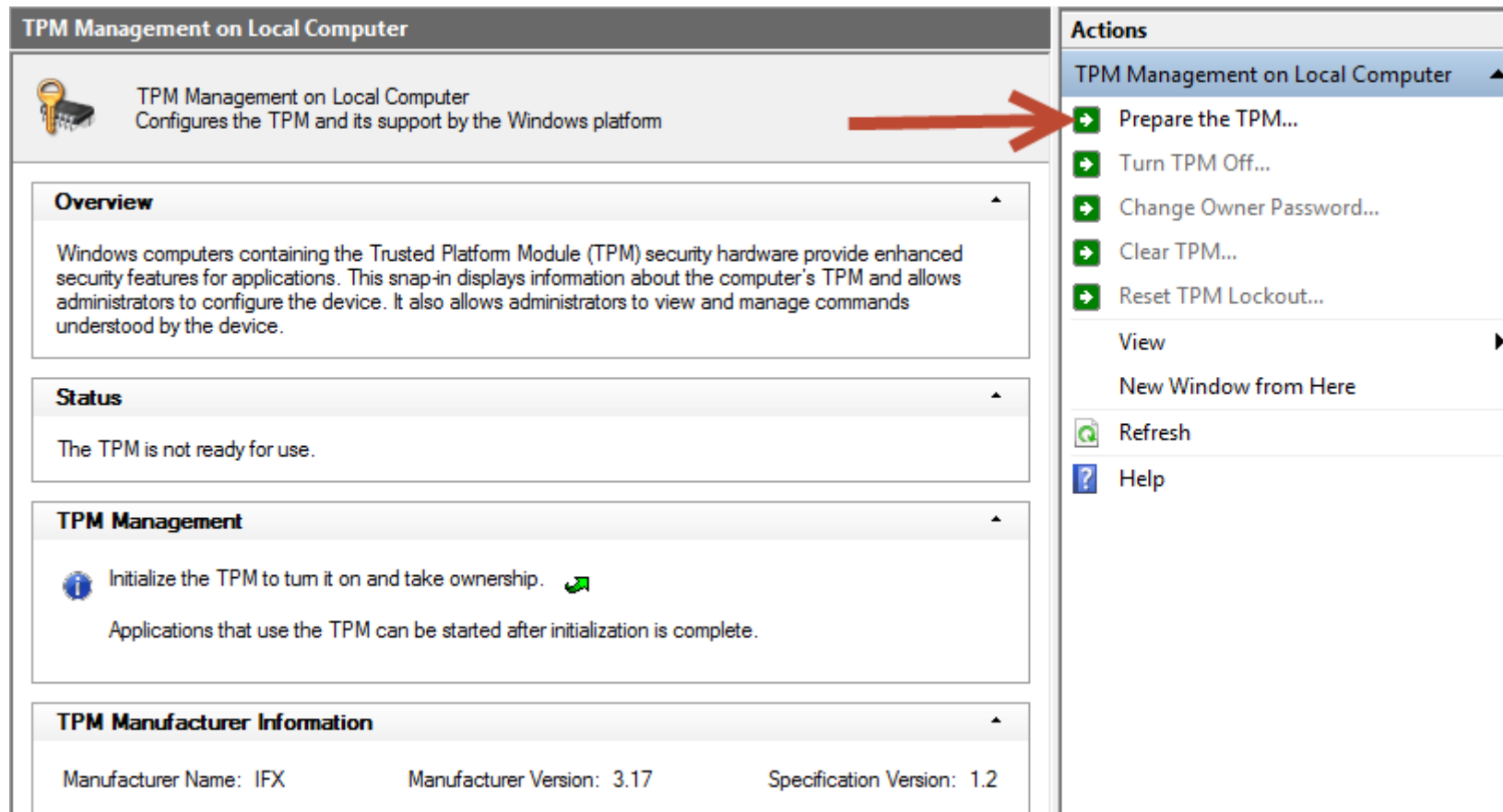
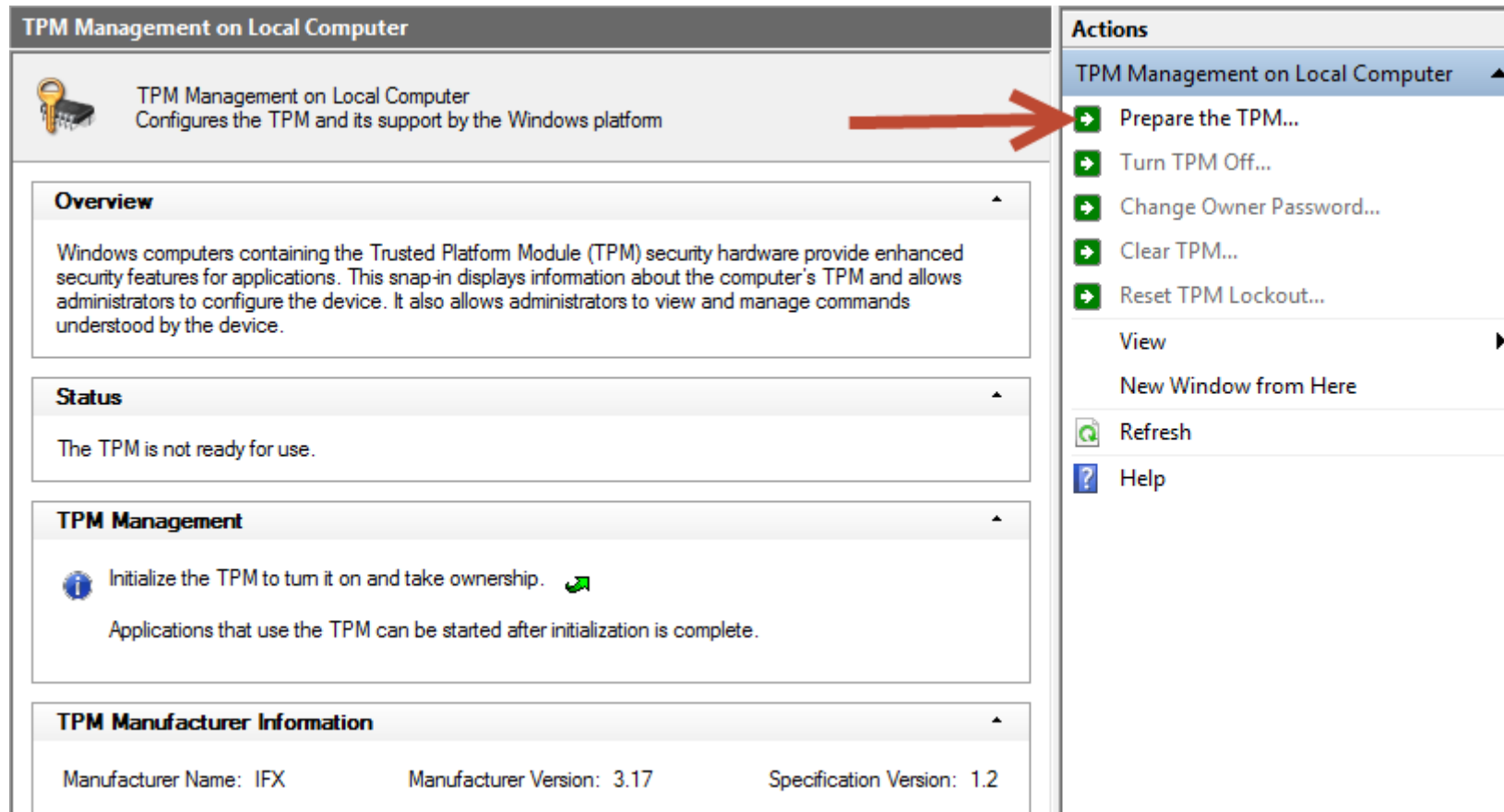


Note: set the registry key 'HKLM\Software\Policies\Microsoft\TPM' [REG_DWORD] 'OSManagedAuthLevel' to 4) to save password in registry in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TPM\WMI\Admin\OwnerAuthFull

After TPM clear in BIOS



Prepare TPM



The screenshot displays the 'TPM Management on Local Computer' console window. The main pane shows the 'Overview' section with a description of TPM, the 'Status' section indicating the TPM is not ready for use, the 'TPM Management' section with an 'Initialize the TPM' instruction, and the 'TPM Manufacturer Information' section. The 'Actions' pane on the right lists several actions, with 'Prepare the TPM...' highlighted by a red arrow.

TPM Management on Local Computer

TPM Management on Local Computer
Configures the TPM and its support by the Windows platform


Overview

Windows computers containing the Trusted Platform Module (TPM) security hardware provide enhanced security features for applications. This snap-in displays information about the computer's TPM and allows administrators to configure the device. It also allows administrators to view and manage commands understood by the device.

Status

The TPM is not ready for use.

TPM Management



Initialize the TPM to turn it on and take ownership. 

Applications that use the TPM can be started after initialization is complete.

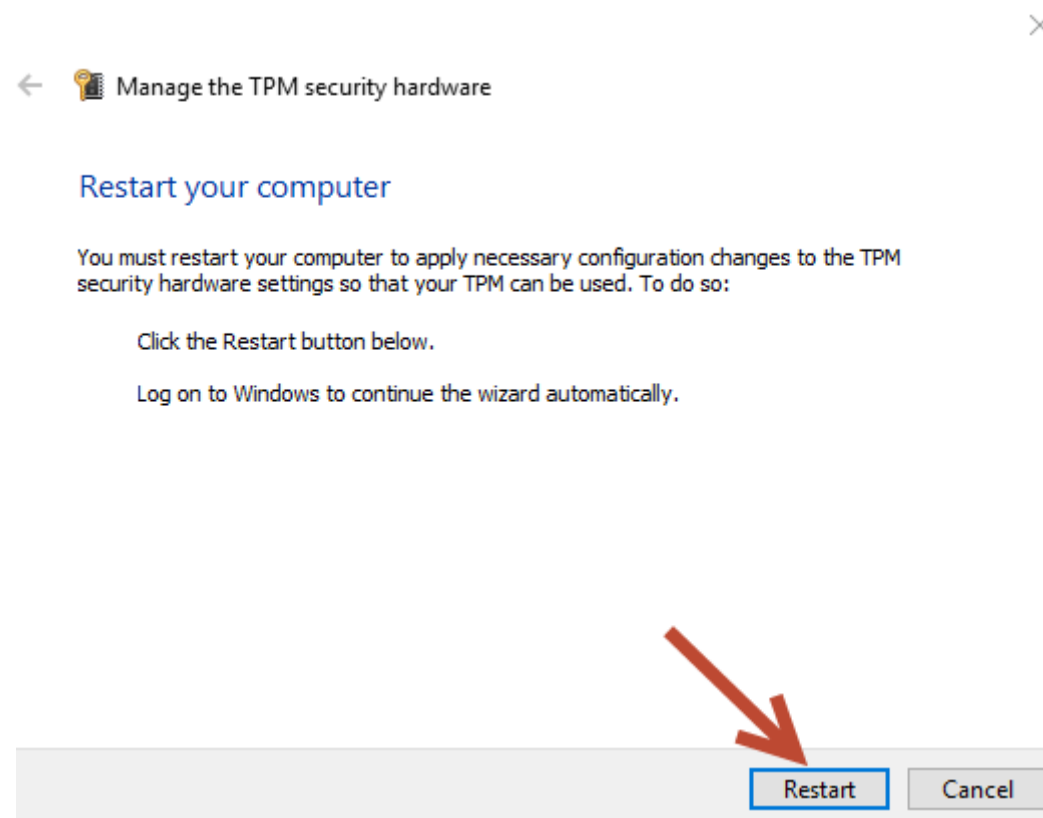
TPM Manufacturer Information

Manufacturer Name: IFX Manufacturer Version: 3.17 Specification Version: 1.2

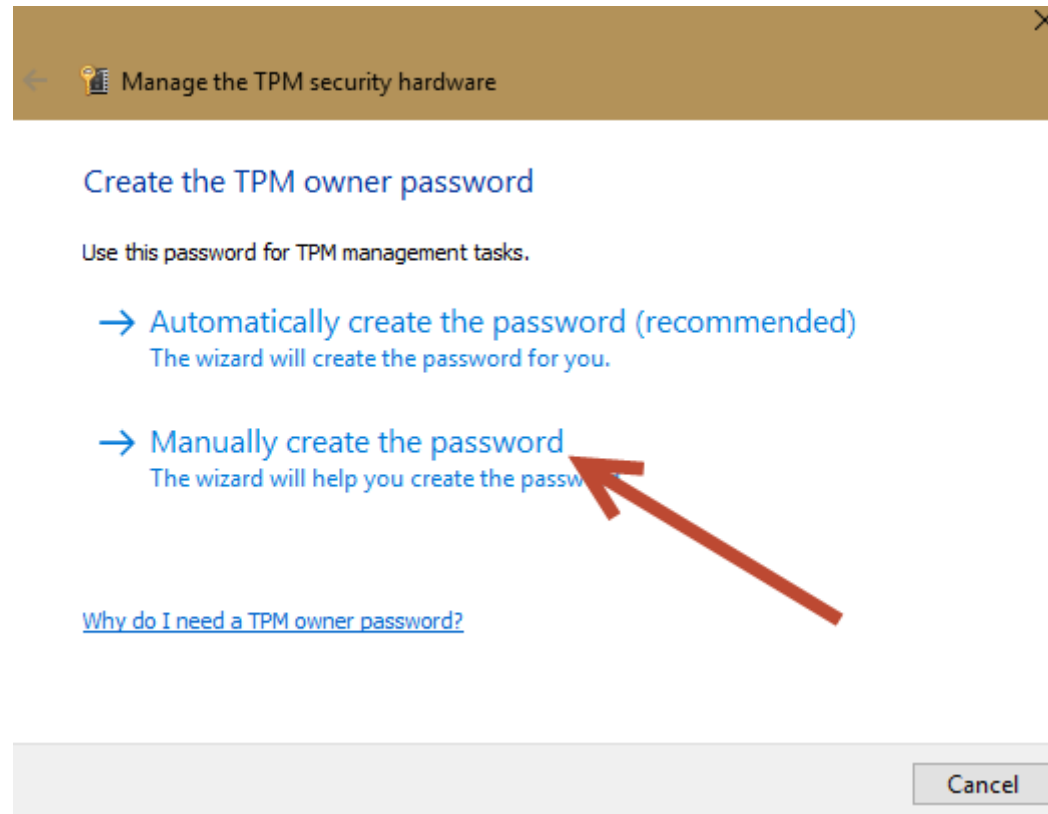
Actions

- TPM Management on Local Computer ▲
- Prepare the TPM...
- Turn TPM Off...
- Change Owner Password...
- Clear TPM...
- Reset TPM Lockout...
- View ▶
- New Window from Here
- Refresh 
- Help 

Restart



Create password



Set TPM owner NEW password


← 🔑 Manage the TPM security hardware ✕

Change your TPM owner password

Password:

Minimum eight characters

Confirm Password:

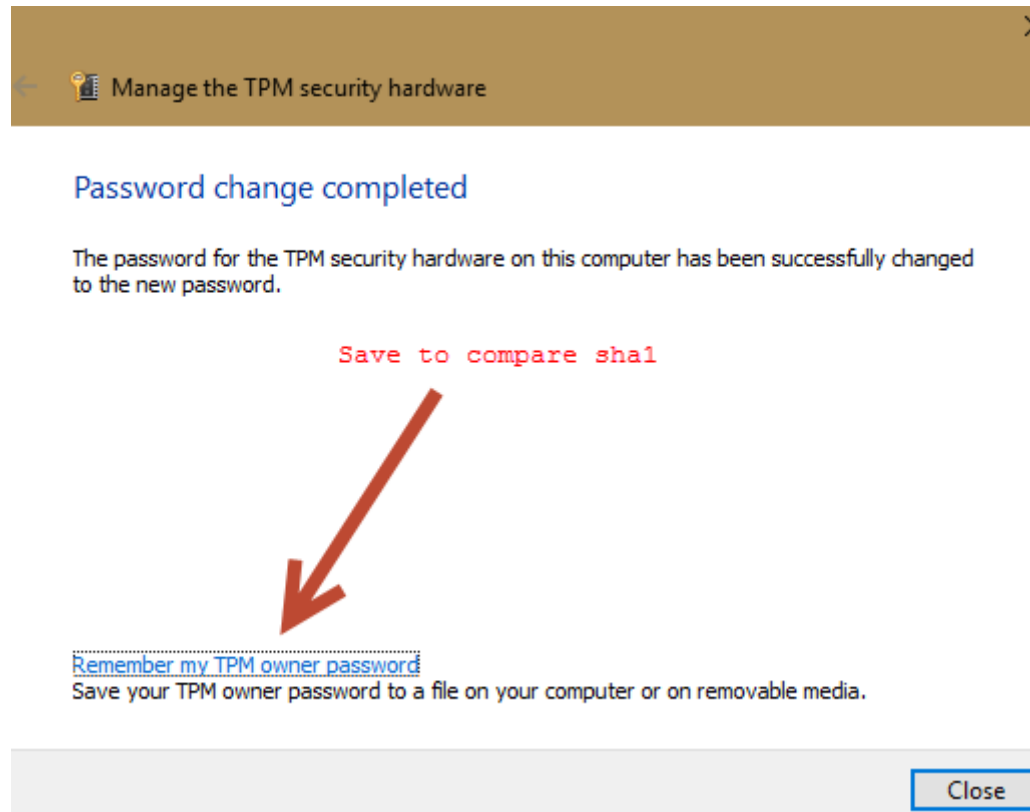


This is NEW password

Change Password

Cancel

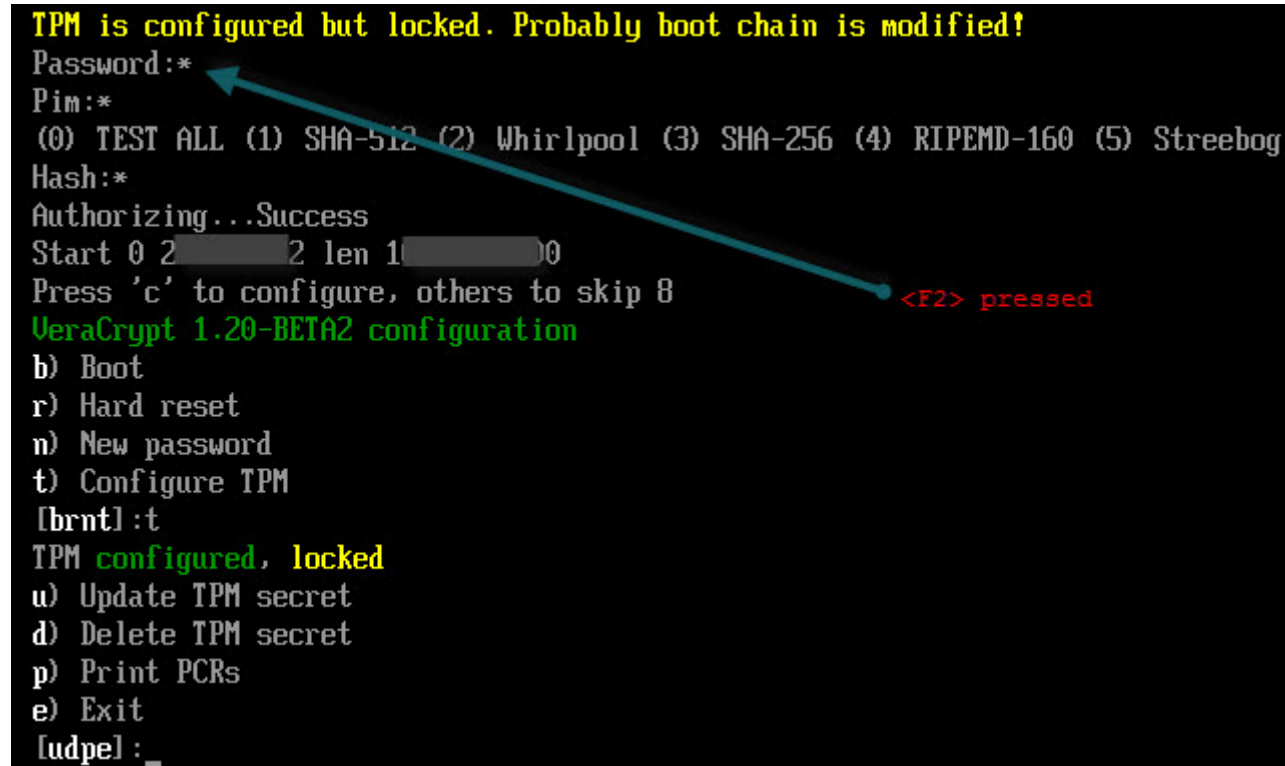
Save to compare



Create TPM key file for VeraCrypt.

Owner password is required to create NV RAM in TPM

The key file is locked to PCRs selected to protect modification of objects selected by PCRs (BIOS, DcsProp, boot loaders).



The screenshot shows the VeraCrypt TPM configuration interface. At the top, a yellow message states: "TPM is configured but locked. Probably boot chain is modified!". Below this, the "Password:*" field is highlighted with a blue arrow. The "Pim:*" field is also visible. A list of hash algorithms is shown: (0) TEST ALL, (1) SHA-512, (2) Whirlpool, (3) SHA-256, (4) RIPEMD-160, and (5) Streebog. The "Hash:*" field is empty. The "Authorizing...Success" message is displayed. The "Start 0 2" and "len 1" fields are shown. The prompt "Press 'c' to configure, others to skip 8" is present. The text "<F2> pressed" is shown in red. The "VeraCrypt 1.20-BETA2 configuration" text is in green. The menu options are: b) Boot, r) Hard reset, n) New password, t) Configure TPM, [brnt]:t, TPM configured, locked, u) Update TPM secret, d) Delete TPM secret, p) Print PCRs, e) Exit, and [udpe]:_. A blue arrow points from the "TPM configured, locked" message to the "<F2> pressed" text.

```
TPM is configured but locked. Probably boot chain is modified!
Password:*
Pim:*
(0) TEST ALL (1) SHA-512 (2) Whirlpool (3) SHA-256 (4) RIPEMD-160 (5) Streebog
Hash:*
Authorizing...Success
Start 0 2 2 len 1 0
Press 'c' to configure, others to skip 8
VeraCrypt 1.20-BETA2 configuration
b) Boot
r) Hard reset
n) New password
t) Configure TPM
[brnt]:t
TPM configured, locked
u) Update TPM secret
d) Delete TPM secret
p) Print PCRs
e) Exit
[udpe]:_
```

Press <F8> (or "TPM lck" button) to add TPM key file to password.

Press <F7> (or "PLT lck" button) to add BIOS serial and USB serial to password as key file

Important: Modification of BIOS or boot loader will block access to TPM! Before TPM/Platform lock - save rescue disk of system encrypted to restore.