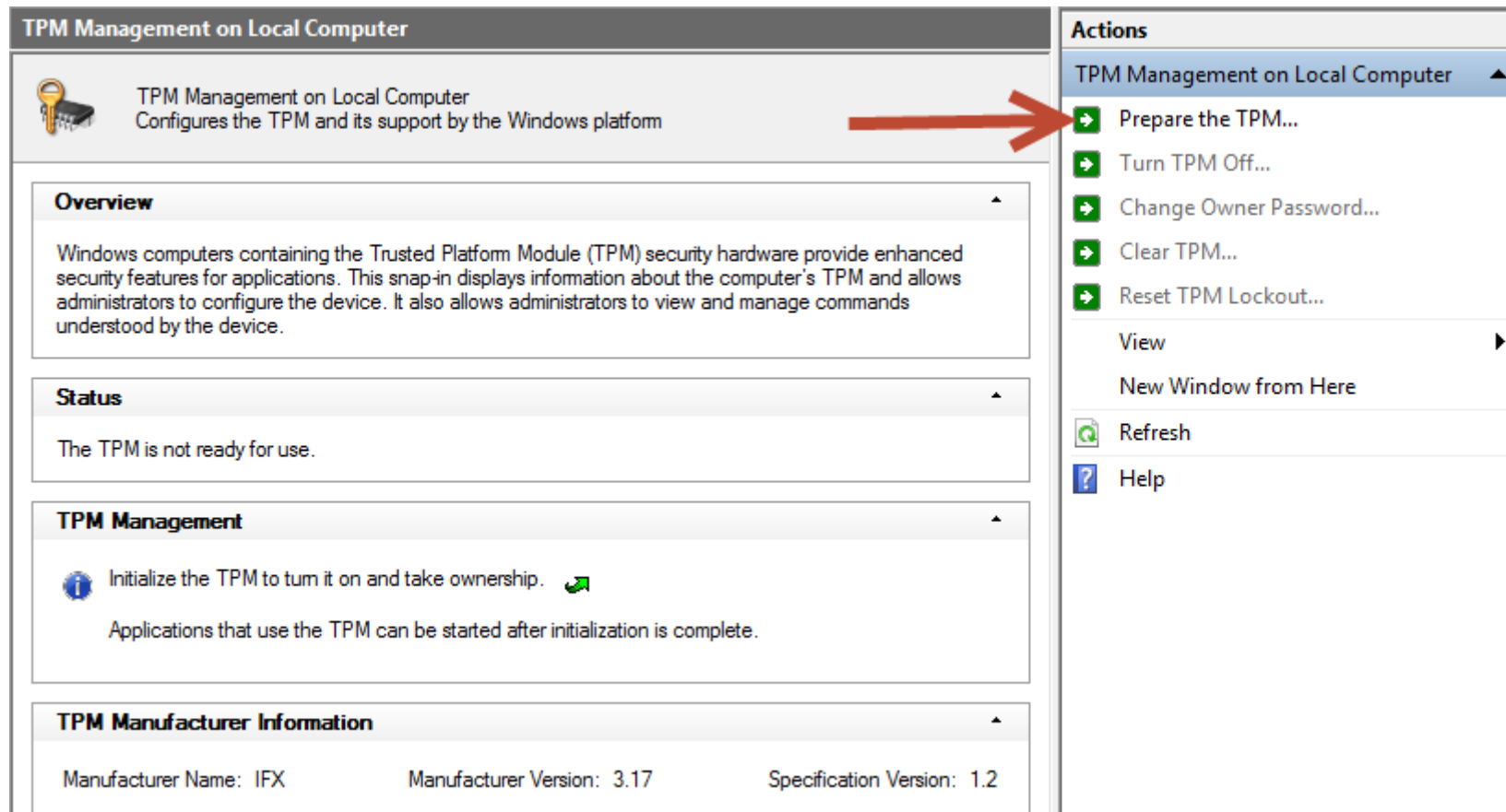


Note: set the registry key 'HKLM\Software\Policies\Microsoft\TPM' [REG_DWORD] 'OSManagedAuthLevel' to 4) to save password in registry in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TPM\WMI\Admin\OwnerAuthFull

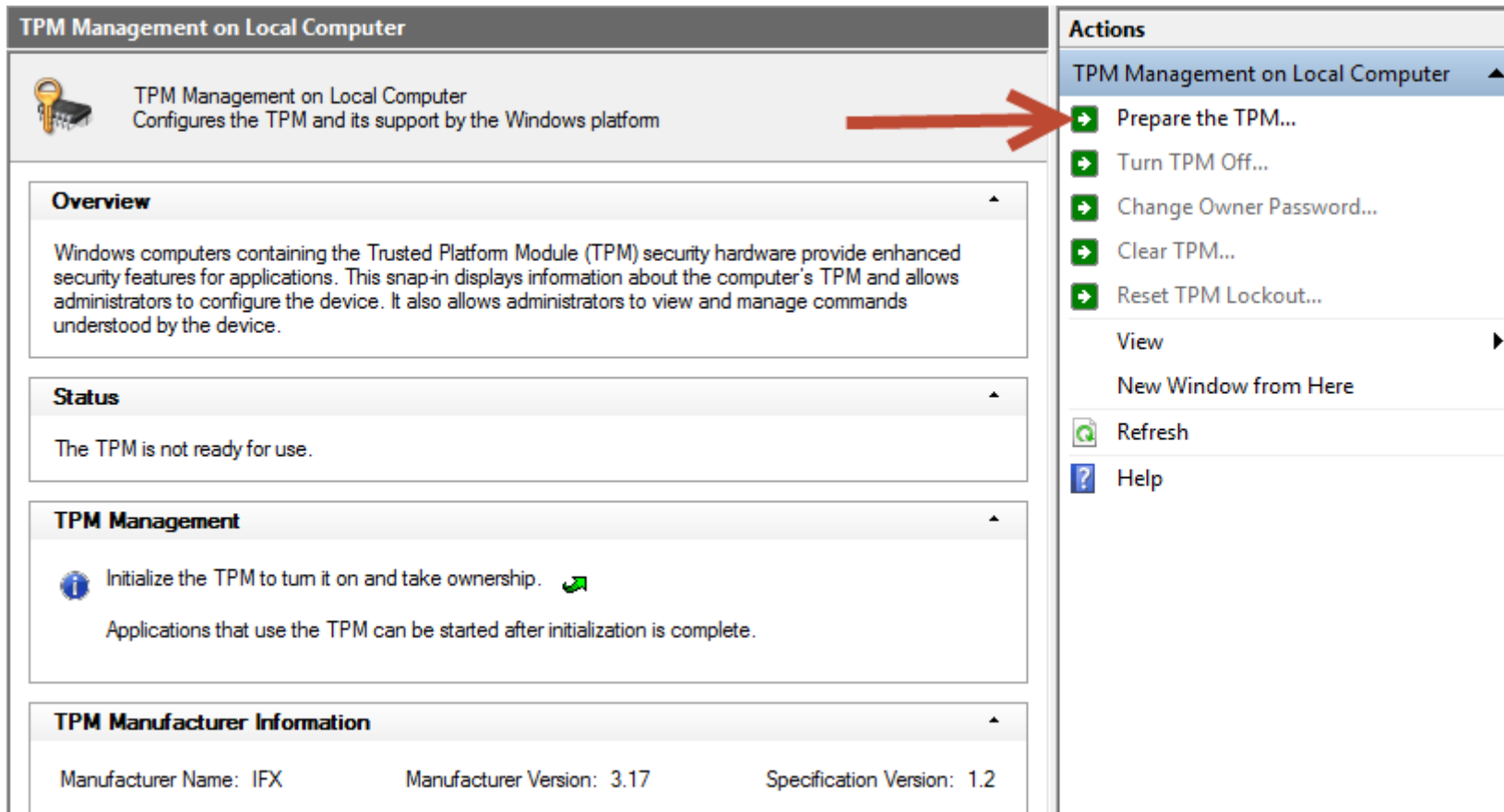
After TPM clear in BIOS



The screenshot shows the 'TPM Management on Local Computer' console window. The main area contains an overview, status, management, and manufacturer information section. A red arrow points to the 'Actions' menu on the right, which is open and shows options like 'Prepare the TPM...', 'Turn TPM Off...', 'Change Owner Password...', 'Clear TPM...', and 'Reset TPM Lockout...'. The status section indicates 'The TPM is not ready for use.' and the management section shows an 'Initialize the TPM' button.

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

Prepare TPM



The image shows the Windows TPM Management console. The main window is titled "TPM Management on Local Computer" and contains several sections: "Overview", "Status", "TPM Management", and "TPM Manufacturer Information". The "Status" section indicates that the TPM is not ready for use. The "TPM Management" section provides instructions to initialize the TPM. The "TPM Manufacturer Information" section lists the manufacturer name as IFX, the manufacturer version as 3.17, and the specification version as 1.2. On the right side, there is an "Actions" pane with a dropdown menu for "TPM Management on Local Computer". The "Prepare the TPM..." option is highlighted with 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...

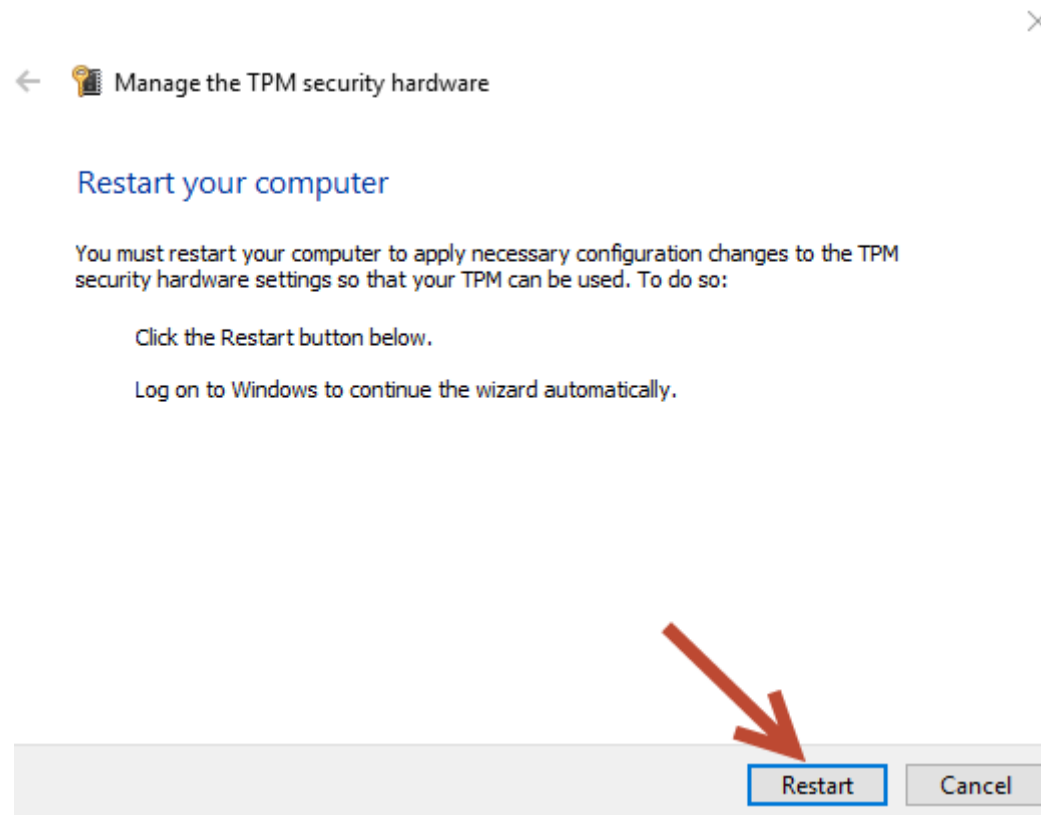
View ▶

New Window from Here

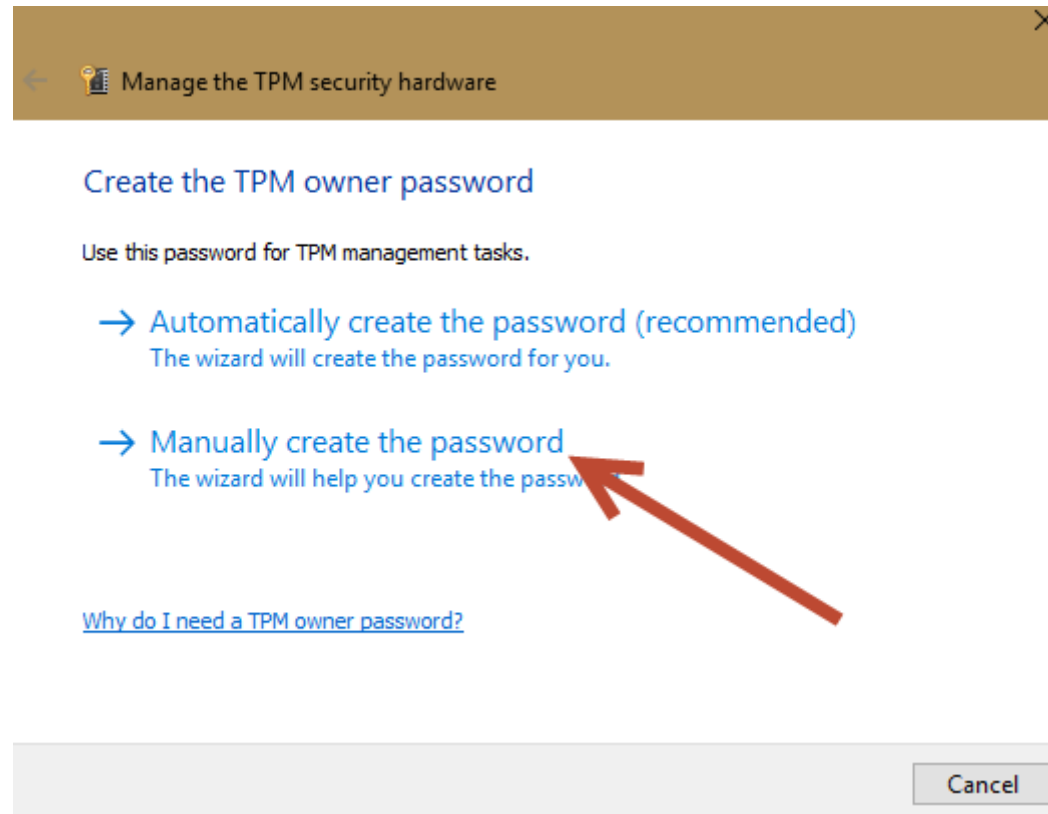
 Refresh

 Help

Restart



Create password



Manage the TPM security hardware

Create the TPM owner password

Use this password for TPM management tasks.

- Automatically create the password (recommended)
The wizard will create the password for you.
- Manually create the password
The wizard will help you create the password.

[Why do I need a TPM owner password?](#)

Cancel

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

Manage the TPM security hardware

Password change completed

The password for the TPM security hardware on this computer has been successfully changed to the new password.

Save to compare sha1

[Remember my TPM owner password](#)

Save your TPM owner password to a file on your computer or on removable media.

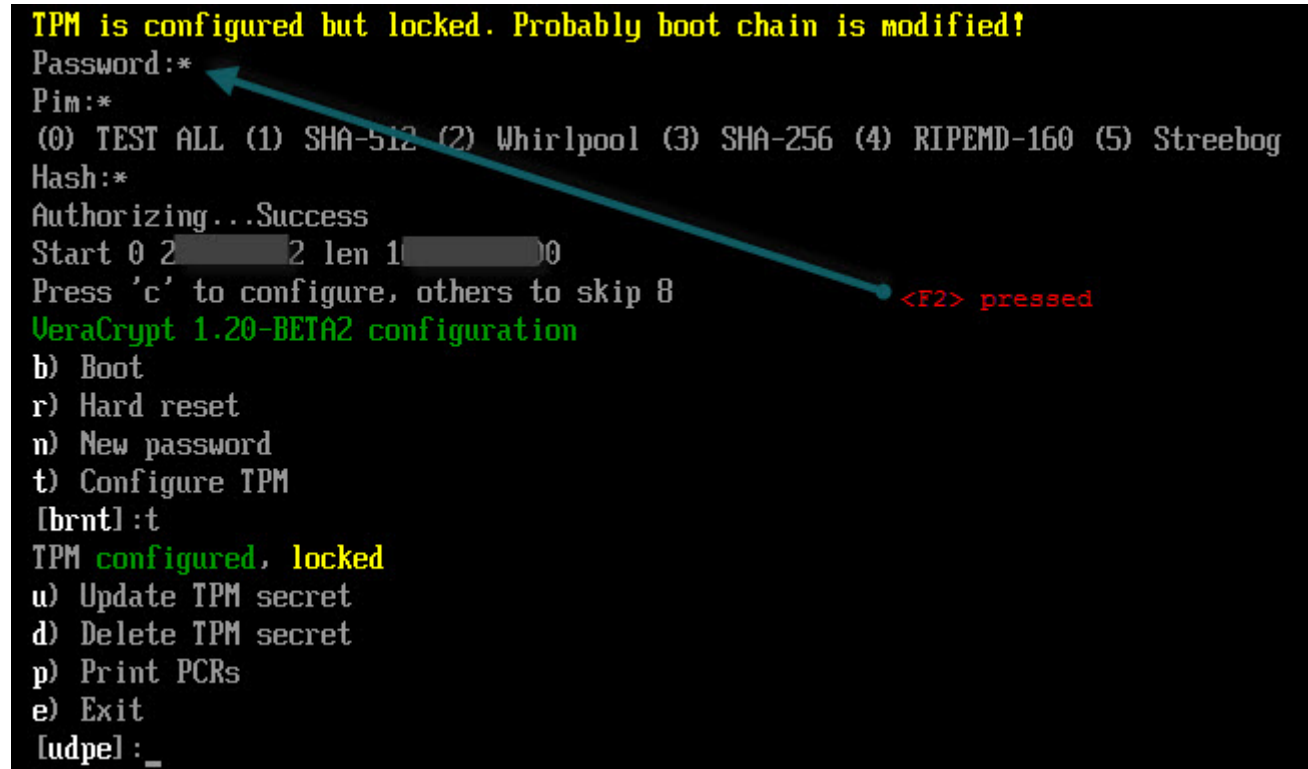
Close

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).

```
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]:_
```

A screenshot of the VeraCrypt TPM configuration interface. The text is displayed on a black background. At the top, a yellow warning message reads "TPM is configured but locked. Probably boot chain is modified!". Below this, the user is prompted for a "Password:*" and "Pim:*". A menu of hash algorithms is shown: "(0) TEST ALL (1) SHA-512 (2) Whirlpool (3) SHA-256 (4) RIPEMD-160 (5) Streebog". The user is then prompted for a "Hash:*" and the process "Authorizing...Success" is shown. The screen displays "Start 0 2 2 len 1 0" and "Press 'c' to configure, others to skip 8". The title "VeraCrypt 1.20-BETA2 configuration" is in green. A list of options is shown: "b) Boot", "r) Hard reset", "n) New password", "t) Configure TPM". The user has selected "t", resulting in "[brnt]:t". The status "TPM configured, locked" is shown in yellow and green. Further options are listed: "u) Update TPM secret", "d) Delete TPM secret", "p) Print PCRs", "e) Exit". The prompt "[udpe]:_" is at the bottom. A red arrow points from the text "<F2> pressed" to the "Password:*" field. Another red arrow points from the text "<F2> pressed" to the "Press 'c' to configure, others to skip 8" line.

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.