Forgot BitLocker PIN: recover encrypted drive

https://4sysops.com/archives/forgot-bitlocker-pin-recover-encrypted-drive/

Contents

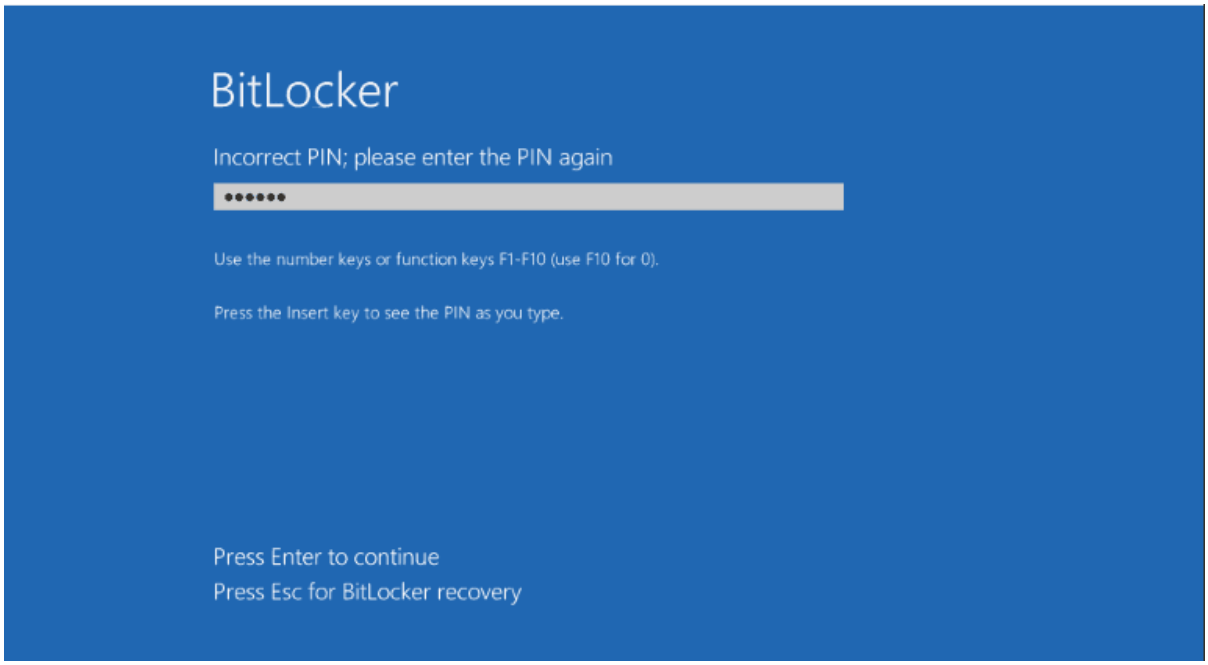
When BitLocker uses TPM as the sole protector during system startup, the drive is unlocked before the user logs in. Hence, the unencrypted Volume Master Key (VMK) is already loaded into the RAM, which an attacker can acquire through a memory dump. Requiring a PIN adds an extra layer of protection against this threat.

While on older BIOS-based systems, even minor changes to the system would redirect users to the BitLocker recovery console upon startup, modern PCs with Secure Boot enabled are more forgiving in this regard. Therefore, a forgotten PIN has become one of the most common reasons for resorting to the recovery key.

TPM allows for numerous incorrect entries

When users are prompted to enter the BitLocker PIN upon PC startup, they typically have 32 retries available by default. Depending on the complexity requirements of the PIN, there's a good chance that users may still recall the chosen secret.

If not, they can switch to the recovery console by pressing the ESC key. The recovery console expects the input of the 48-digit recovery key in such scenarios.

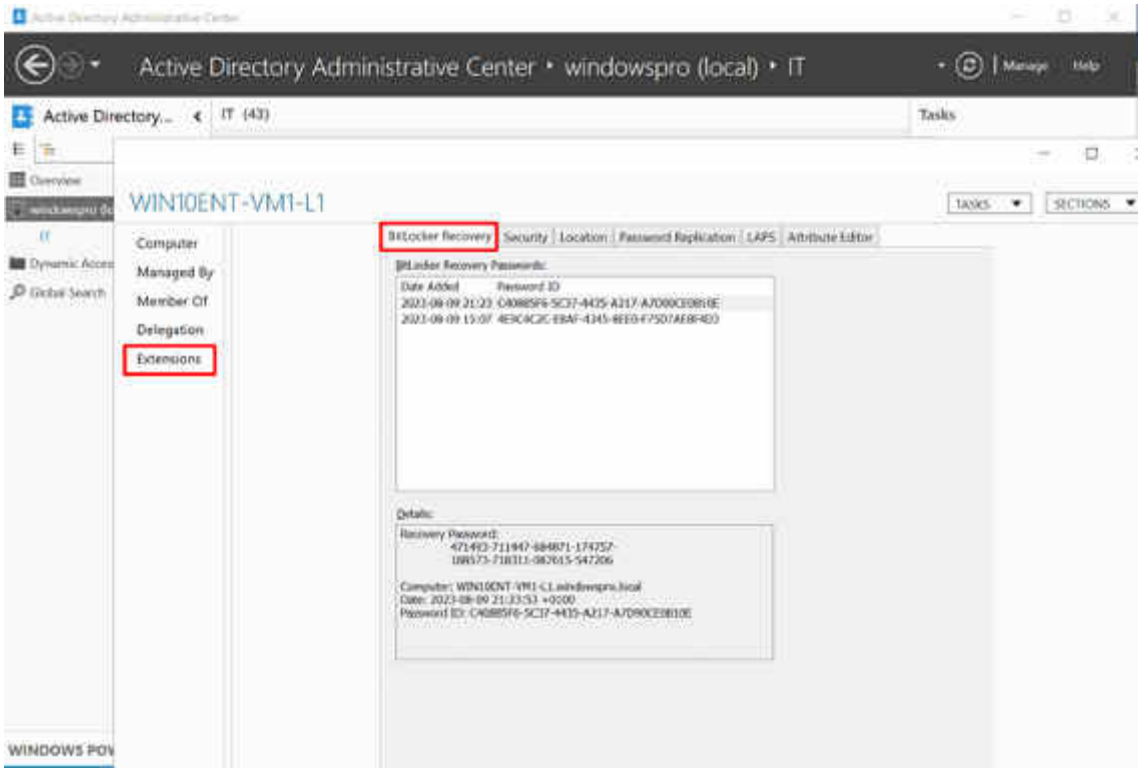


If users cannot recall the PIN, they can open the recovery console by pressing ESC.

Finding the recovery key

When activating BitLocker, users have various options for storing the recovery key, including printing it on paper or saving it in a file.

However, in a managed environment, the key is typically stored in a central location, usually in Active Directory. From there, it can be retrieved using *Active Directory Users and Computers* or the AD Administrative Center.

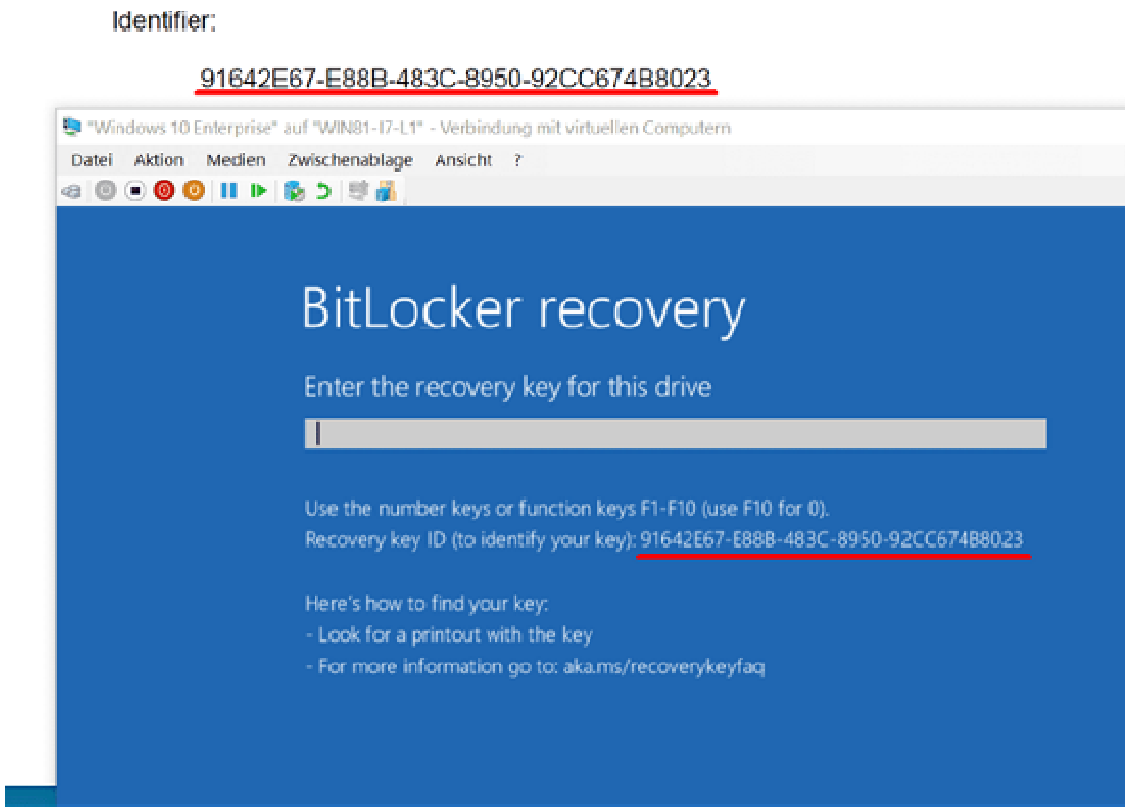


Retrieving BitLocker Recovery Keys from Active Directory.

Alternatively, Entra ID or a Microsoft account can also serve as storage locations for the recovery key. In the former case, the key can also be retrieved via Intune.

In larger enterprises where employees are not personally known to the helpdesk, the question arises of how to reliably identify them, especially when they report issues while on the go. Ensuring the recovery key does not fall into unauthorized hands is crucial.

Each recovery key has an ID associated with it, allowing you to verify which computer it is connected to. After entering the key, the PC should unlock accordingly.



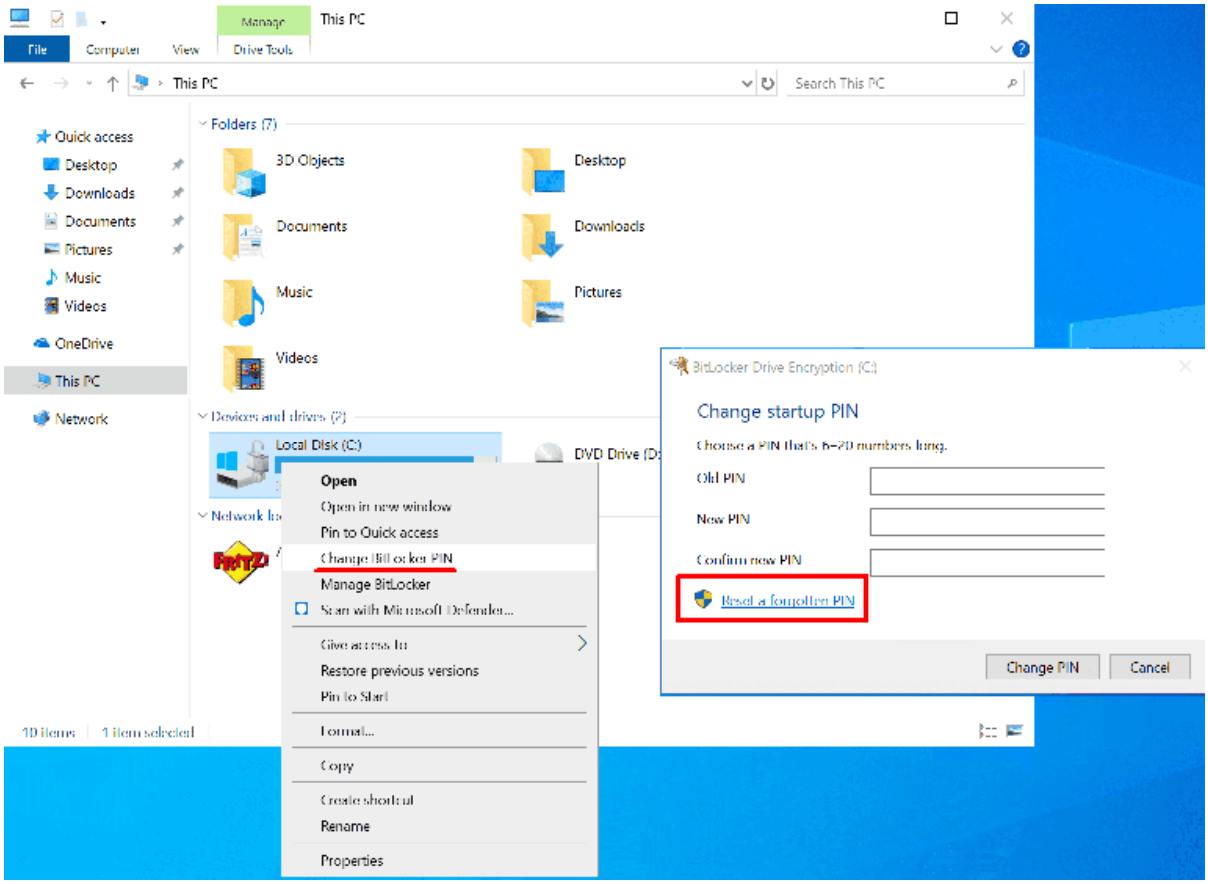
Here, the recovery key stored in a PDF contains the ID required by the computer.

Change or reset PIN

Once users regain access to their computers, they should set a new PIN since they can no longer remember the old one. Otherwise, they will require the recovery key again after the next reboot.

This can be done through the BitLocker applet in the Control Panel or via the drive's properties. The respective dialog box initially expects the input of the old PIN, which is unlikely to be available in this situation.

Therefore, by clicking on the link to reset a forgotten PIN, you access a dialog box that only expects the input of a new PIN. However, administrative permissions are required for this.



Without knowledge of the old PIN, resetting it requires elevated permissions.

Instead of granting users access to an admin account, a script could be executed in the context of a privileged account, running the following command:

manage-bde -changepin c:

As with Windows passwords, admins cannot force users to change their PIN. BitLocker does not have such a mechanism. Instead, they can merely remind users to do so.

Summary

A forgotten BitLocker PIN is likely the most common reason for resorting to the 48-digit recovery key. This key is found in Active Directory or Entra ID in managed environments, where the helpdesk can retrieve it using the appropriate tools.

Each recovery key has an ID that must match the one displayed on the recovery console.