Bitlocker Needs your Recovery Key_Encryption

Last updated by | Kevin Gregoire | Mar 29, 2022 at 11:47 AM PDT

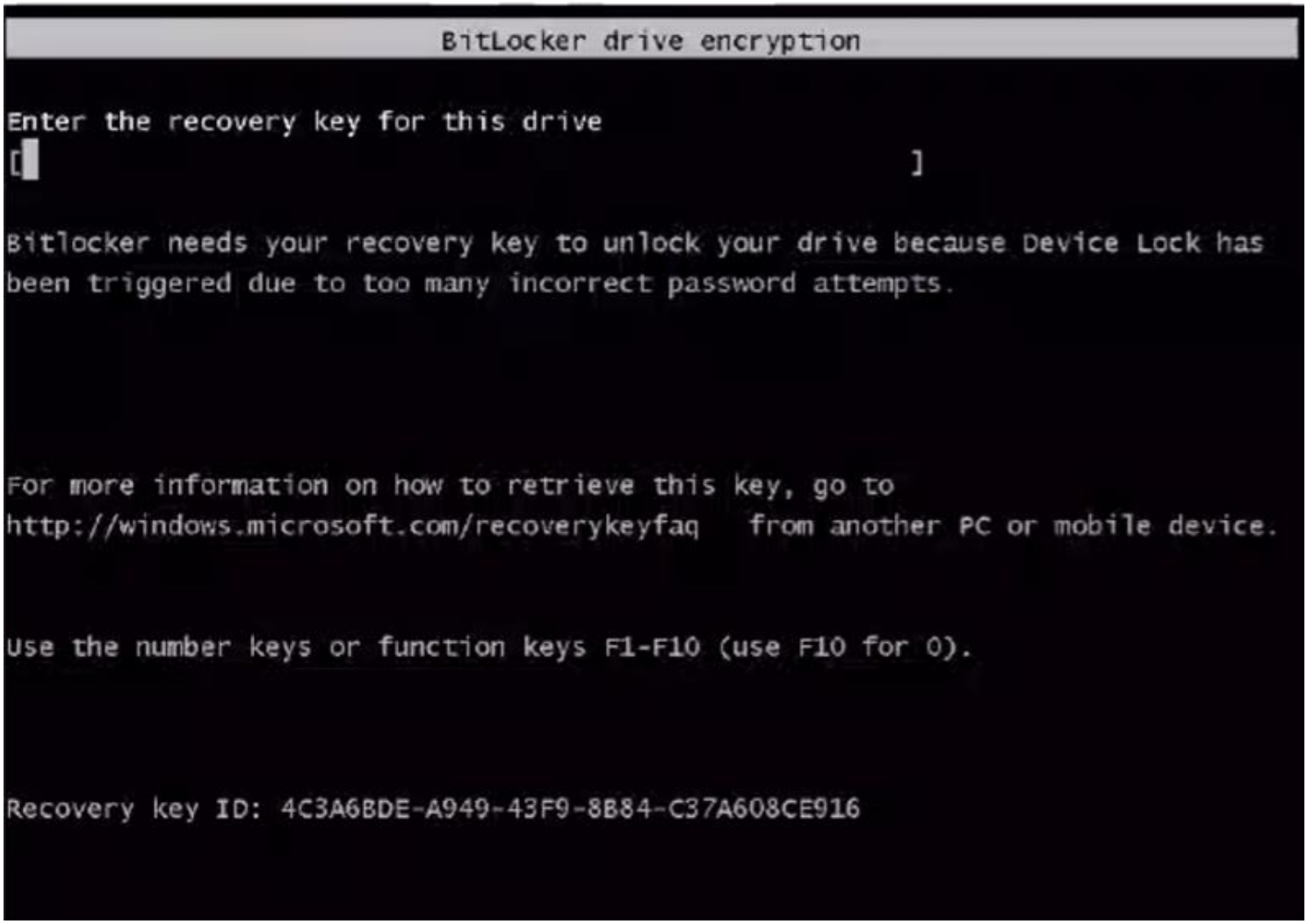
Tags

cw.Azure-Encryption cw.TSG

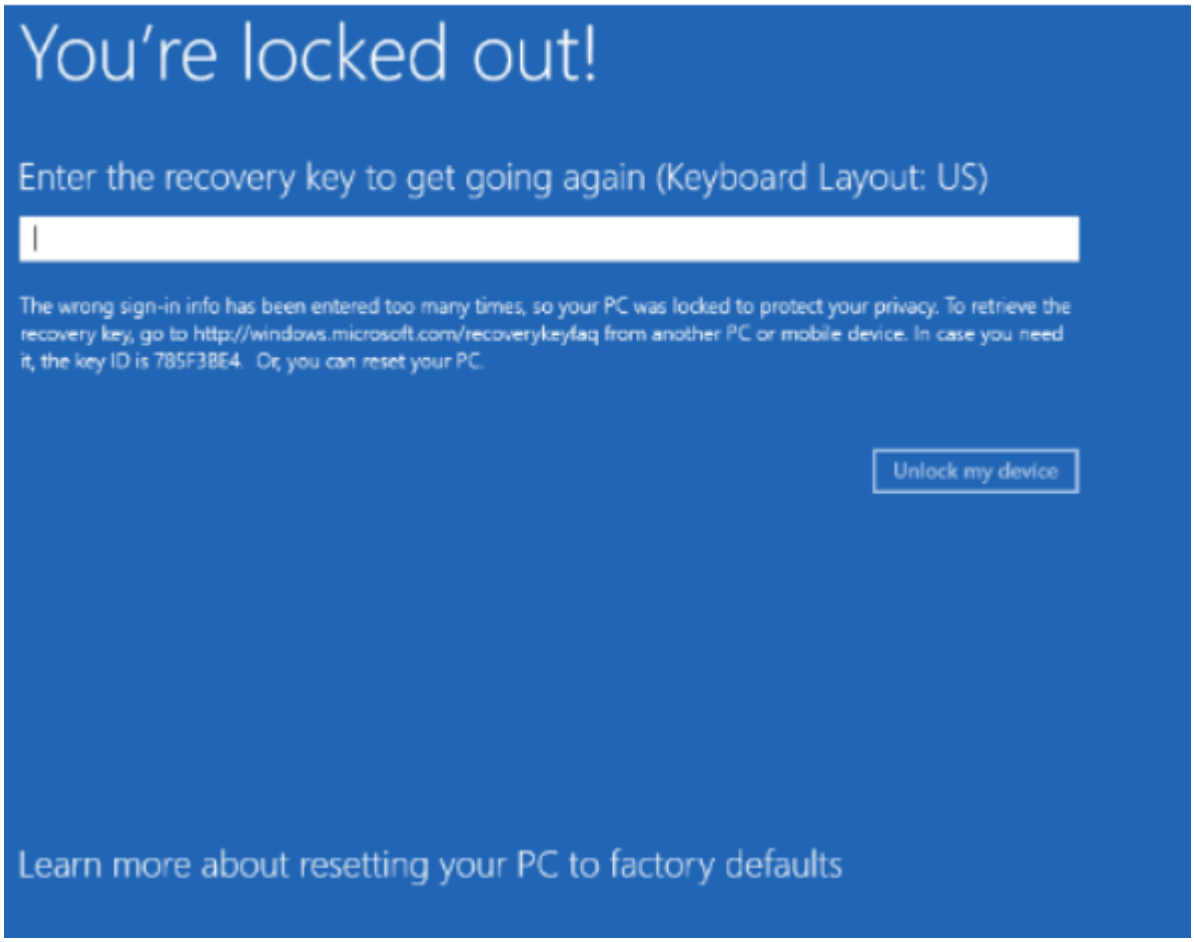
Contents

Symptom

VM encrypted with ADE falls in a non boot state. The screenshot shows the OS is requesting a Recovery Key.



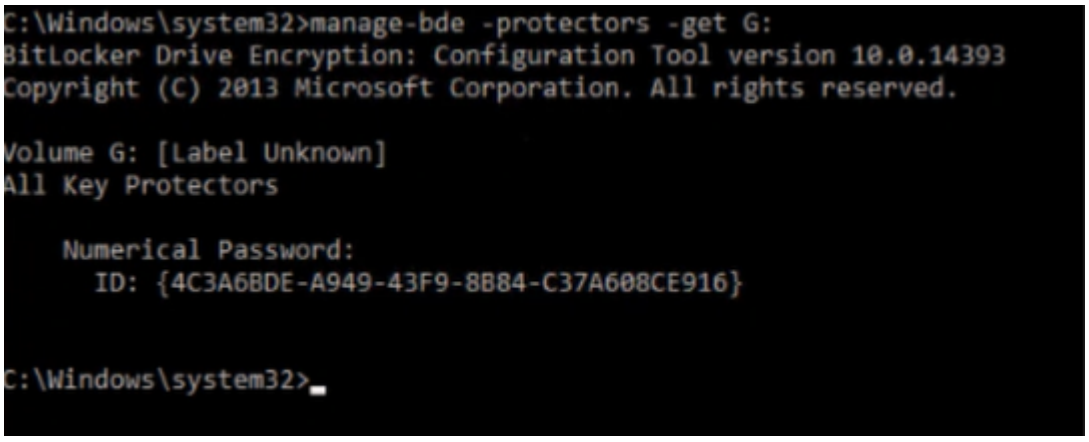
Bitlocker needs your recovery key to unlock your drive because Device Lock has been triggered due to many incorrect password attempts.



You're locked out! Enter the recovery key to get going again (Keyboard Layout: US)
The wrong sign-in info has been entered too many times, so your PC was locked to protect your privacy. To retrieve the recovery key, go to http://windows.microsoft.com/recoverykeyfaq from another PC or mobile device. In case you need it, the key ID is XXXXXXX. Or, you can reset your PC.

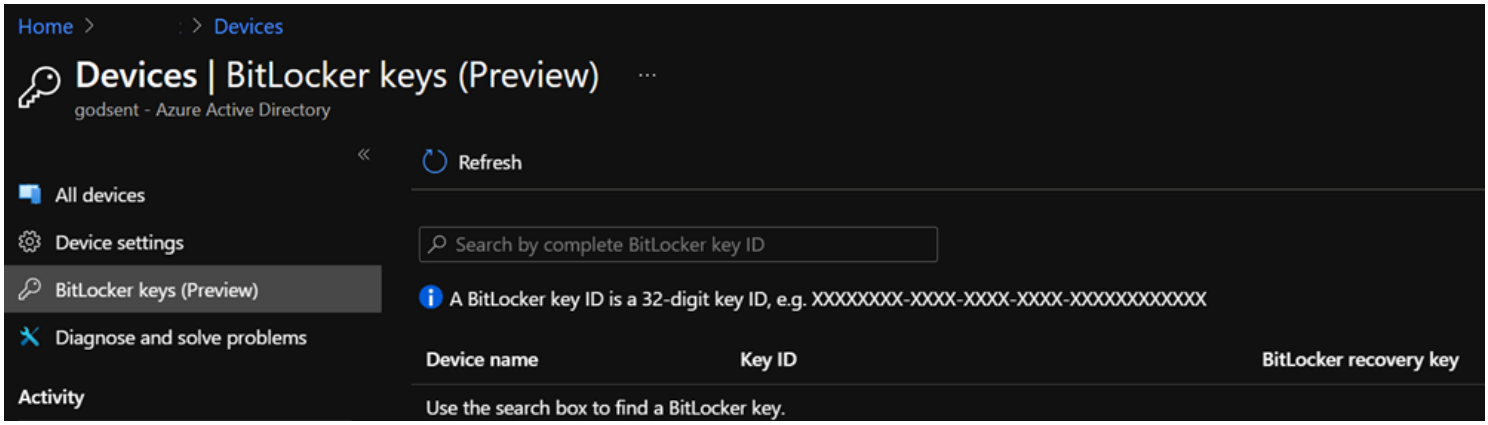
Root Cause Analysis

Due to the customer setting the GPO policy MaxDevicePasswordFailedAttempts which specifies how many times an incorrect password can be entered before the device is rebooted, the device may be put into lock mode, which requires the recovery key to unlock the device in the presence of disk encryption. This policy leaves the External Protector unusable, even if you are presenting it the right key to unlock, it will no longer be able to perform the operation. When an External Protector has been disabled, there is no way you can recover the VM or set again the external recovery key.



Mitigation

The **only** way that the VM can recovered is that the VM in question is Domain joined to an **Azure Active Directory (AAD)** , it is possible to get the Recovery Key from **Azure Active Directory** > **Devices** > **Bitlocker Keys**



If the VM is on-premise domain joined, only Active Directory (AD), it is not possible to unlock the VM and the VM falls into an unrecoverable state. **This policy MaxDevicePasswordFailedAttempts is not compatible with ADE**. If customer wants to use the MaxDevicePasswordFailedAttempts policy, they need to disable the encryption. If not the VMs encrypted with ADE are under risk of falling in an unrecoverable state if they trigger this policy.

Need additional help or have feedback?

To engage the Azure Encryption SMEs...	*To provide feedback on this page...*	*To provide kudos on this page...*
Please reach out to the **Azure Encryption SMEs** for faster assistance. Make sure to use the **Ava process** for faster assistance.	Use the **Azure Encryption Feedback** form to submit detailed feedback on improvements or new content ideas for Azure Encryption. ***Please note*** the link to the page is required when submitting feedback on existing pages! If it is a new content idea, please put N/A in the Wiki Page Link.	Use the **Azure Encryption Kudos** form to submit kudos on the page. Kudos will help us improve our wiki content overall! ***Please note*** the link to the page is required when submitting kudos!