**SQL User Creation**

You will need to create a SQL user for your script to use to retrieve the recovery key from the MBAM or ConfigMgr database (we can’t use windows auth since the Task Sequence runs from WinPE)

A screenshot of a computer

Description automatically generated

I made my user called “CrowdStrikeFix” – note that we switched the new user wizard to create the user with SQL Server Authentication to do this. I removed the Enforce password expiration option here (optional), which also removes the “User must change password at next logon” option (required).

A screenshot of a computer

Description automatically generated

Now we need to grant the new user some permissions. Those depend on if you are using standalone MBAM or using ConfigMgr’s new built-in MBAM feature (Standalone is being deprecated this year!)

A screenshot of a computer

Description automatically generated

ConfigMgr MBAM:

Right click our new user under logins and select properties. Under the User Mapping page, check the box next to the CM\_<SiteCode> database and grant the db\_datareader role.  
A screenshot of a computer

Description automatically generated

Under the CM\_<SiteCode> database, there is a directory called Scalar-Valued Functions – we need to grant execute permissions on the RecoveryAndHardwareCore.DecryptString functionfound there (Right click it and select properties):

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

***For Standalone MBAM:***   
We just need to grant db\_datareader role to our new login for the MBAM Recovery and Hardware Service database.

A screenshot of a computer

Description automatically generated

**Script Setup:**

For the script setup, you need to set the following options to prepare the script for use in the task sequence:

$MBAMIsStandalone = $false # Set to true if you are still using standalone MBAM (Not the new built-in ConfigMgr MBAM feature)

$DBUserName = 'CrowdStrikeFix' # You can change this if you like

$DBUserPass = 'SomeSecurePassword' # This needs to match your SQL User account's password

$RebootTimerSeconds = 10 # number of seconds to wait after completion (fail or success) before rebooting automatically

# Standalone MBAM Section - ignore if using New ConfigMgr Built-In MBAM

$MBAMSQLServerFQDN = "someserver.somedomain.somecompany.com"# Use ConfigMgr DB Server Here if ConfigMgr is using new integrated MBAM

# ConfigMgr Built-In MBAM (New feature, this is not the same as standalone MBAM with ConfigMgr integration)

$ConfigMgrSQLServerFQDN = "someserver.somedomain.somecompany.com" # Only use if your org is using new ConfigMgr MBAM feature (not standalone MBAM)

$ConfigMgrSiteCode = "FOO"

That’s all for the script, we will use it in the Task sequence setup below.

**Task Sequence Setup:**

Task Sequence is simple, only one “Run a Powershell Script” step is needed. Enter the Script to avoid the need to distribute content:  
A screenshot of a computer

Description automatically generated

Deploy the Task Sequence to All Systems (you may have to set the option to allow the task sequence to be deployed to large collections to do this).

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

For the rest of the options, just take the defaults and apply.

At this point, you should now simply need to send users instructions on how to PXE boot your particular PC brand/models. Because of the required deployment, the task sequence should auto-run + reboot their machine, which should follow the normal boot order and boot back into a working windows since the task sequence will have nuked the bad driver.