MBAM INTEGRATION WITH CURRENT BRANCH 1910

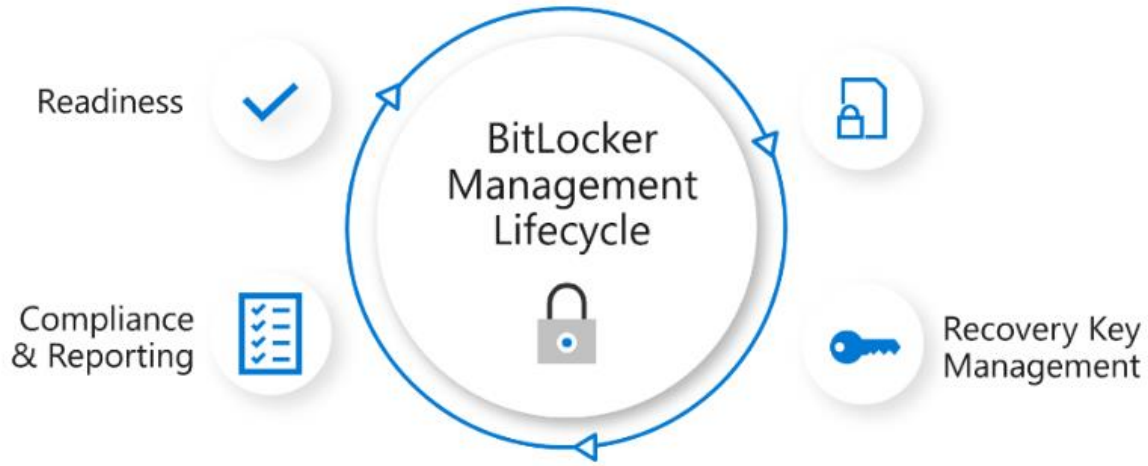
In this post, I will show you how to integrate MBAM (Microsoft Bit Locker Administration & Management) within Current Branch 1910.

HTTPS PRE REQ:

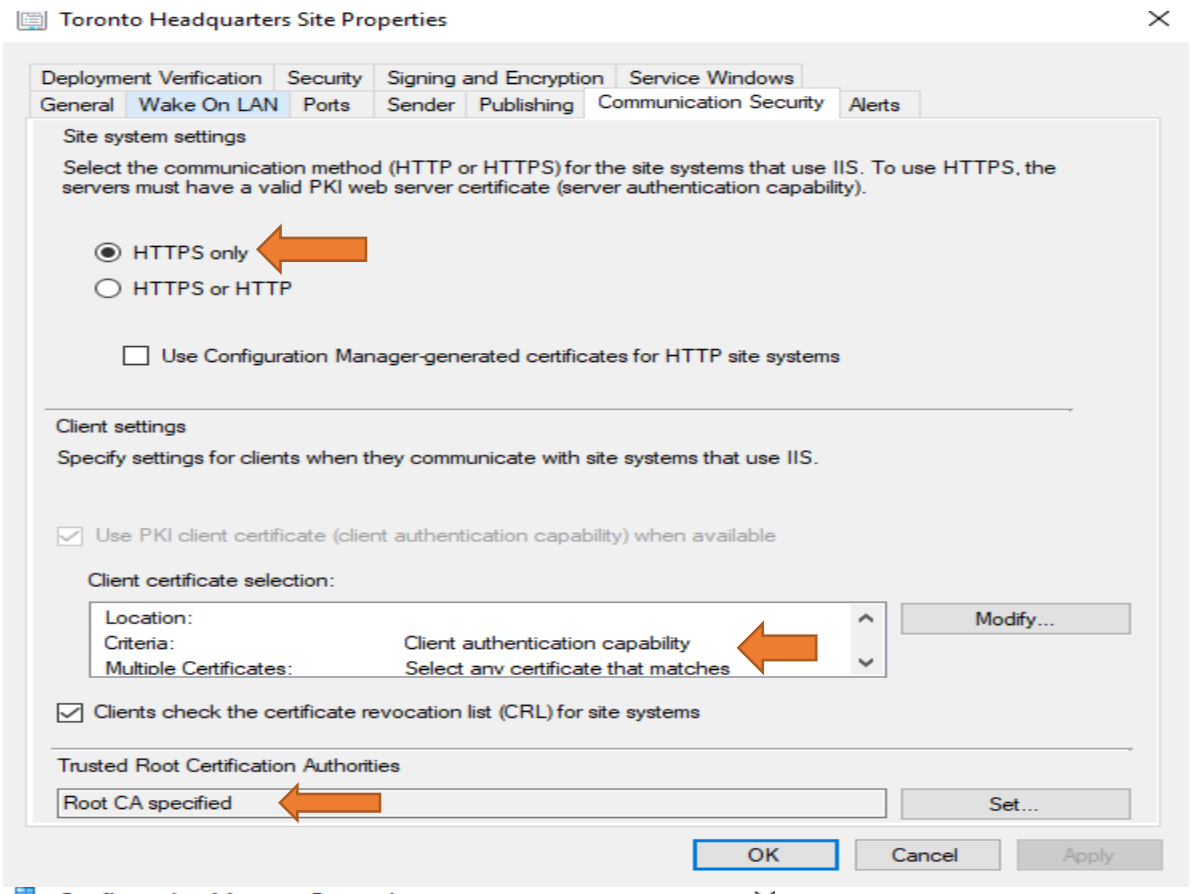
First you have to take care of PKI (Public Key Infrastructure) installation. I won't go into detail – you can refer to these articles.

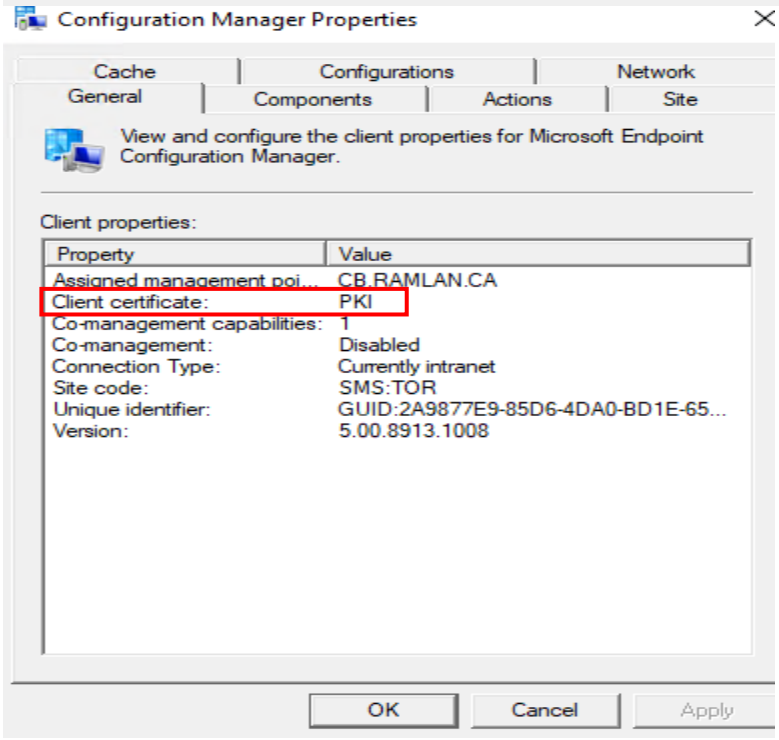
It's worth investing time at Microsoft ConfigMgr documentation site and read up on how to do this.

1. Plan for security in Configuration Manager – https://docs.microsoft.com/en-us/sccm/core/plan-design/security/plan-for-security
2. PKI certificate requirements for System Center Configuration Manager – https://docs.microsoft.com/en-us/sccm/core/plan-design/network/pki-certificate-requirements
3. Step-by-step example deployment of the PKI certificates for System Center Configuration Manager: Windows Server 2008 certification authority – https://docs.microsoft.com/en-us/sccm/core/plan-design/network/example-deployment-of-pki-certificates
4. https://www.windows-noob.com/forums/topic/16252-how-can-i-configure-pki-in-a-lab-on-windows-server-2016-part-1/



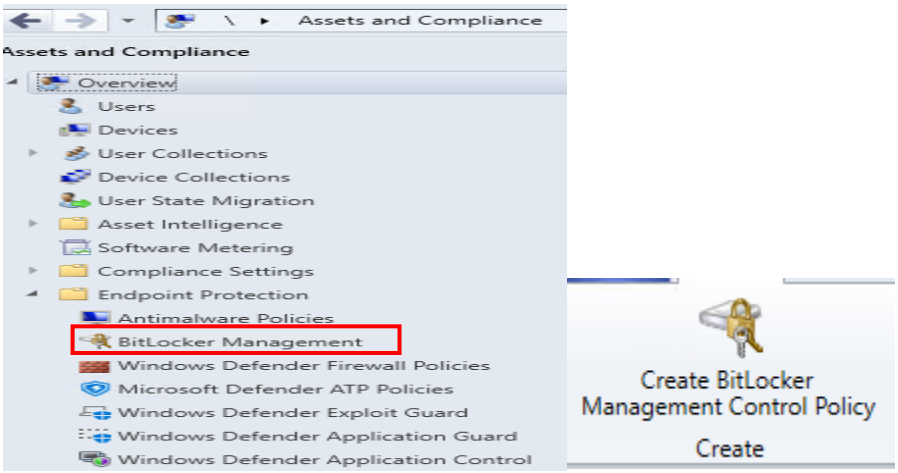
Once you have PKI infrastructure then we are ready to go ahead with the integration. Within my lab, I already have PKI installed. Here is the screen shot

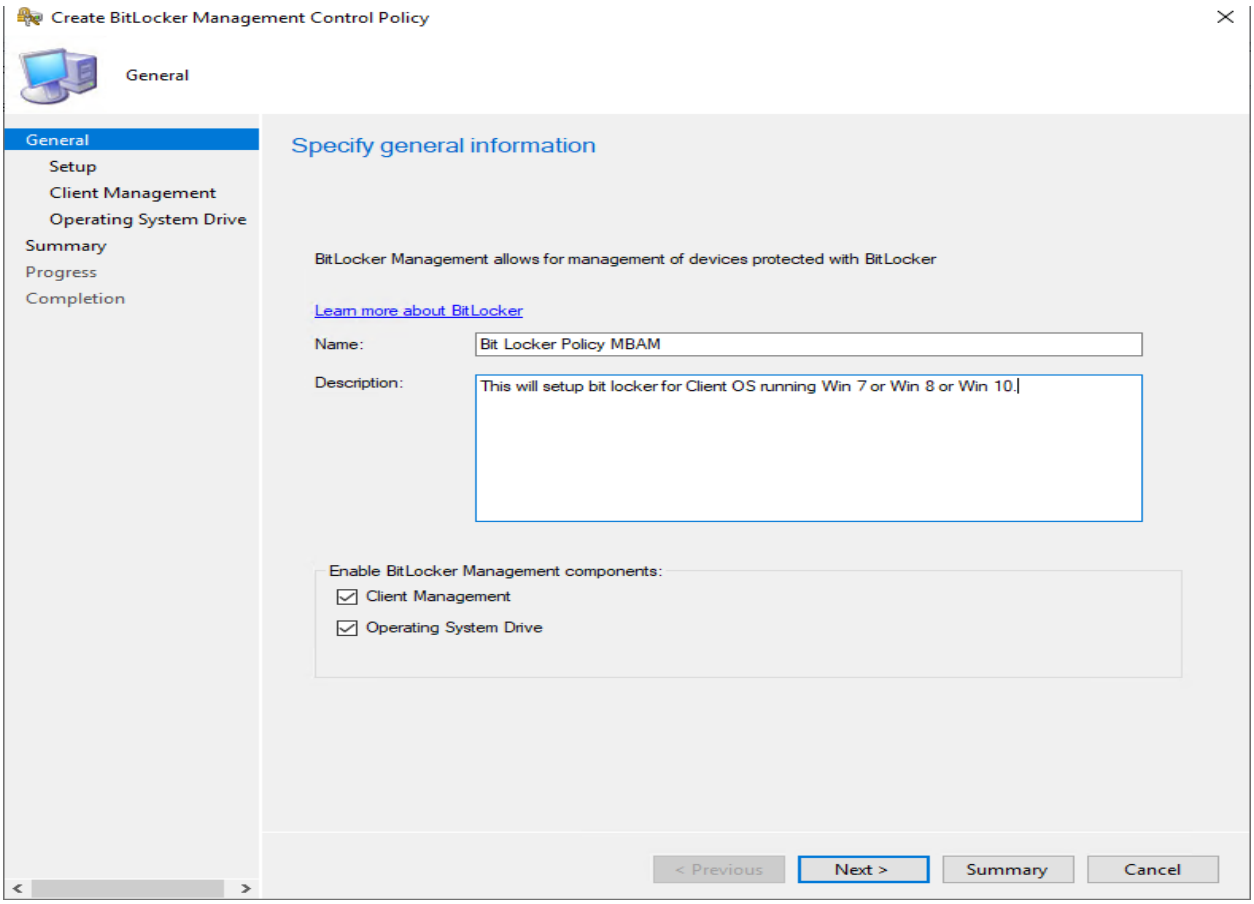




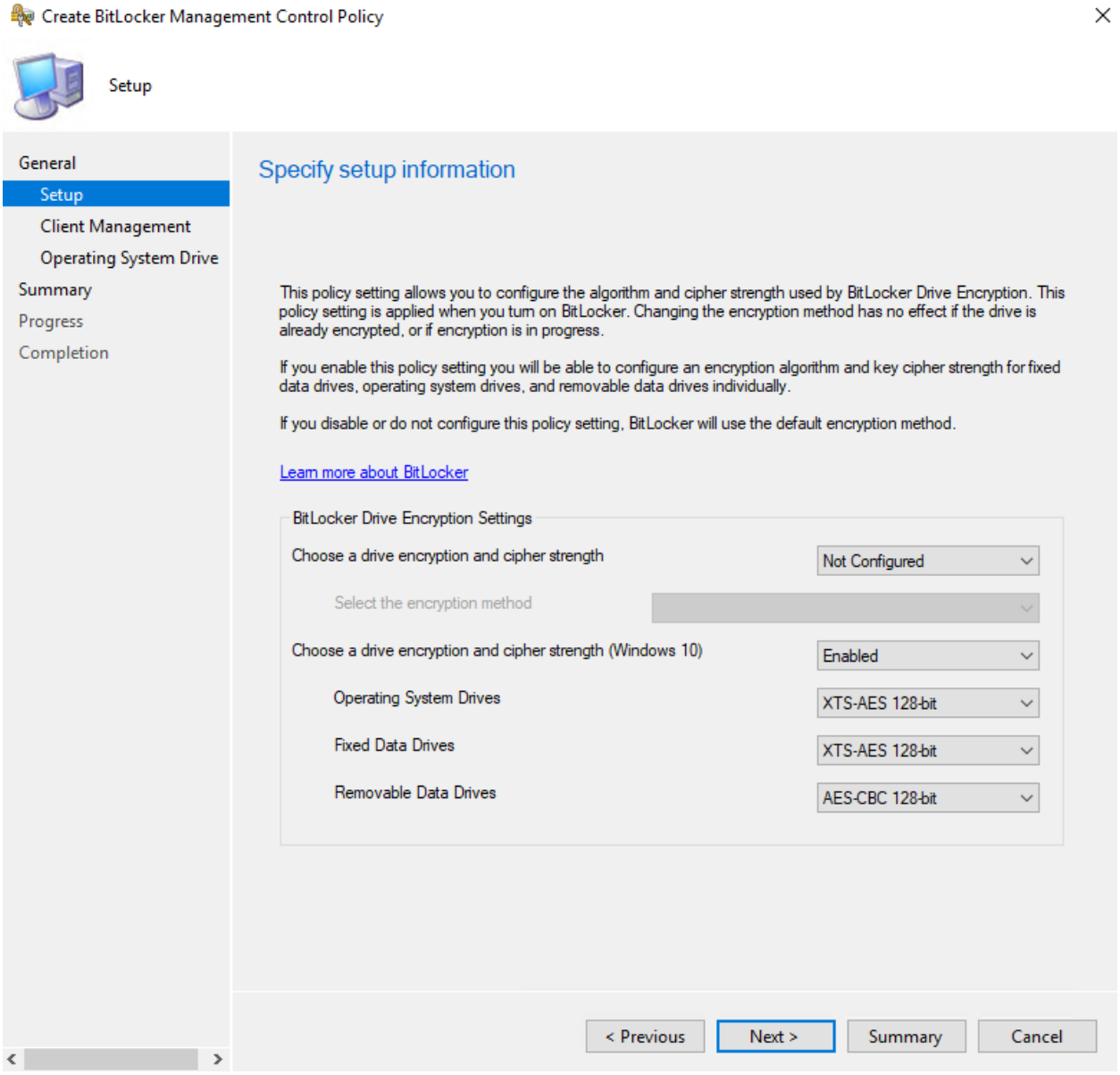
SET MBAM POLICY:

You'll find new MBAM features under \Assets and Compliance\Overview\Endpoint Protection\Bit locker Management (MBAM) in the ConfigMgr console. The first step in the process to implement MBAM is to create your MBAM control policy. To do this, right-click Bit locker Management (MBAM) and select Create BitLocker Management Control Policy.

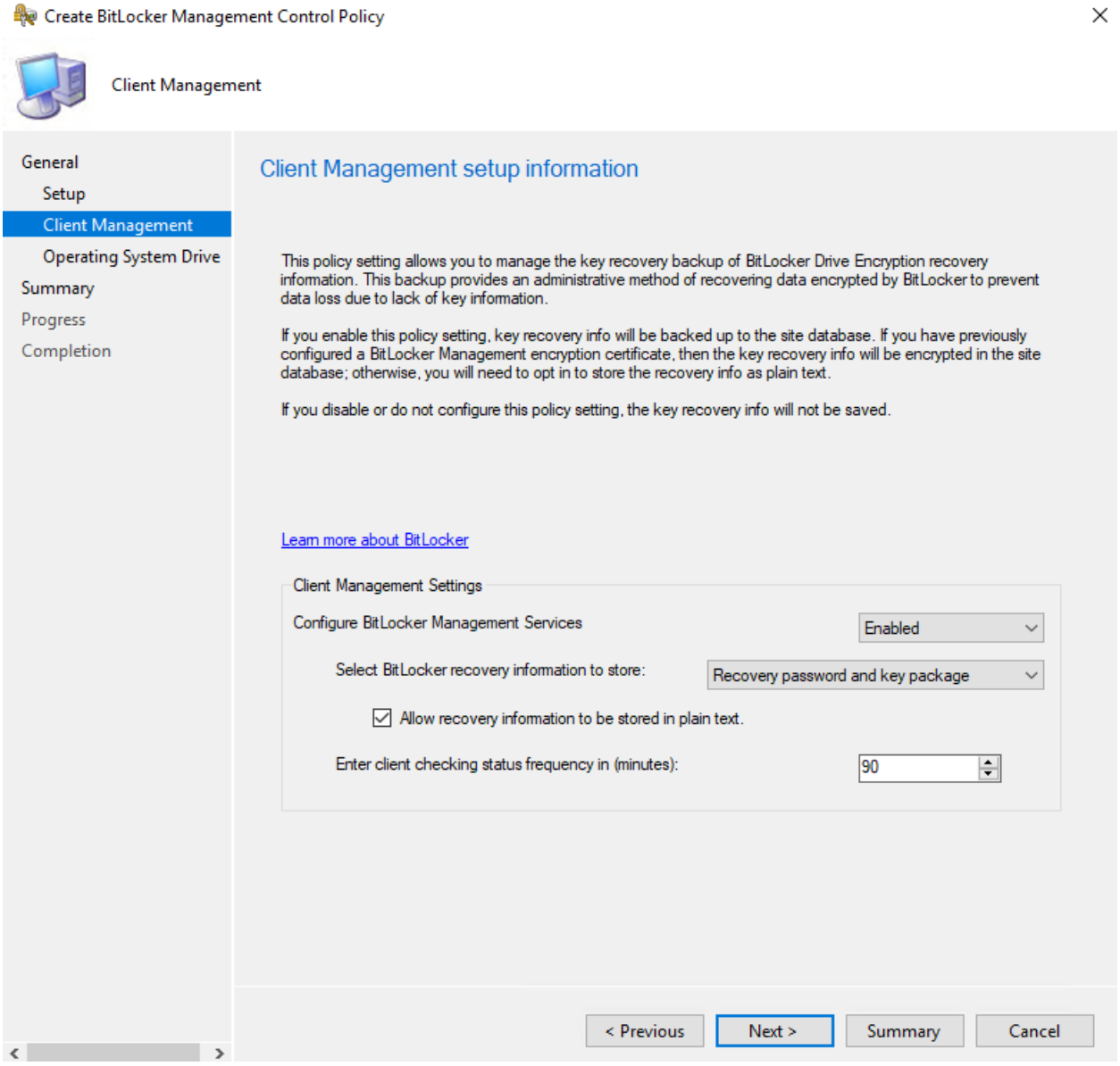




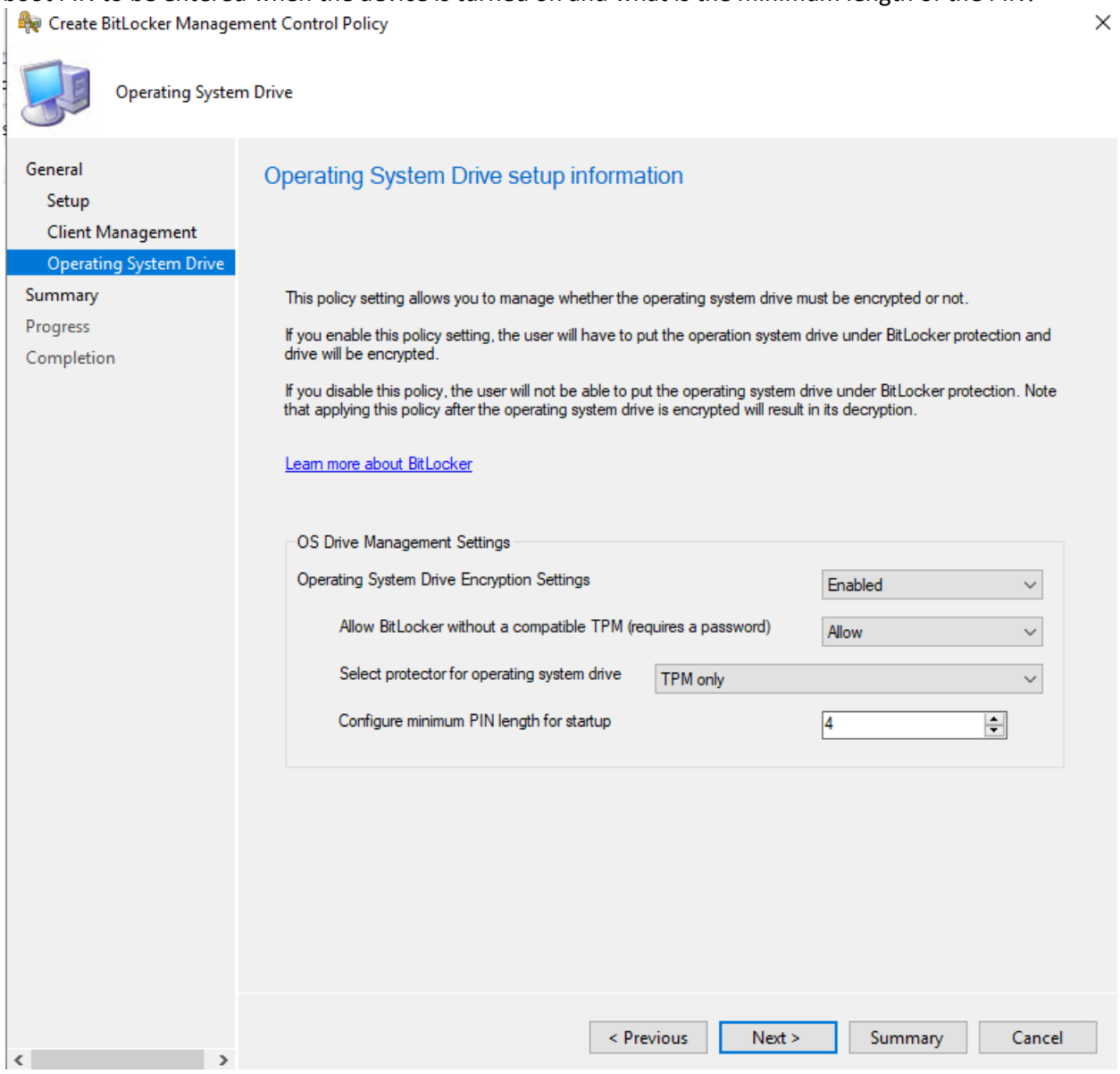
At the Setup screen you will need to decide whether to enable drive encryption and what cipher strength to apply. The top set of options relate to Windows 7 or 8/8.1 devices, whilst our Windows 10 settings are contained in the last set of drop downs. These give us access to the XTS-AES encryption algorithm introduced with Windows 10 1511. I recommend setting operating system encryption to 256-bit to take advantage of the increased bit strength.

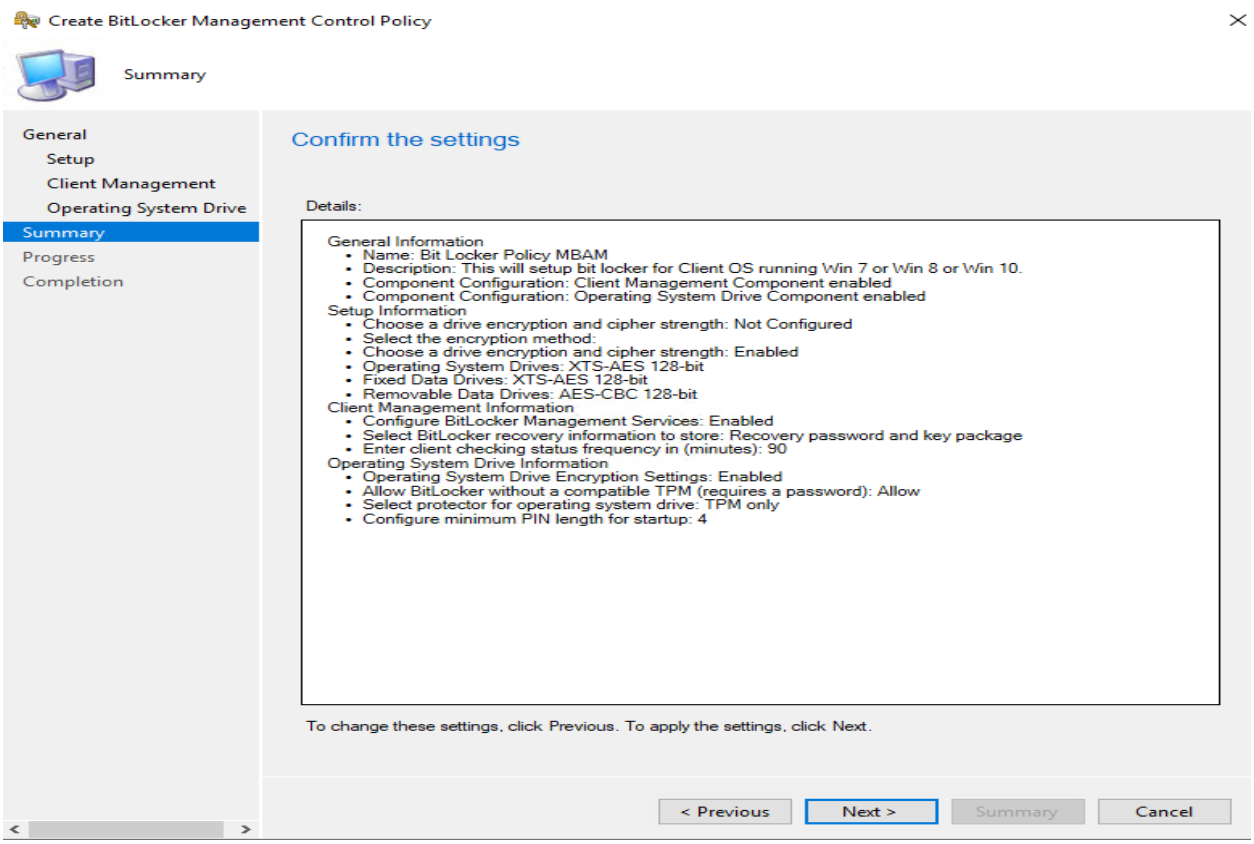


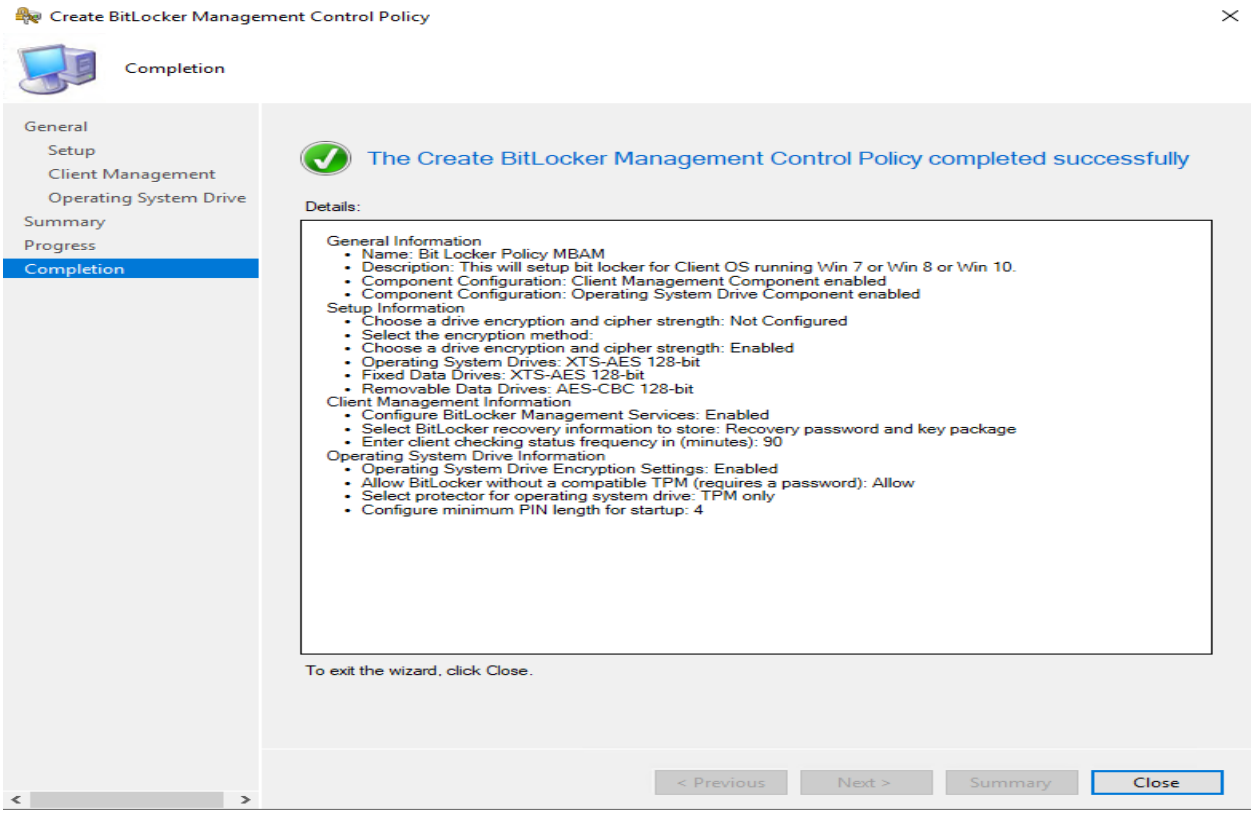
The Client Management screen sets the MBAM settings. Do we want to enable MBAM (I'm pretty sure we do)? Do we want to store the recovery password and key package, or the recovery password only? How often should client check-in with the MBAM service, the default being every 90 minutes?



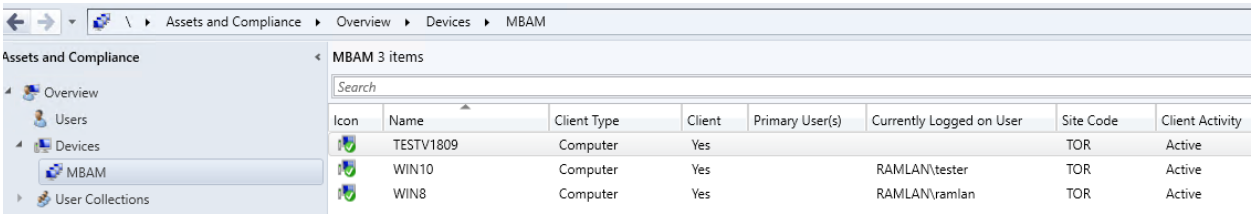
Finally, the Operating System Drive screen allows the definition of TPM options. Do we allow encryption of device without a compatible TPM device? Do we want to set TPM or TPM+PIN, which requires a pre-boot PIN to be entered when the device is turned on and what is the minimum length of the PIN?

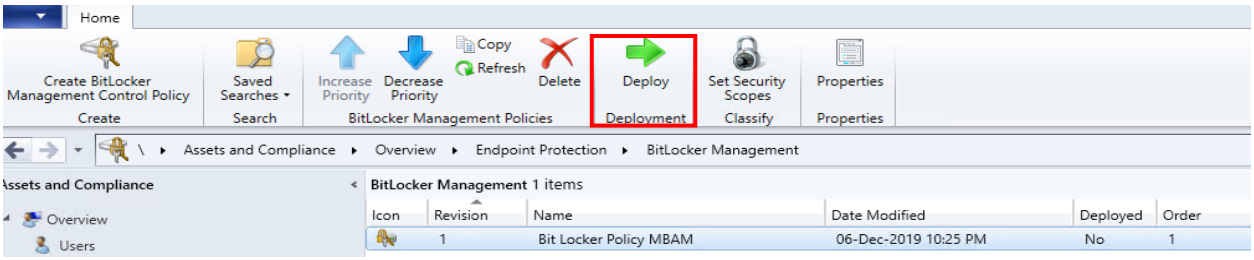


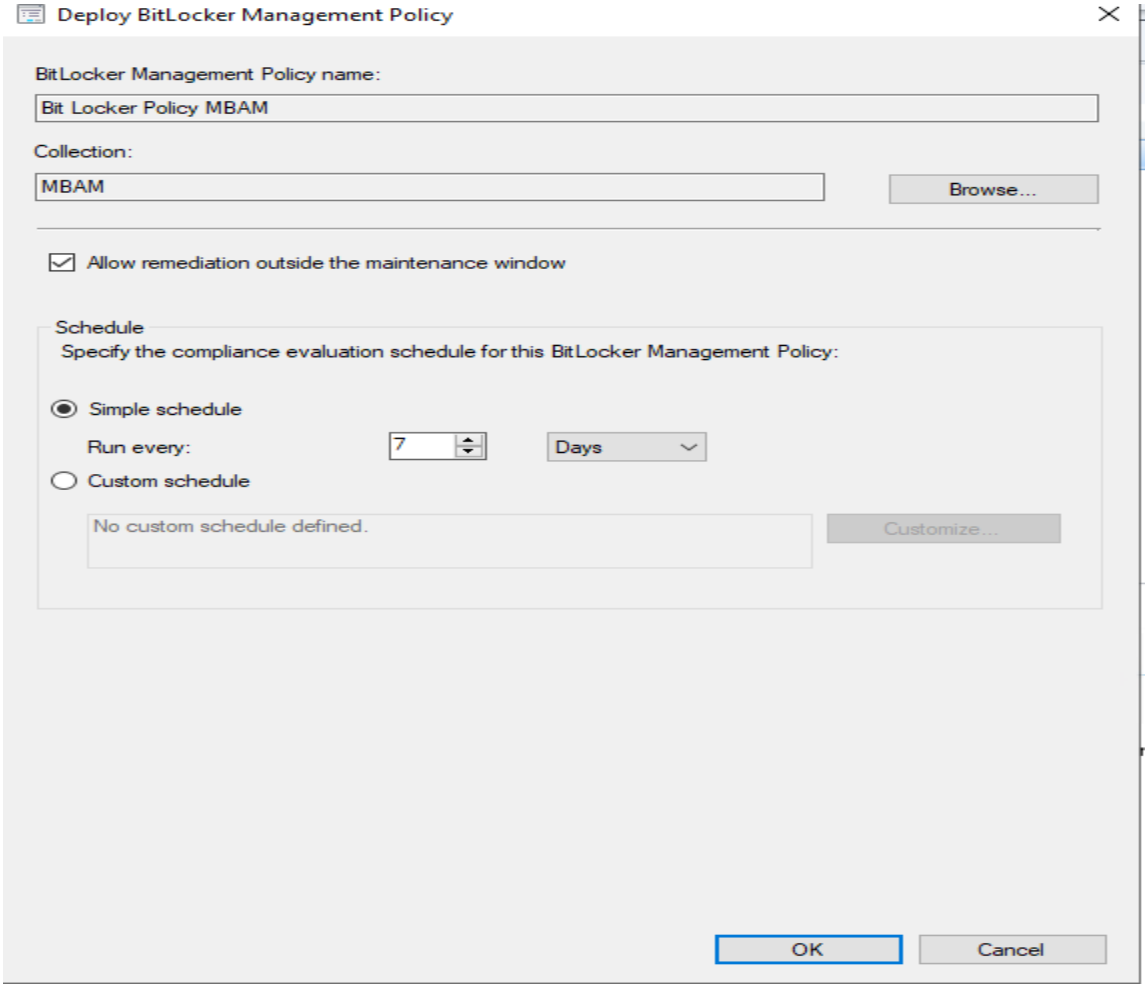

Create BitLocker Management Control Policy
Summary
General
Setup
Client Management
Operating System Drive
Summary
Progress
Completion
Confirm the settings
Details:
General Information
• Name: Bit Locker Policy MBAM
• Description: This will setup bit locker for Client OS running Win 7 or Win 8 or Win 10.
• Component Configuration: Client Management Component enabled
• Component Configuration: Operating System Drive Component enabled
Setup Information
• Choose a drive encryption and cipher strength: Not Configured
• Select the encryption method:
• Choose a drive encryption and cipher strength: Enabled
• Operating System Drives: XTS-AES 128-bit
• Fixed Data Drives: XTS-AES 128-bit
• Removable Data Drives: AES-CBC 128-bit
Client Management Information
• Configure BitLocker Management Services: Enabled
• Select BitLocker recovery information to store: Recovery password and key package
• Enter client checking status frequency in (minutes): 90
Operating System Drive Information
• Operating System Drive Encryption Settings: Enabled
• Allow BitLocker without a compatible TPM (requires a password): Allow
• Select protector for operating system drive: TPM only
• Configure minimum PIN length for startup: 4
To change these settings, click Previous. To apply the settings, click Next.
< Previous
Next >
Summary
Cancel


Create BitLocker Management Control Policy
Completion
General
Setup
Client Management
Operating System Drive
Summary
Progress
Completion
The Create BitLocker Management Control Policy completed successfully
Details:
General Information
• Name: Bit Locker Policy MBAM
• Description: This will setup bit locker for Client OS running Win 7 or Win 8 or Win 10.
• Component Configuration: Client Management Component enabled
• Component Configuration: Operating System Drive Component enabled
Setup Information
• Choose a drive encryption and cipher strength: Not Configured
• Select the encryption method:
• Choose a drive encryption and cipher strength: Enabled
• Operating System Drives: XTS-AES 128-bit
• Fixed Data Drives: XTS-AES 128-bit
• Removable Data Drives: AES-CBC 128-bit
Client Management Information
• Configure BitLocker Management Services: Enabled
• Select BitLocker recovery information to store: Recovery password and key package
• Enter client checking status frequency in (minutes): 90
Operating System Drive Information
• Operating System Drive Encryption Settings: Enabled
• Allow BitLocker without a compatible TPM (requires a password): Allow
• Select protector for operating system drive: TPM only
• Configure minimum PIN length for startup: 4
To exit the wizard, click Close.
< Previous
Next >
Summary
Close

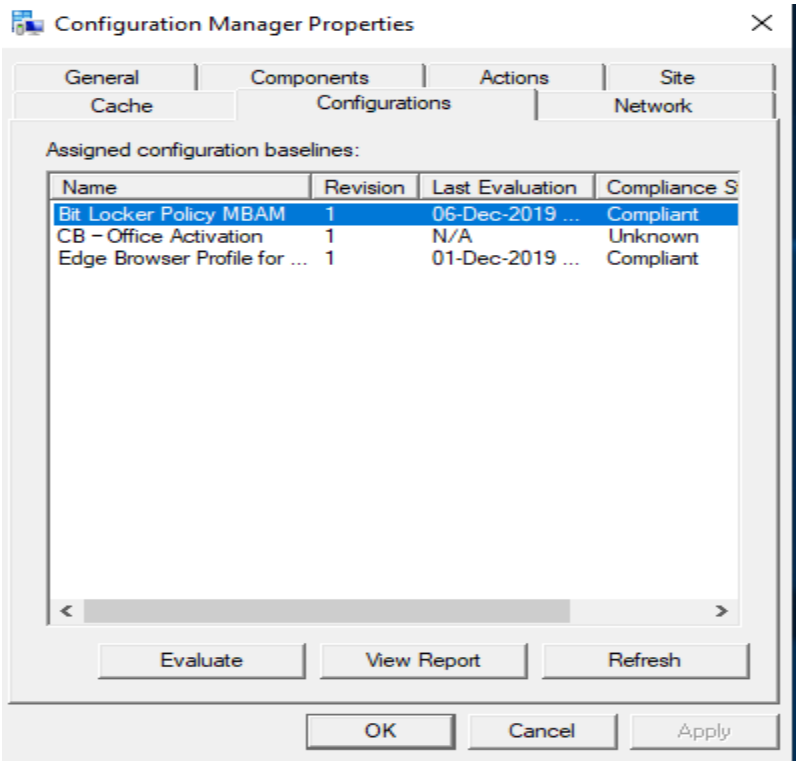
Now it is time to deploy this policy to MBAM collection. I don't have any physical system running Win 7 or Win 8 or Win 10. I will try and use virtual machine and see, if bit locker will work on these systems. They are all Windows 10 workstation running v1909.





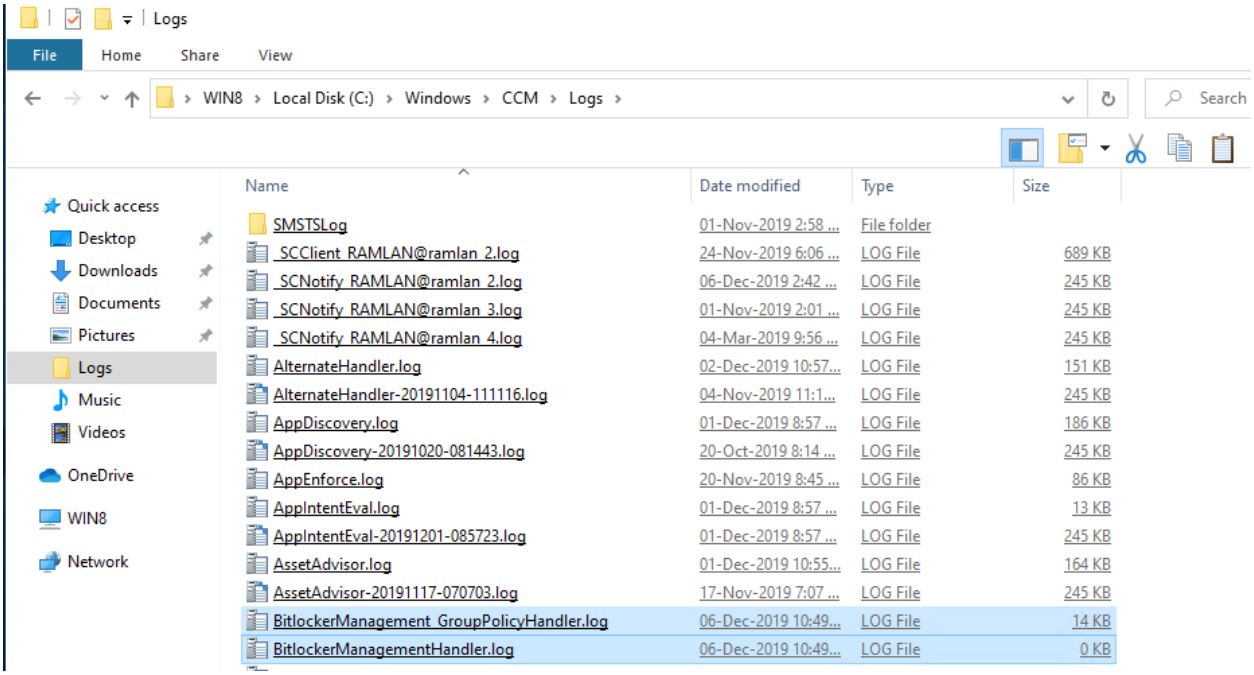


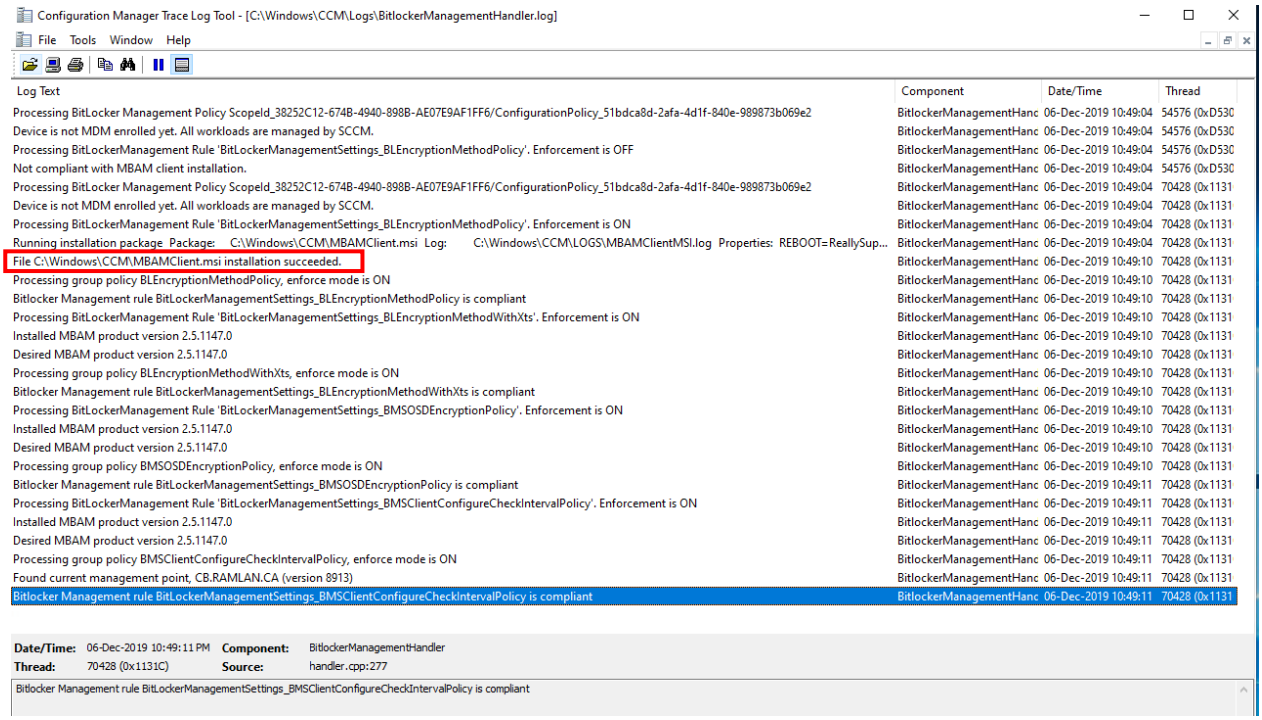
After running Machine and User policy on Win 10 workstation the MBAM policy is compliant.

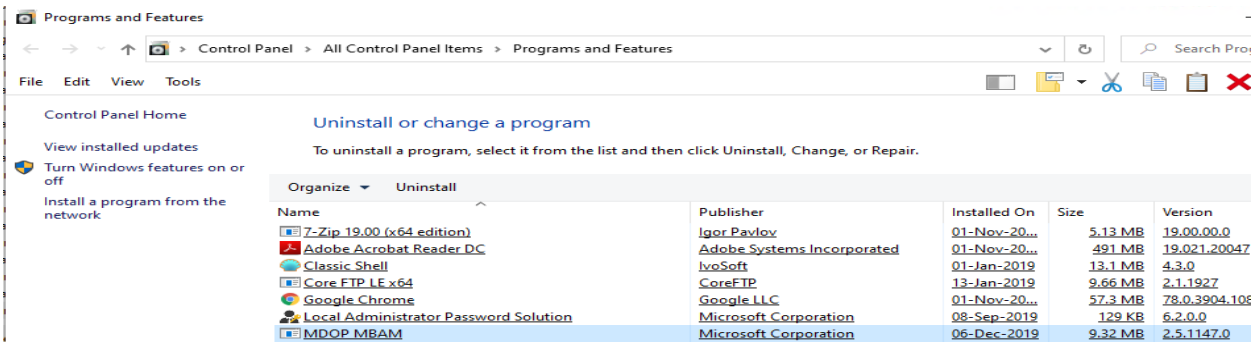


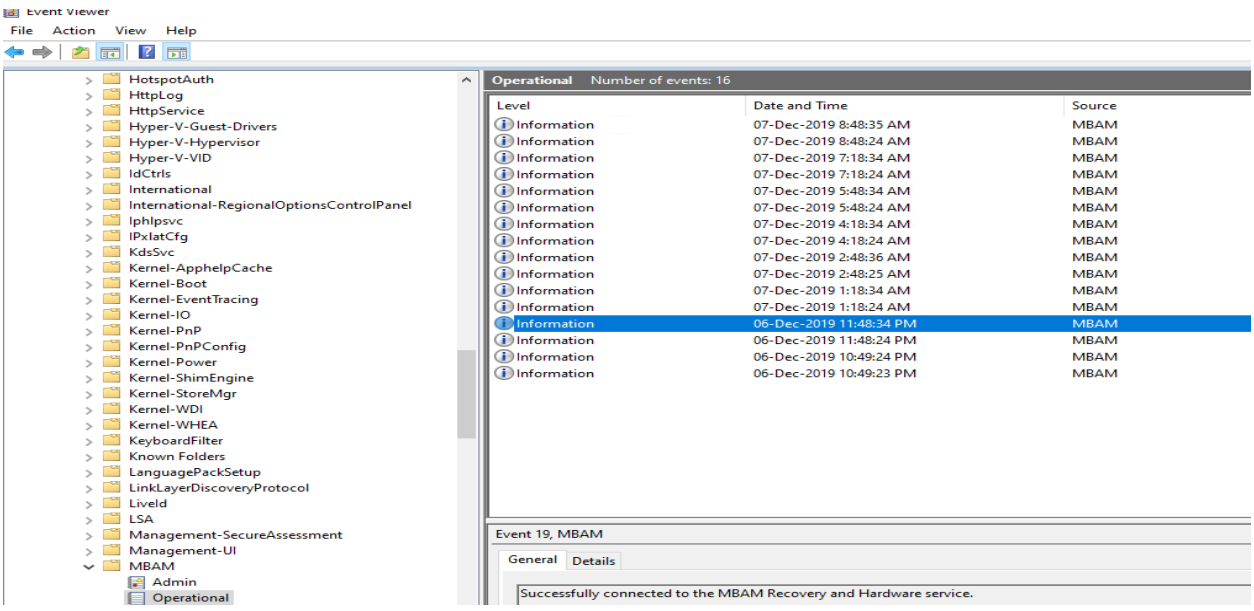
Two new log files will appear in the CCM\Logs folder on the device. These are the BitLockerManagementHandler.log and the BitLockerManagement_GroupPolicyHandler.log.

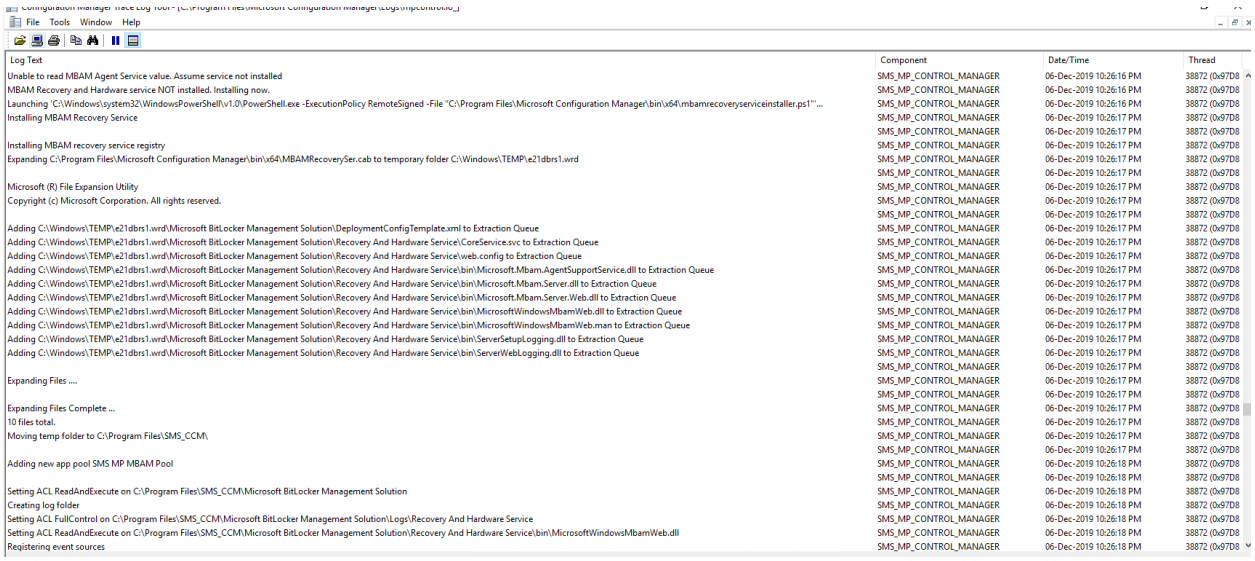
The BitLockerManagementHandler.log records the installation of the MBAM client install on the device.




Configuration Manager Trace Log Tool - [C:\Windows\CCM\Logs\BitlockerManagementHandler.log]
File Tools Window Help
Log Text | Component | Date/Time | Thread
Processing BitLocker Management Policy ScopeId_38252C12-674B-4940-898B-AE07E9AF1FF6/ConfigurationPolicy_51bdca8d-2afa-4d1f-840e-989873b069e2 | BitlockerManagementHanc | 06-Dec-2019 10:49:04 | 54576 (0xD530
Device is not MDM enrolled yet. All workloads are managed by SCCM. | BitlockerManagementHanc | 06-Dec-2019 10:49:04 | 54576 (0xD530
Processing BitLockerManagement Rule 'BitLockerManagementSettings_BLEncryptionMethodPolicy'. Enforcement is OFF | BitlockerManagementHanc | 06-Dec-2019 10:49:04 | 54576 (0xD530
Not compliant with MBAM client installation. | BitlockerManagementHanc | 06-Dec-2019 10:49:04 | 54576 (0xD530
Processing BitLocker Management Policy ScopeId_38252C12-674B-4940-898B-AE07E9AF1FF6/ConfigurationPolicy_51bdca8d-2afa-4d1f-840e-989873b069e2 | BitlockerManagementHanc | 06-Dec-2019 10:49:04 | 70428 (0x1131
Device is not MDM enrolled yet. All workloads are managed by SCCM. | BitlockerManagementHanc | 06-Dec-2019 10:49:04 | 70428 (0x1131
Processing BitLockerManagement Rule 'BitLockerManagementSettings_BLEncryptionMethodPolicy'. Enforcement is ON | BitlockerManagementHanc | 06-Dec-2019 10:49:04 | 70428 (0x1131
Running installation package Package: C:\Windows\CCM\MBAMClient.msi Log: C:\Windows\CCM\LOGS\MBAMClientMSI.log Properties: REBOOT=ReallySup... | BitlockerManagementHanc | 06-Dec-2019 10:49:04 | 70428 (0x1131
File C:\Windows\CCM\MBAMClient.msi installation succeeded. | BitlockerManagementHanc | 06-Dec-2019 10:49:10 | 70428 (0x1131
Processing group policy BLEncryptionMethodPolicy, enforce mode is ON | BitlockerManagementHanc | 06-Dec-2019 10:49:10 | 70428 (0x1131
Bitlocker Management rule BitLockerManagementSettings_BLEncryptionMethodPolicy is compliant | BitlockerManagementHanc | 06-Dec-2019 10:49:10 | 70428 (0x1131
Processing BitLockerManagement Rule 'BitLockerManagementSettings_BLEncryptionMethodWithXts'. Enforcement is ON | BitlockerManagementHanc | 06-Dec-2019 10:49:10 | 70428 (0x1131
Installed MBAM product version 2.5.1147.0 | BitlockerManagementHanc | 06-Dec-2019 10:49:10 | 70428 (0x1131
Desired MBAM product version 2.5.1147.0 | BitlockerManagementHanc | 06-Dec-2019 10:49:10 | 70428 (0x1131
Processing group policy BLEncryptionMethodWithXts, enforce mode is ON | BitlockerManagementHanc | 06-Dec-2019 10:49:10 | 70428 (0x1131
Bitlocker Management rule BitLockerManagementSettings_BLEncryptionMethodWithXts is compliant | BitlockerManagementHanc | 06-Dec-2019 10:49:10 | 70428 (0x1131
Processing BitLockerManagement Rule 'BitLockerManagementSettings_BMSOSDEncryptionPolicy'. Enforcement is ON | BitlockerManagementHanc | 06-Dec-2019 10:49:10 | 70428 (0x1131
Installed MBAM product version 2.5.1147.0 | BitlockerManagementHanc | 06-Dec-2019 10:49:10 | 70428 (0x1131
Desired MBAM product version 2.5.1147.0 | BitlockerManagementHanc | 06-Dec-2019 10:49:10 | 70428 (0x1131
Processing group policy BMSOSDEncryptionPolicy, enforce mode is ON | BitlockerManagementHanc | 06-Dec-2019 10:49:10 | 70428 (0x1131
Bitlocker Management rule BitLockerManagementSettings_BMSOSDEncryptionPolicy is compliant | BitlockerManagementHanc | 06-Dec-2019 10:49:11 | 70428 (0x1131
Processing BitLockerManagement Rule 'BitLockerManagementSettings_BMSClientConfigureCheckIntervalPolicy'. Enforcement is ON | BitlockerManagementHanc | 06-Dec-2019 10:49:11 | 70428 (0x1131
Installed MBAM product version 2.5.1147.0 | BitlockerManagementHanc | 06-Dec-2019 10:49:11 | 70428 (0x1131
Desired MBAM product version 2.5.1147.0 | BitlockerManagementHanc | 06-Dec-2019 10:49:11 | 70428 (0x1131
Processing group policy BMSClientConfigureCheckIntervalPolicy, enforce mode is ON | BitlockerManagementHanc | 06-Dec-2019 10:49:11 | 70428 (0x1131
Found current management point, CB.RAMLAN.CA (version 8913) | BitlockerManagementHanc | 06-Dec-2019 10:49:11 | 70428 (0x1131
Bitlocker Management rule BitLockerManagementSettings_BMSClientConfigureCheckIntervalPolicy is compliant | BitlockerManagementHanc | 06-Dec-2019 10:49:11 | 70428 (0x1131
Date/Time: 06-Dec-2019 10:49:11 PM Component: BitlockerManagementHandler
Thread: 70428 (0x1131C) Source: handler.cpp:277
Bitlocker Management rule BitLockerManagementSettings_BMSClientConfigureCheckIntervalPolicy is compliant

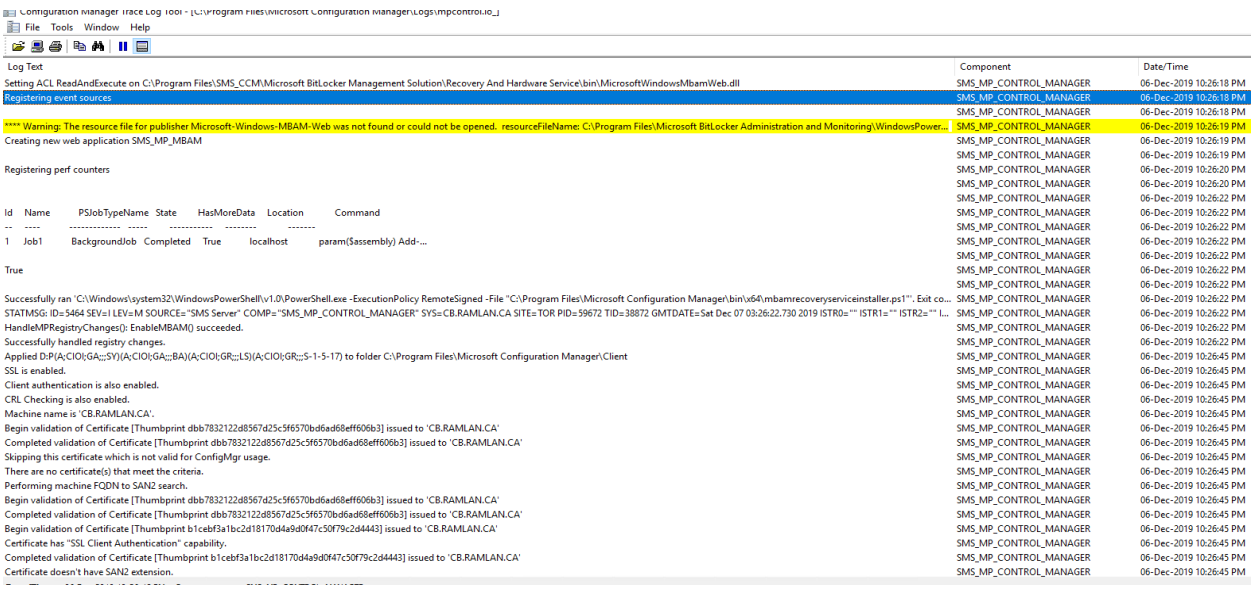

Programs and Features
Control Panel > All Control Panel Items > Programs and Features
File Edit View Tools
Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Uninstall or change a program
To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.
Organize Uninstall
Name | Publisher | Installed On | Size | Version
7-Zip 19.00 (x64 edition) | Igor Pavlov | 01-Nov-20... | 5.13 MB | 19.00.00.0
Adobe Acrobat Reader DC | Adobe Systems Incorporated | 01-Nov-20... | 491 MB | 19.021.20047
Classic Shell | IvoSoft | 01-Jan-2019 | 13.1 MB | 4.3.0
Core FTP LE x64 | CoreFTP | 13-Jan-2019 | 9.66 MB | 2.1.1927
Google Chrome | Google LLC | 01-Nov-20... | 57.3 MB | 78.0.3904.108
Local Administrator Password Solution | Microsoft Corporation | 08-Sep-2019 | 129 KB | 6.2.0.0
MDOP MBAM | Microsoft Corporation | 06-Dec-2019 | 9.32 MB | 2.5.1147.0


Event Viewer
File Action View Help
HotspotAuth
HttpLog
HttpService
Hyper-V-Guest-Drivers
Hyper-V-Hypervisor
Hyper-V-VID
IdCtrls
International
International-RegionalOptionsControlPanel
Iphlpsvc
IPxlatCfg
KdsSvc
Kernel-AppHelpCache
Kernel-Boot
Kernel-EventTracing
Kernel-IO
Kernel-PnP
Kernel-PnPConfig
Kernel-Power
Kernel-ShimEngine
Kernel-StoreMgr
Kernel-WDI
Kernel-WHEA
KeyboardFilter
Known Folders
LanguagePackSetup
LinkLayerDiscoveryProtocol
LiveId
LSA
Management-SecureAssessment
Management-UI
MBAM
Admin
Operational
Operational Number of events: 16
Level | Date and Time | Source
Information | 07-Dec-2019 8:48:35 AM | MBAM
Information | 07-Dec-2019 8:48:24 AM | MBAM
Information | 07-Dec-2019 7:18:34 AM | MBAM
Information | 07-Dec-2019 7:18:24 AM | MBAM
Information | 07-Dec-2019 5:48:34 AM | MBAM
Information | 07-Dec-2019 5:48:24 AM | MBAM
Information | 07-Dec-2019 4:18:34 AM | MBAM
Information | 07-Dec-2019 4:18:24 AM | MBAM
Information | 07-Dec-2019 2:48:36 AM | MBAM
Information | 07-Dec-2019 2:48:25 AM | MBAM
Information | 07-Dec-2019 1:18:34 AM | MBAM
Information | 07-Dec-2019 1:18:24 AM | MBAM
Information | 06-Dec-2019 11:48:34 PM | MBAM
Information | 06-Dec-2019 11:48:24 PM | MBAM
Information | 06-Dec-2019 10:49:24 PM | MBAM
Information | 06-Dec-2019 10:49:23 PM | MBAM
Event 19, MBAM
General Details
Successfully connected to the MBAM Recovery and Hardware service.



File Tools Window Help

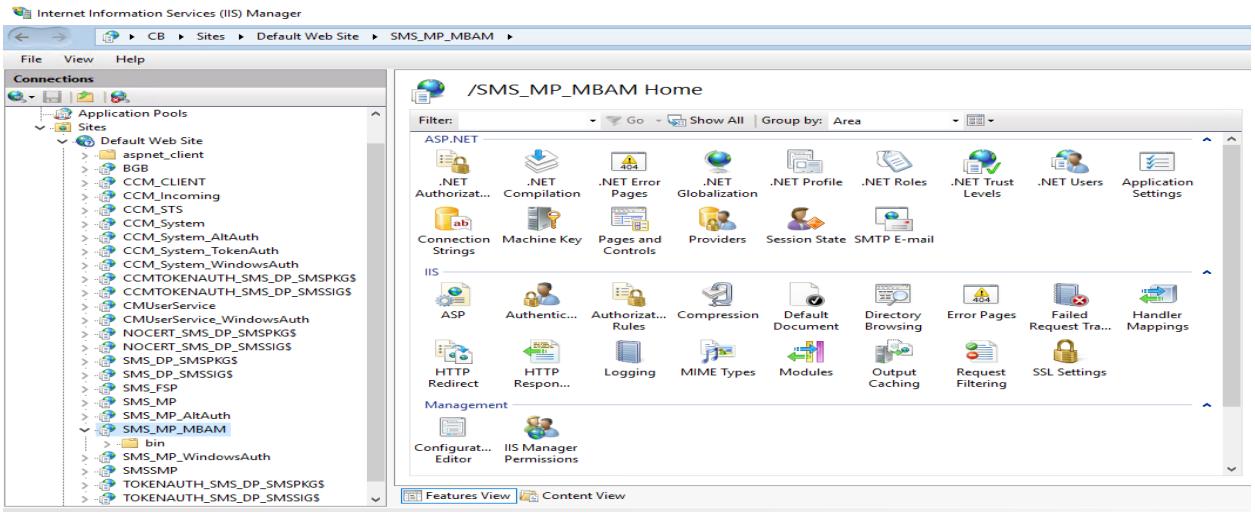
Log Text	Component	Date/Time	Thread
Unable to read MBAM Agent Service value. Assume service not installed	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:16 PM	38872 (0x97D8
MBAM Recovery and Hardware service NOT installed. Installing now.	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:16 PM	38872 (0x97D8
Launching 'C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe -ExecutionPolicy RemoteSigned -File "C:\Program Files\Microsoft Configuration Manager\bin\x64\mbamrecoveryserviceinstaller.ps1"'...	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:16 PM	38872 (0x97D8
Installing MBAM Recovery Service	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
Installing MBAM recovery service registry	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
Expanding C:\Program Files\Microsoft Configuration Manager\bin\x64\MBAMRecoverySer.cab to temporary folder C:\Windows\TEMP\e21dbrs1.wrd	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
Microsoft (R) File Expansion Utility	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
Copyright (c) Microsoft Corporation. All rights reserved.	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
Adding C:\Windows\TEMP\e21dbrs1.wrd\Microsoft BitLocker Management Solution\DeploymentConfigTemplate.xml to Extraction Queue	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
Adding C:\Windows\TEMP\e21dbrs1.wrd\Microsoft BitLocker Management Solution\Recovery And Hardware Service\CoreService.svc to Extraction Queue	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
Adding C:\Windows\TEMP\e21dbrs1.wrd\Microsoft BitLocker Management Solution\Recovery And Hardware Service\web.config to Extraction Queue	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
Adding C:\Windows\TEMP\e21dbrs1.wrd\Microsoft BitLocker Management Solution\Recovery And Hardware Service\bin\Microsoft.Mbam.AgentSupportService.dll to Extraction Queue	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
Adding C:\Windows\TEMP\e21dbrs1.wrd\Microsoft BitLocker Management Solution\Recovery And Hardware Service\bin\Microsoft.Mbam.Server.dll to Extraction Queue	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
Adding C:\Windows\TEMP\e21dbrs1.wrd\Microsoft BitLocker Management Solution\Recovery And Hardware Service\bin\Microsoft.Mbam.Server.Web.dll to Extraction Queue	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
Adding C:\Windows\TEMP\e21dbrs1.wrd\Microsoft BitLocker Management Solution\Recovery And Hardware Service\bin\MicrosoftWindowsMbamWeb.dll to Extraction Queue	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
Adding C:\Windows\TEMP\e21dbrs1.wrd\Microsoft BitLocker Management Solution\Recovery And Hardware Service\bin\MicrosoftWindowsMbamWeb.man to Extraction Queue	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
Adding C:\Windows\TEMP\e21dbrs1.wrd\Microsoft BitLocker Management Solution\Recovery And Hardware Service\bin\ServerSetupLogging.dll to Extraction Queue	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
Adding C:\Windows\TEMP\e21dbrs1.wrd\Microsoft BitLocker Management Solution\Recovery And Hardware Service\bin\ServerWebLogging.dll to Extraction Queue	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
Expanding Files	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
Expanding Files Complete ...	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
10 files total.	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
Moving temp folder to C:\Program Files\SMS_CCM\	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:17 PM	38872 (0x97D8
Adding new app pool SMS MP MBAM Pool	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:18 PM	38872 (0x97D8
	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:18 PM	38872 (0x97D8
Setting ACL ReadAndExecute on C:\Program Files\SMS_CCM\Microsoft BitLocker Management Solution	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:18 PM	38872 (0x97D8
Creating log folder	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:18 PM	38872 (0x97D8
Setting ACL FullControl on C:\Program Files\SMS_CCM\Microsoft BitLocker Management Solution\Logs\Recovery And Hardware Service	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:18 PM	38872 (0x97D8
Setting ACL ReadAndExecute on C:\Program Files\SMS_CCM\Microsoft BitLocker Management Solution\Recovery And Hardware Service\bin\MicrosoftWindowsMbamWeb.dll	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:18 PM	38872 (0x97D8
Registering event sources	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:18 PM	38872 (0x97D8



Configuration Manager Trace Log Tool - [C:\Program Files\Microsoft Configuration Manager\Logs\mpcontrol.log]

File Tools Window Help

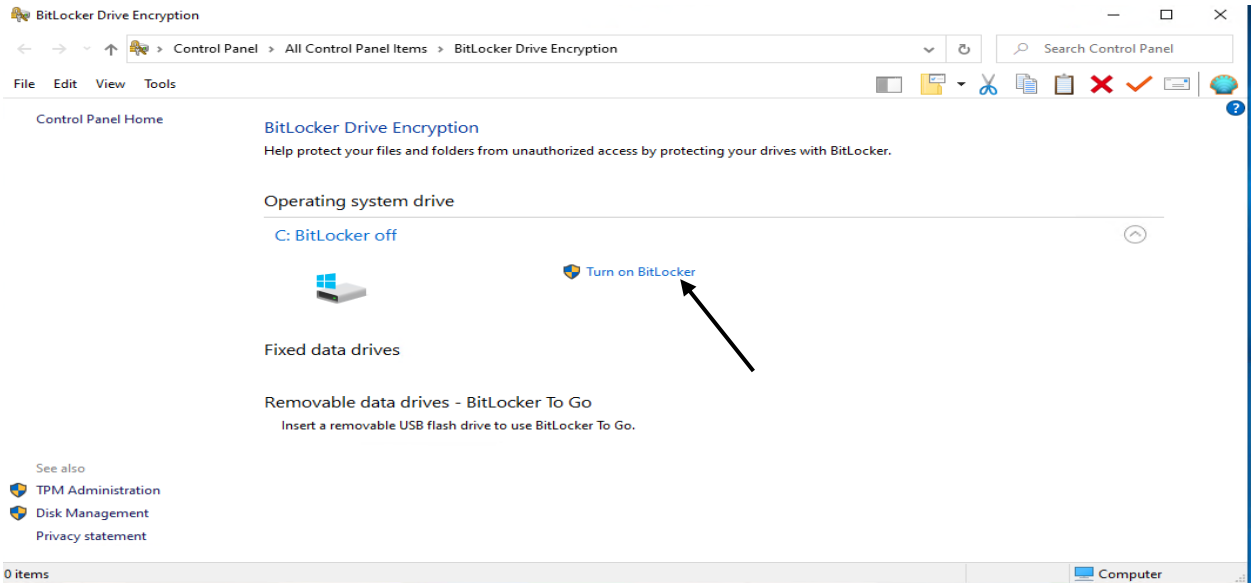
Log Text	Component	Date/Time
Setting ACL ReadAndExecute on C:\Program Files\SMS_CCM\Microsoft BitLocker Management Solution\Recovery And Hardware Service\bin\MicrosoftWindowsMbamWeb.dll	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:18 PM
Registering event sources	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:18 PM
	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:18 PM
**** Warning: The resource file for publisher Microsoft-Windows-MBAM-Web was not found or could not be opened. resourceFileName: C:\Program Files\Microsoft BitLocker Administration and Monitoring\WindowsPower...	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:19 PM
Creating new web application SMS_MP_MBAM	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:19 PM
	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:19 PM
Registering perf counters	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:20 PM
	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:20 PM
	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:22 PM
Id Name PSJobTypeName State HasMoreData Location Command	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:22 PM
-- ---- ------------- ----- ----------- -------- -------	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:22 PM
1 Job1 BackgroundJob Completed True localhost param($assembly) Add-...	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:22 PM
	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:22 PM
True	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:22 PM
	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:22 PM
Successfully ran 'C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe -ExecutionPolicy RemoteSigned -File "C:\Program Files\Microsoft Configuration Manager\bin\x64\mbamrecoveryserviceinstaller.ps1"'. Exit co...	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:22 PM
STATMSG: ID=5464 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_MP_CONTROL_MANAGER" SYS=CB.RAMLAN.CA SITE=TOR PID=59672 TID=38872 GMTDATE=Sat Dec 07 03:26:22.730 2019 ISTR0="" ISTR1="" ISTR2="" I...	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:22 PM
HandleMPRegistryChanges(): EnableMBAM() succeeded.	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:22 PM
Successfully handled registry changes.	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:22 PM
Applied D:P(A;CIOI;GA;;;SY)(A;CIOI;GA;;;BA)(A;CIOI;GR;;;LS)(A;CIOI;GR;;;S-1-5-17) to folder C:\Program Files\Microsoft Configuration Manager\Client	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:45 PM
SSL is enabled.	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:45 PM
Client authentication is also enabled.	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:45 PM
CRL Checking is also enabled.	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:45 PM
Machine name is 'CB.RAMLAN.CA'.	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:45 PM
Begin validation of Certificate [Thumbprint dbb7832122d8567d25c5f6570bd6ad68eff606b3] issued to 'CB.RAMLAN.CA'	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:45 PM
Completed validation of Certificate [Thumbprint dbb7832122d8567d25c5f6570bd6ad68eff606b3] issued to 'CB.RAMLAN.CA'	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:45 PM
Skipping this certificate which is not valid for ConfigMgr usage.	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:45 PM
There are no certificate(s) that meet the criteria.	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:45 PM
Performing machine FQDN to SAN2 search.	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:45 PM
Begin validation of Certificate [Thumbprint dbb7832122d8567d25c5f6570bd6ad68eff606b3] issued to 'CB.RAMLAN.CA'	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:45 PM
Completed validation of Certificate [Thumbprint dbb7832122d8567d25c5f6570bd6ad68eff606b3] issued to 'CB.RAMLAN.CA'	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:45 PM
Begin validation of Certificate [Thumbprint b1cebf3a1bc2d18170d4a9d0f47c50f79c2d4443] issued to 'CB.RAMLAN.CA'	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:45 PM
Certificate has "SSL Client Authentication" capability.	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:45 PM
Completed validation of Certificate [Thumbprint b1cebf3a1bc2d18170d4a9d0f47c50f79c2d4443] issued to 'CB.RAMLAN.CA'	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:45 PM
Certificate doesn't have SAN2 extension.	SMS_MP_CONTROL_MANAGER	06-Dec-2019 10:26:45 PM

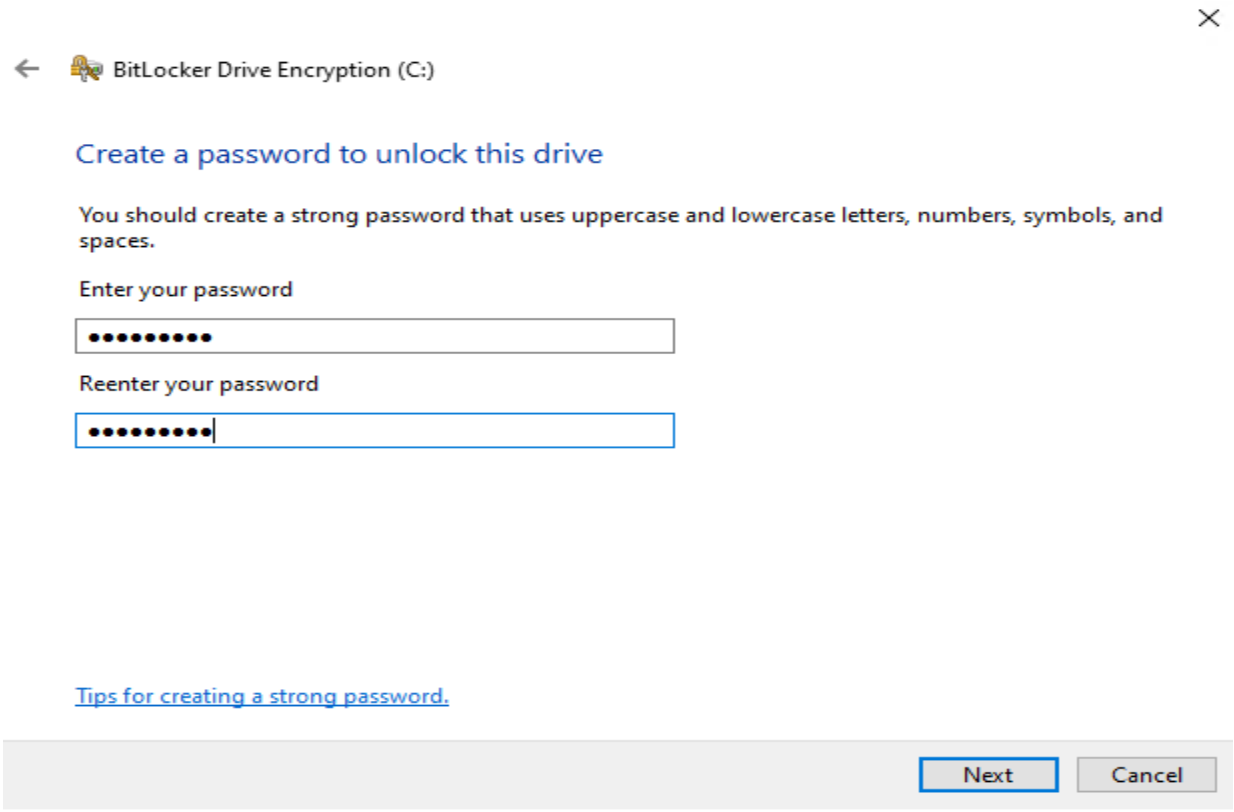


Encryption and MBAM magic:

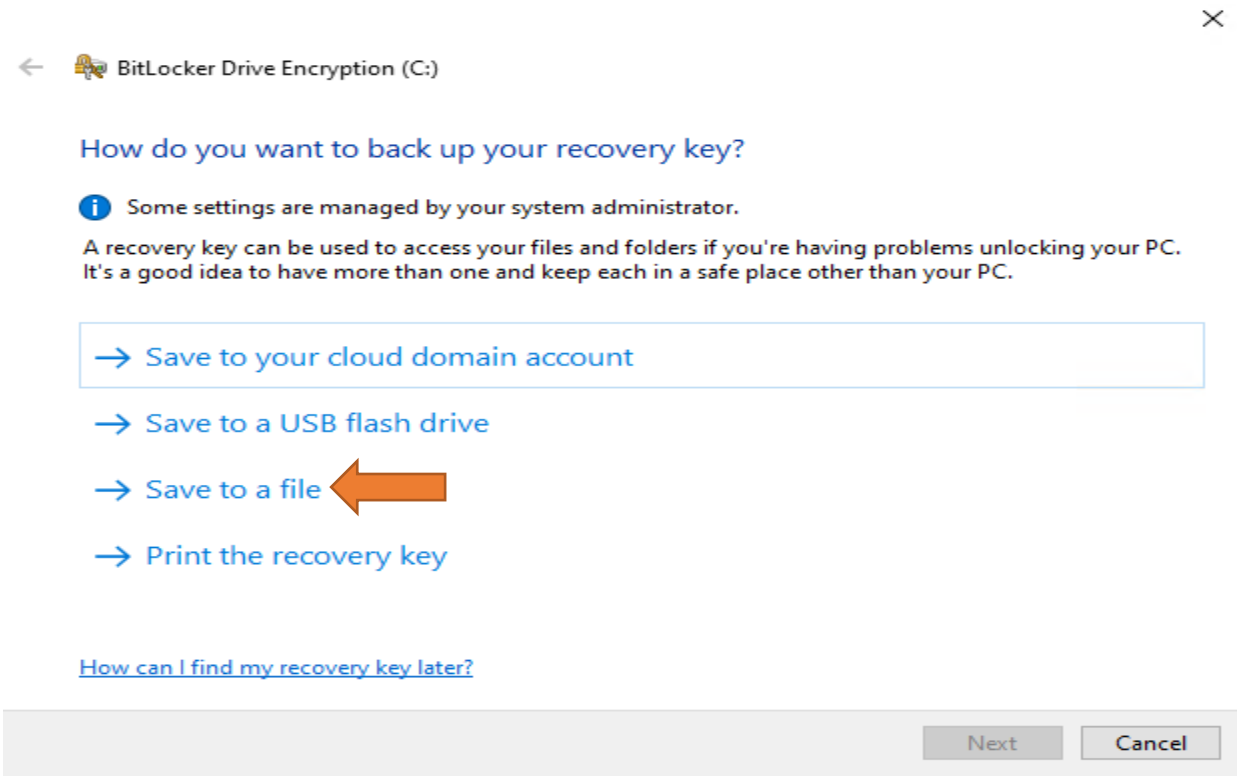
Here is the screen shot of Windows 10 workstation where Bit Locker is turned off. I was not using bit locker before. Now we have integrated MBAM with CB1910 and created MBAM policy, we can turn on bit locker. You don't have to do this, if you have physical machine. I am running all virtual machines. Hence have to turn bit locker to start the encryption process.

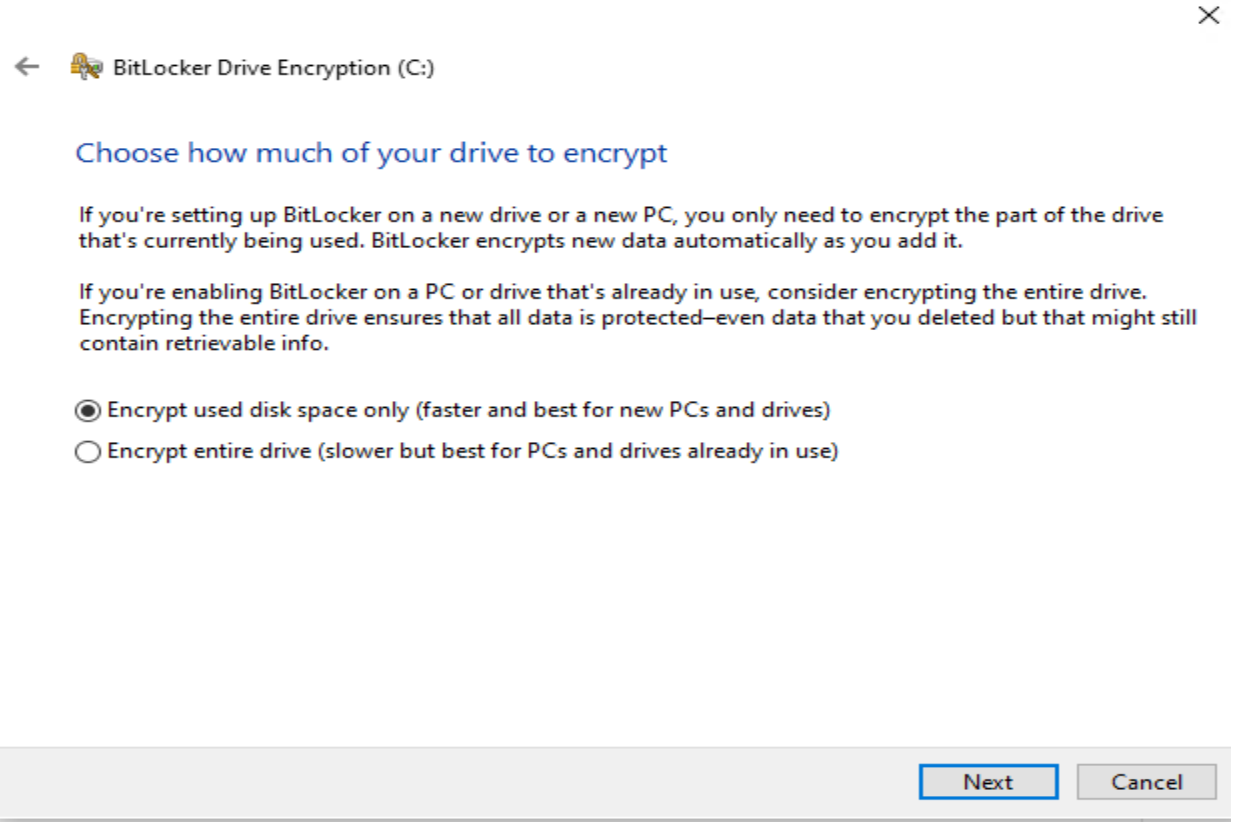
If you are testing this with a virtual machine, you might get a failure to encrypt error. The Event Viewer logs might state BitLocker Drive Encryption only supports Used Space Only Encryption on thin provisioned storage.

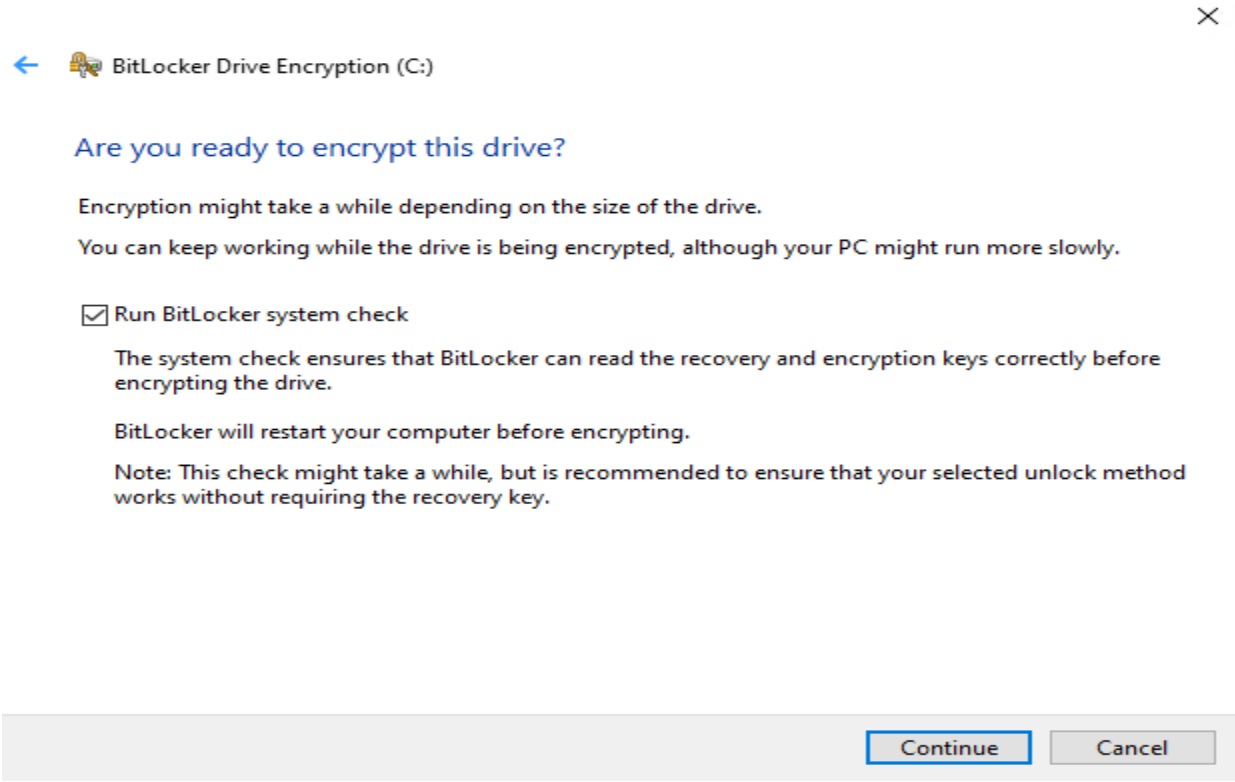


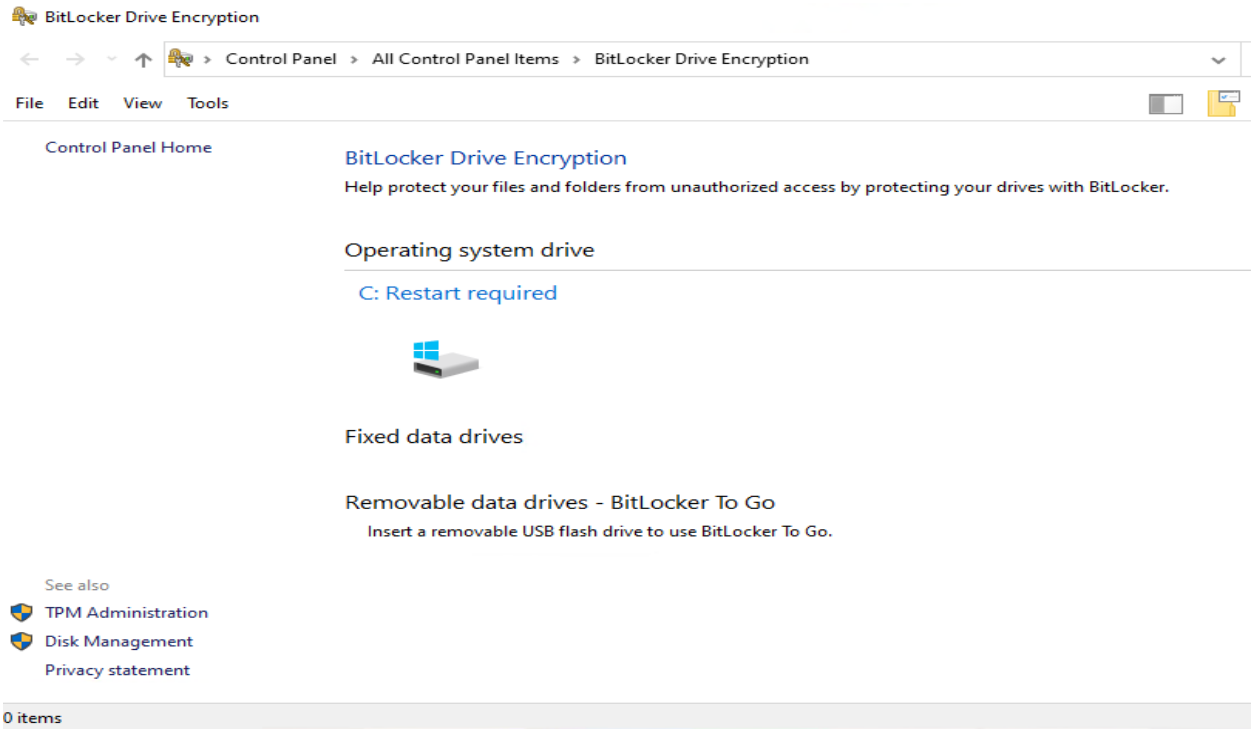


I saved the key to network share on DC.

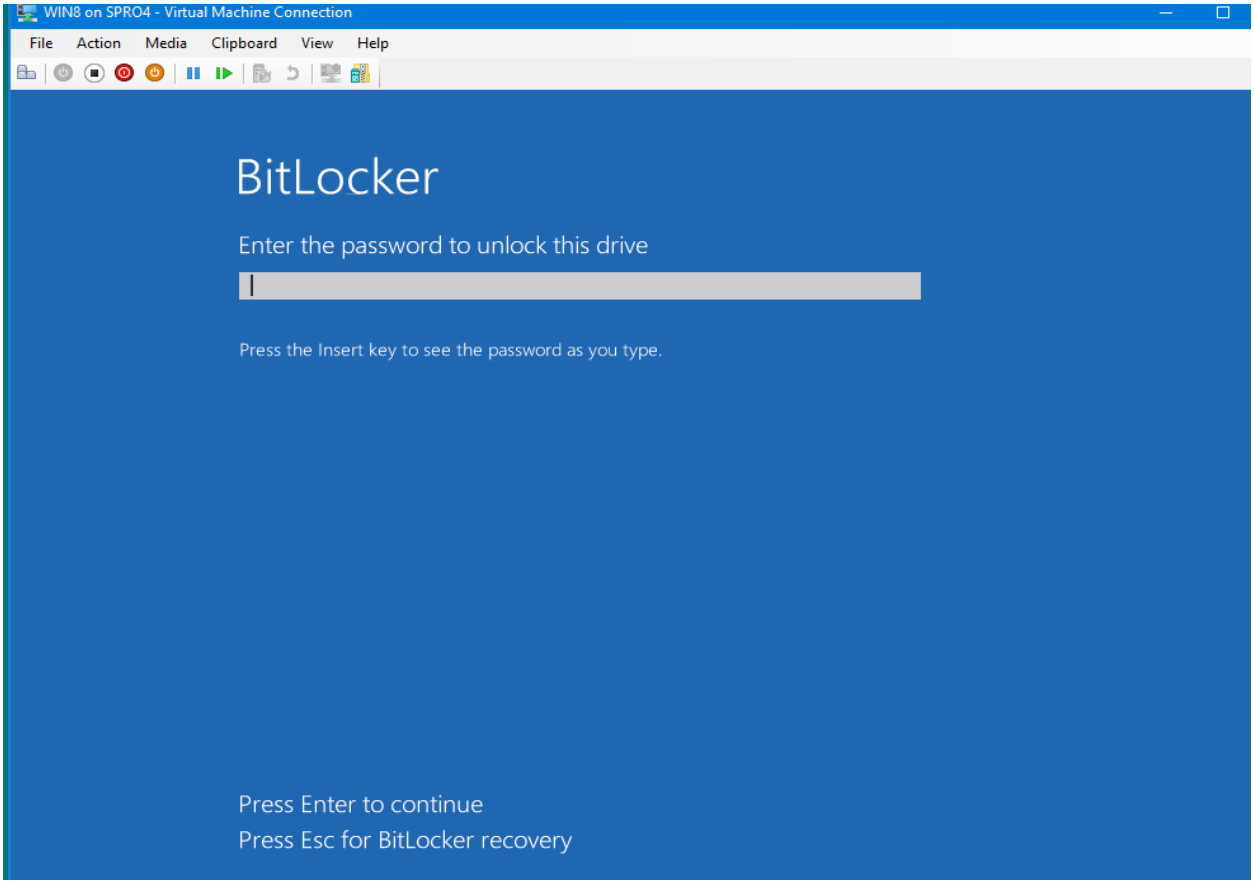



BitLocker Drive Encryption (C:)
Choose how much of your drive to encrypt
If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.
If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected–even data that you deleted but that might still contain retrievable info.
Encrypt used disk space only (faster and best for new PCs and drives)
Encrypt entire drive (slower but best for PCs and drives already in use)
Next
Cancel

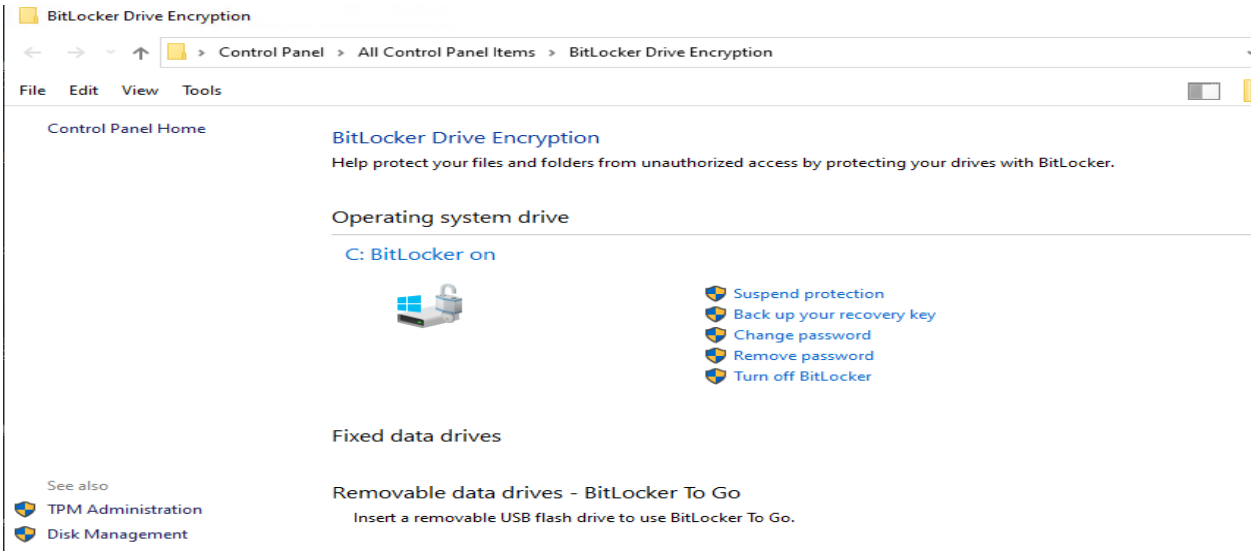

BitLocker Drive Encryption (C:)
Are you ready to encrypt this drive?
Encryption might take a while depending on the size of the drive.
You can keep working while the drive is being encrypted, although your PC might run more slowly.
Run BitLocker system check
The system check ensures that BitLocker can read the recovery and encryption keys correctly before encrypting the drive.
BitLocker will restart your computer before encrypting.
Note: This check might take a while, but is recommended to ensure that your selected unlock method works without requiring the recovery key.
Continue
Cancel



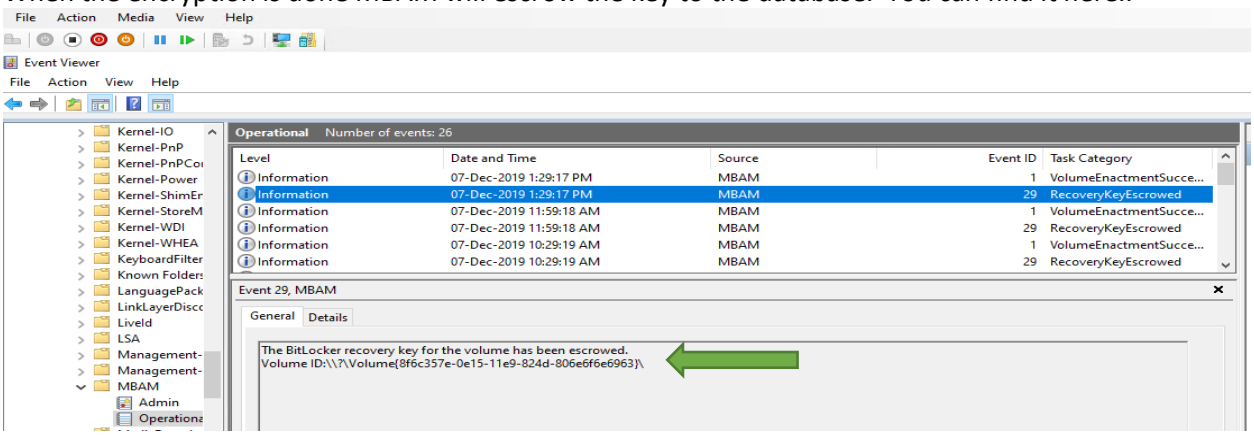
On restart we have to enter the password that was set before.



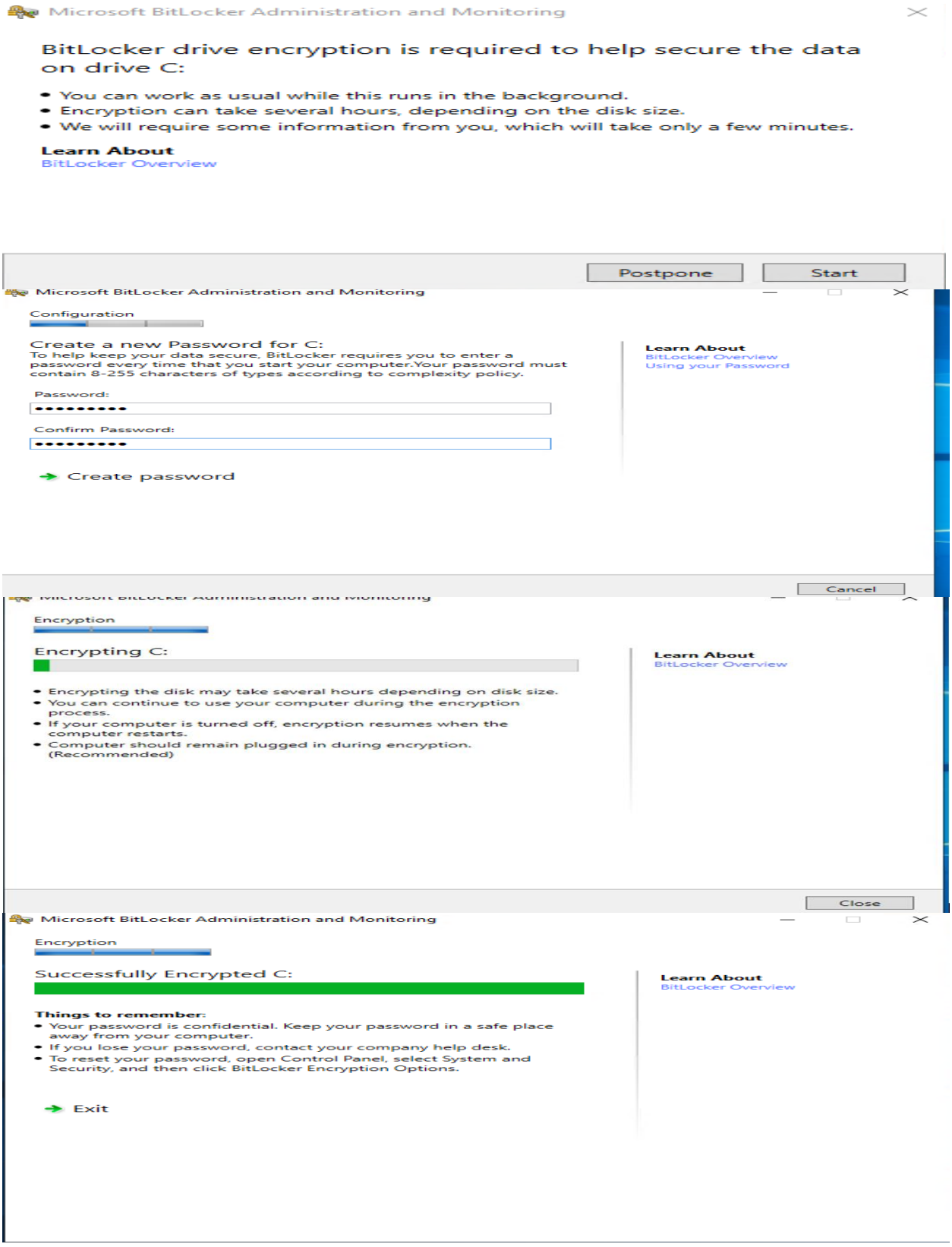
Encryption has started



When the encryption is done MBAM will escrow the key to the database. You can find it here..

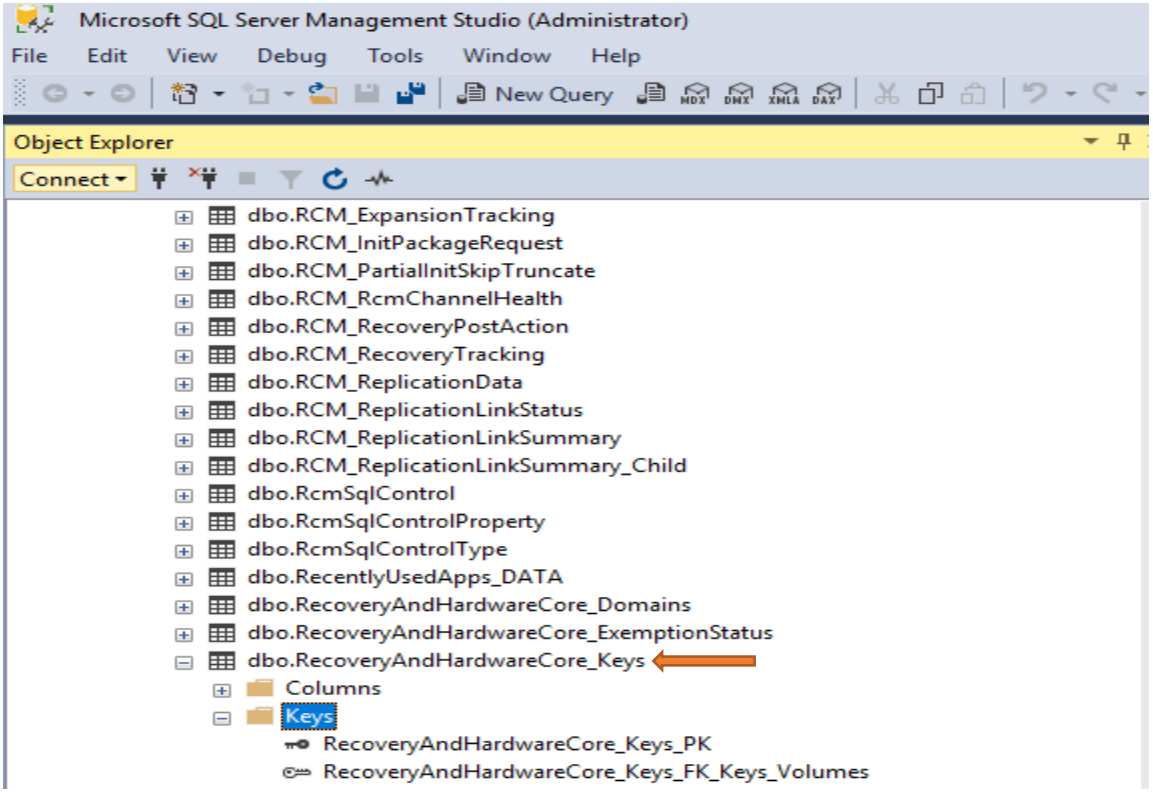


You might see this type of screen shot as well when the MBAM policy is applied.



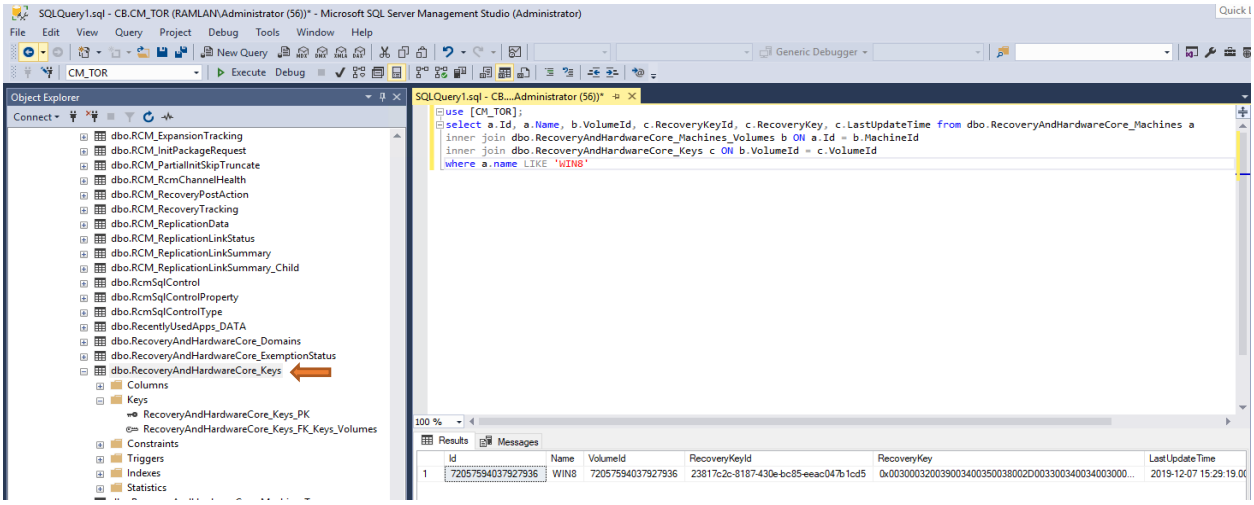
Getting keys from the Database:

The recovery keys are stored in SCCM Database at this location dbo.RecoveryAndHardwareCore_Keys



<u>Get Recovery key data based on Computer Name</u>

```
use [CM_TOR];
select a.Id, a.Name, b.VolumeId, c.RecoveryKeyId, c.RecoveryKey, c.LastUpdateTime from
dbo.RecoveryAndHardwareCore_Machines a
inner join dbo.RecoveryAndHardwareCore_Machines_Volumes b ON a.Id = b.MachineId
inner join dbo.RecoveryAndHardwareCore_Keys c ON b.VolumeId = c.VolumeId
where a.name LIKE 'WIN8'
```



Now we have a fully integrated MBAM within CB1910. If you had setup MBAM server before in production it can be retired. I am not sure how recovery key will be moved or transferred or will the same key work after the integration.

With this question in mind and no answer, I posted a short tweet and got these responses.

Thanks

Ram Lan
7th Dec 2019