GUIDE – APRIL 2019

PRINTED 1 APRIL 2019

MANAGING THE ENCRYPTION LIFE-CYCLE FOR WINDOWS 10: VMWARE WORKSPACE ONE OPERATIONAL TUTORIAL

VMware Workspace ONE

vmware®

Table of Contents

Managing the Encryption Life-Cycle for Windows 10

Overview

Introduction

VMware provides this operational tutorial to help you with your VMware Workspace ONE® environment. This tutorial helps you to manage the encryption life-cycle for Windows 10 devices using VMware Workspace ONE® UEM. You migrate from McAfee Management of Native Encryption, configure a BitLocker Encryption profile, and verify the encryption settings applied.

Audience

This operational tutorial is intended for IT professionals and Workspace ONE administrators of existing production environments. Familiarity with networking and storage in a virtual environment is assumed, including Active Directory, identity management, and directory services. Knowledge of additional technologies such as VMware Identity Manager™ and VMware Workspace ONE® UEM, is also helpful.

Managing the Encryption Life-Cycle for Windows 10

Introduction

This exercise helps you to configure automated encryption with Workspace ONE UEM. In this exercise, you migrate from McAfee, configure a BitLocker Encryption profile, and verify the profile applied. The steps are sequential and build upon one another, so make sure that you complete the steps in order.

Consumer Simple Encryption

When it comes to BitLocker encryption for Windows 10 devices, a security by design approach provides the best user experience. Security by design implements device encryption in a way that feels like a non-disruptive, natural part of the device experience. To watch a video demonstrating security by design, click VMware Workspace ONE BitLocker Management End-User Experience or click the video itself.

Enterprise Secure Devices

Create a BitLocker Encryption profile to keep Windows 10 device data enterprise secure. Once configured, Workspace ONE UEM Agent automatically enforces encryption settings as part of the device's general security posture. To watch a video demonstrating this procedure, click VMware Workspace ONE BitLocker Management Experience, or click the video itself.

Prerequisites

Before you can perform the procedures in this tutorial, you must satisfy the following requirements. For more information, see the VMware Identity Manager Documentation and VMware Workspace ONE UEM Documentation.

Check that you have the following components installed and configured:

- Windows Pro, Enterprise, or Education device, enrolled in Workspace ONE UEM. For more information, compare Windows 10 editions, or contact a Microsoft representative.
- Two partition minimum
- 350MB boot partition with appropriate format
    - NTFS Mode — Use if booting in legacy BIOS mode
    - FAT32 Mode — Use if booting in UEFI mode
- TPM version 1.2 or later
- Meet Windows system requirements for BitLocker
- Workspace ONE Self-Service Portal URL

For additional assistance and information, see the MS BitLocker FAQ.

Migrate from McAfee Management of Native Encryption (MNE)

Migrating from another BitLocker management provider such as McAfee is straightforward. However, the process changes depending on which protectors you use. Currently, there are two primary use cases:

- Trusted Platform Module (TPM) Only.
- TPM + PIN or Password.

1. Remove McAfee MNE Agent from the System

Remove McAfee MNE agent from the system or configure McAfee policy to set encryption policy to **Report Only** mode (instead of encforce) after the AirWatch Unified Agent for Windows is installed.

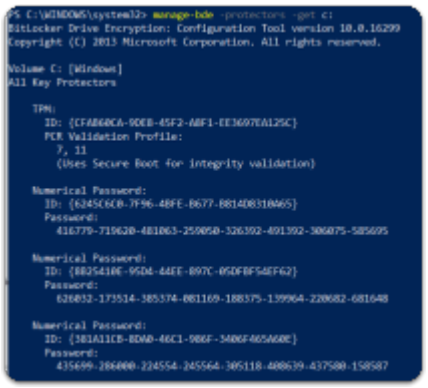
If you are currently only using TPM to store your BitLocker Recovery Key, you ready to Configure the BitLocker Encryption Profile in Workspace ONE UEM.

If you are currently using a PIN or Password in addition to TPN, you are ready to Clear Out Key Protectors.

2. Clear Out Key Protectors (Optional)

If you require a PIN or Password with MNE, use an elevated command prompt to clear out Key Protectors.

2.1. Determine which Key Protectors are in Use



Enter the following command for each encrypted drive letter to see what key protectors are in use.

```
manage-bde -protectors -get c:
```

2.2. Remove Key Protectors

Enter the following command to remove all key protectors.

```
manage-bde protectors delete
```

Alternatively, enter the following command to remove key protectors by type.

```
manage-bde protectors delete C: -type -password
```

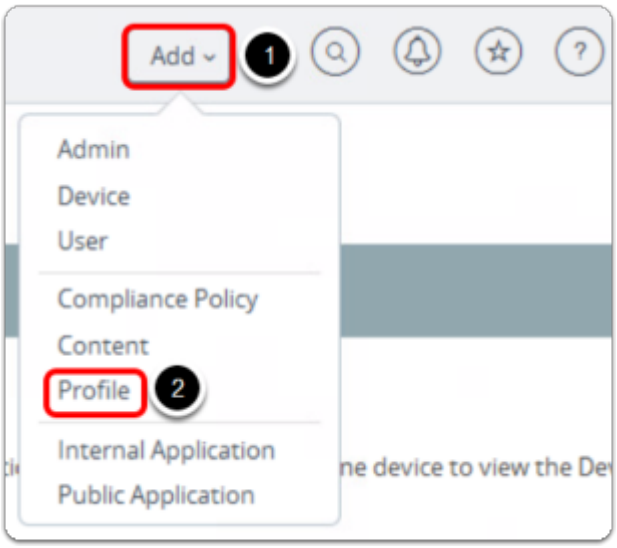
After migrating from McAfee, you are ready to configure the BitLocker Profile for Windows in Workspace ONE UEM.

Configure BitLocker Encryption Profile

Profiles allow you to modify how the enrolled devices behave. This section helps you to configure and deploy Bitlocker encryption using a profile that we will verify applied to the device.

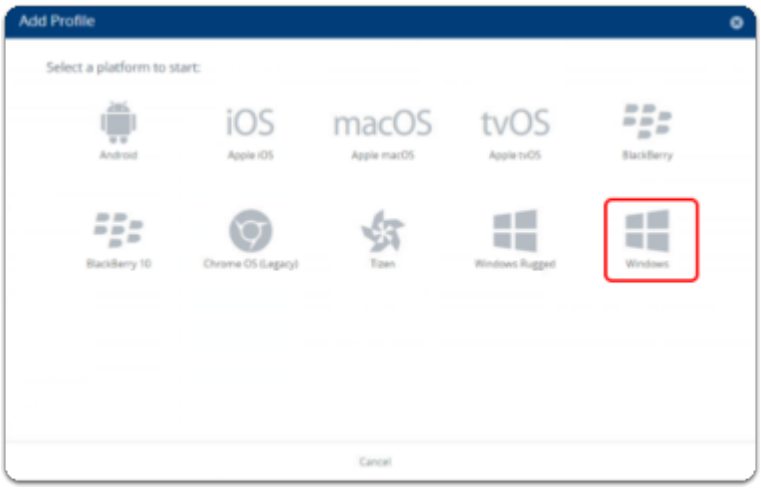
Add a Profile

1. Navigate to Profile Settings



1. In the upper-right corner of Workspace ONE UEM Console, select **Add**.
2. Select **Profile.**

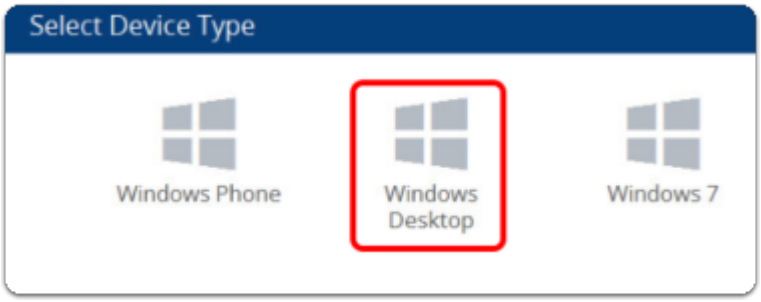
2. Add a Windows Profile



Select the **Windows** icon.

Note: Make sure that you are selecting **Windows** and *not* Windows Rugged.

3. Add a Windows Desktop Profile



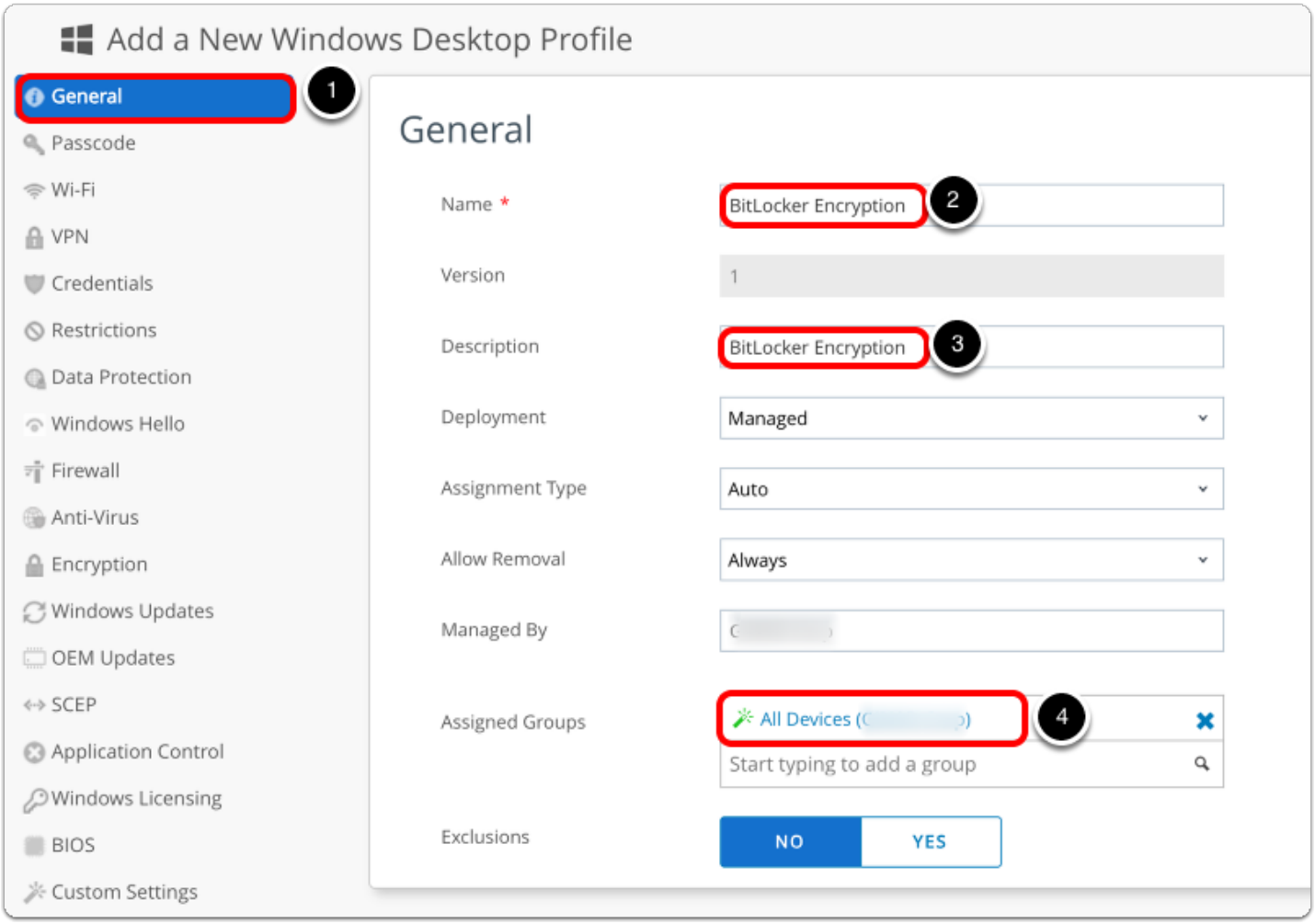
Select **Windows Desktop**.

4. Select Context - Device Profile

Select **Device Profile**.

Configure Profile Settings

1. Define General Settings

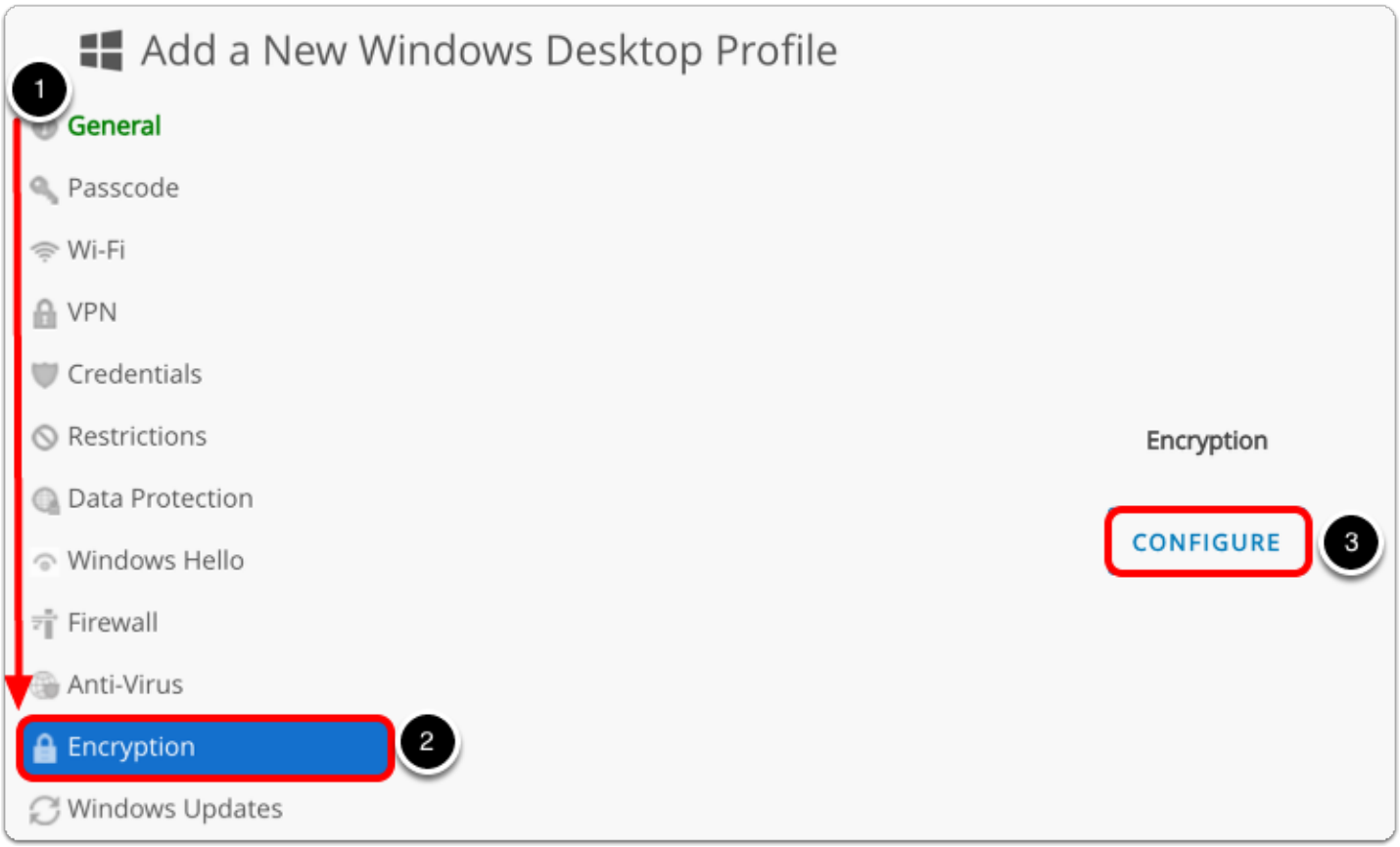


1. Select **General** if it is not already selected.
2. Enter a profile name in the **Name** text box, for example, `BitLocker Encryption`.
3. Copy the profile name into the Description text box.
4. Click in the **Assigned Groups** field. This will pop-up the list of created Assignment Groups. Select the **All Devices** Assignment Group.
   Note: You may need to scroll down to view the Assigned Groups field.

Note: You *do not* need to click **Save & Publish** at this point. This interface allows you to move around to different payload

configuration screens before saving.

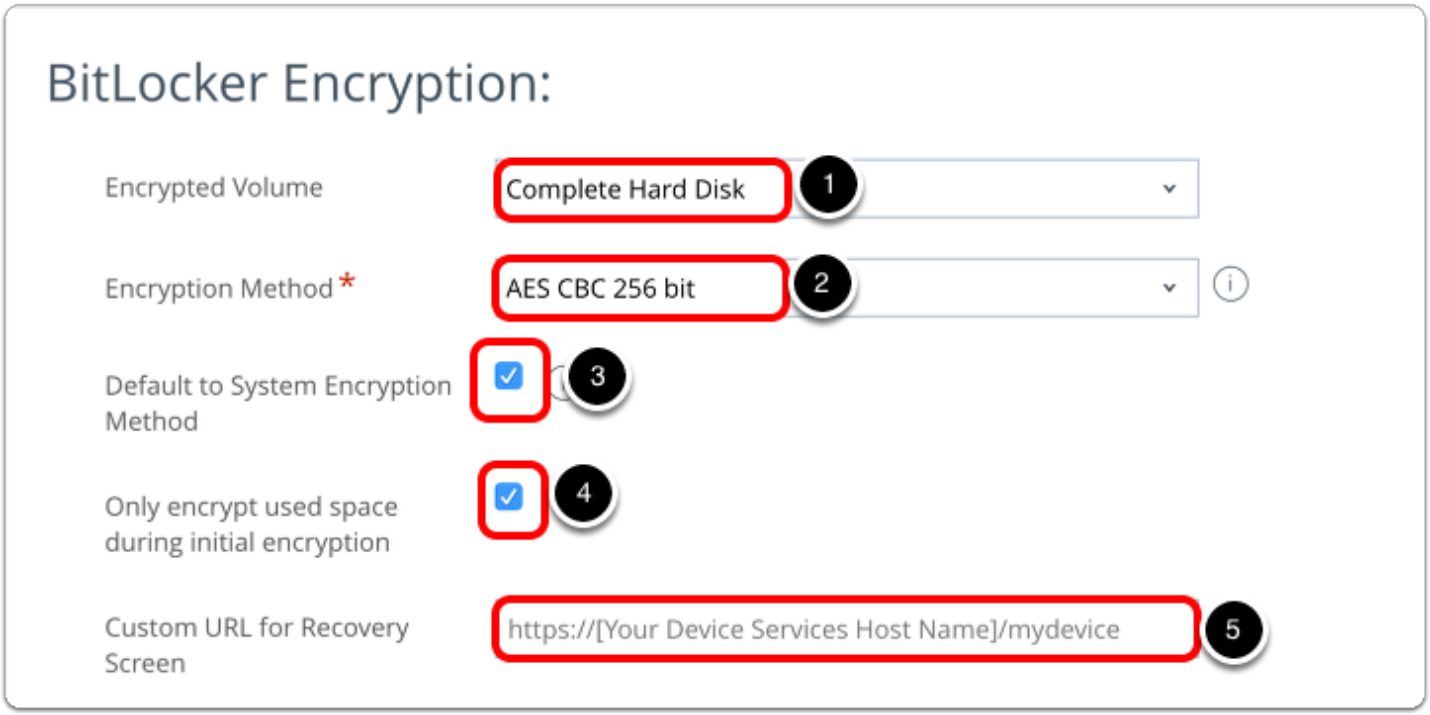
2. Open the Encryption Payload



Note: When initially setting a payload, a Configure button will show to reduce the risk of accidentally setting a payload configuration.

1. Scroll through the payload section on the left until you see the Bitlocker payload.
2. Select the **Encryption** payload.
3. Click the **Configure** button to begin configuring the payload settings.

3. Configure Bitlocker Encryption Settings



1. Select **Complete Hard Disk** from the Encrypted Volume drop-down menu. This encrypts the entire hard disk on the device, including the System Partition where the OS is installed.
2. Select **XTS AES 256 bit** from the Encryption Method drop-down menu.
3. Enable **Default to the System Encryption Method** as a failsafe for devices that do not support the selected encryption method. For example, selecting this setting ensures that Windows 10 1507 and below devices—which do not support XTS encryption—will still get encrypted.
4. Enable **Only Encrypt Used Space During Initial Encryption** to reduce the time required for encryption.

Important: The drive's unused space remains unencrypted, potentially placing confidential data at risk.

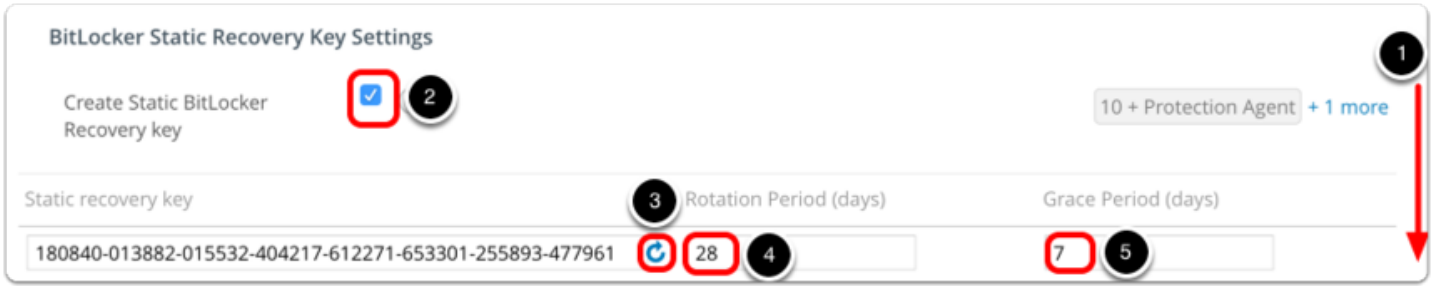
1. Enter the Self-Service Portal URL, `https://[Your Device Services Host Name]/MyDevice` in the Custom URL for Recovery textbox. This URL displays on the lock screen and directs end users to their recovery key.

4. Configure Bitlocker Authentication Settings

1. Using the scroll bar on the right, scroll down to the **BitLocker Authentication Settings** section.
2. Select **TPM** as the Authentication Mode to use the device's Trusted Platform Module to authenticate.
3. Select **Enforce Encryption PIN on Login** to require pre-boot authentication. This locks out the OS at startup and auto-resume, and requires a PIN to unlock devices.
4. Specify the Pin Length to match organizational complexity requirements. For example, enter 8.

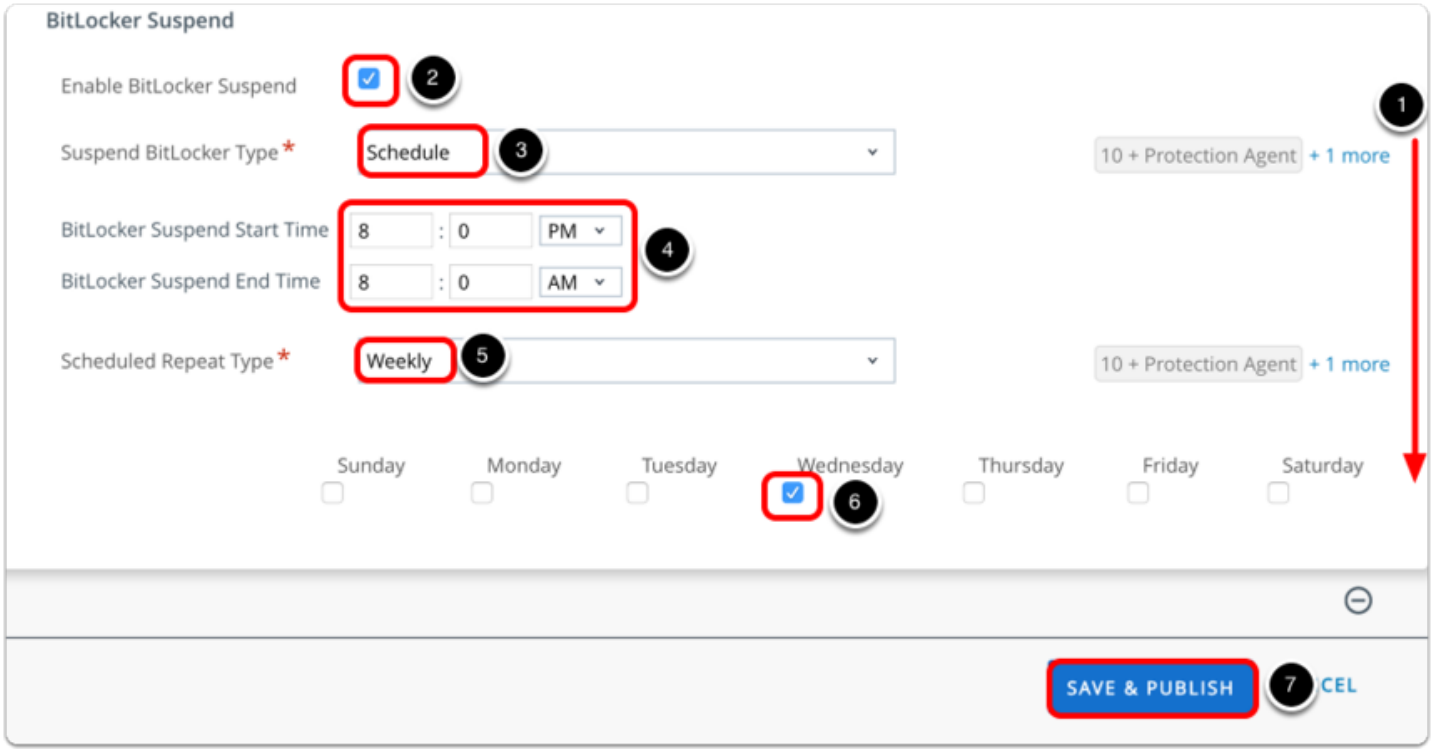
5. Select **Use Password if TPM Not Present** to use a password as a fallback if TPM is unavailable. If deselected, devices that do not have TPM *do not encrypt*.
6. Configure Minimum Password Length to match organizational complexity requirements. For example, enter 8. Settings apply to the *Password Authentication Mode*, and the setting *Use Password if TPM Not Available*.

5. Configure BitLocker Static Recovery Key Settings



1. Using the scroll bar on the right, scroll down to the **BitLocker Static Recovery Key Settings** section.
2. Select **Create Static BitLocker Recovery Key** to create a shared key for a group of devices. This simplifies key recovery for IT personnel who use the shared key to unlock devices.
3. Click the arrow icon to generate a static recovery key.
4. Enter 28 or any value greater than 0 into the **Rotation Period** text box to create a rotation schedule. Enter to opt out of the rotation schedule.
5. Enter 7 into the **Grace Period** text box to specify the number of days after rotation that the previous recovery key still works.

6. Configure BitLocker Suspend



1. Using the scroll bar on the right, scroll down to the **BitLocker Suspend** section.
2. Select **Enable BitLocker Suspend.** This suspends BitLocker encryption during maintenance periods, and allows devices to reboot without end-user interaction. This setting is particularly important for kiosk or shared devices.
3. Select **Schedule f**rom the Suspend BitLocker Type drop-down menu. This suspends BitLocker during a specific time period that repeats daily or weekly.
4. Enter the suspend start and end time.
    - **BitLocker Suspend Start Time** — Set to 8:00 PM
    - **BitLocker Suspend End Time** — Set to 8:00 AM

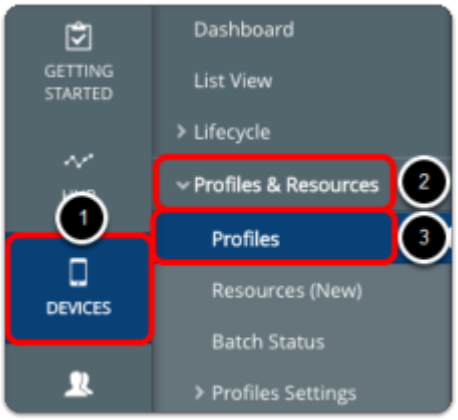
5. Select **Weekly** from the the Scheduled Repeat Type drop-down menu.
6. Select a day of the week to repeat the schedule.
7. Click **Save & Publish.**

7. Publish the BitLocker Encryption Profile

Click **Publish**.

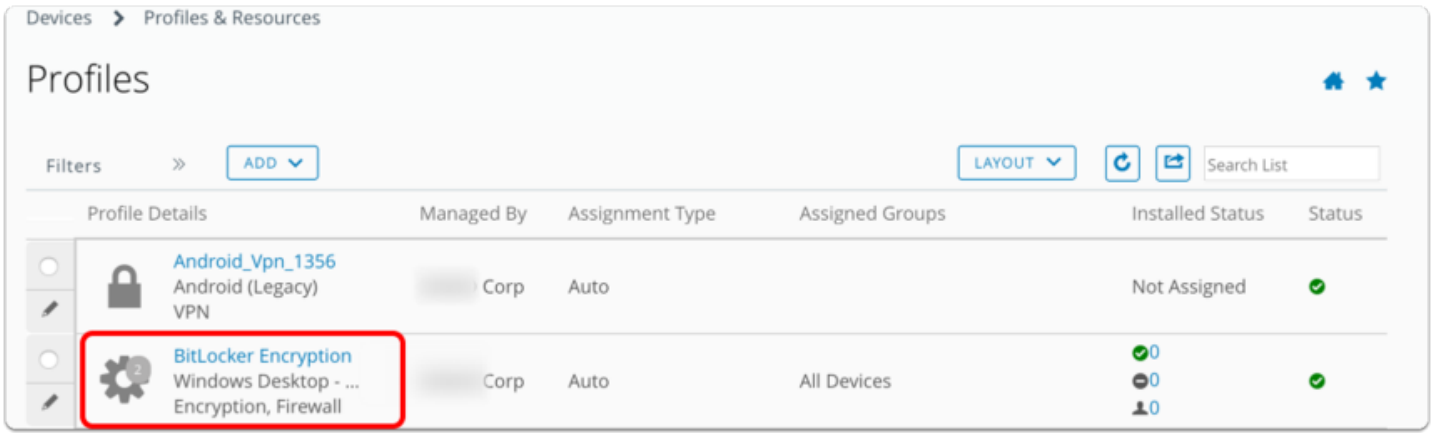
Verify the Profile Exists

1. Navigate to Profiles List View



1. From the left column in the Workspace ONE UEM Console, select **Devices**.
2. Select **Profiles & Resources**.
3. Select **Profiles**.

2. Locate the Profile in the List View

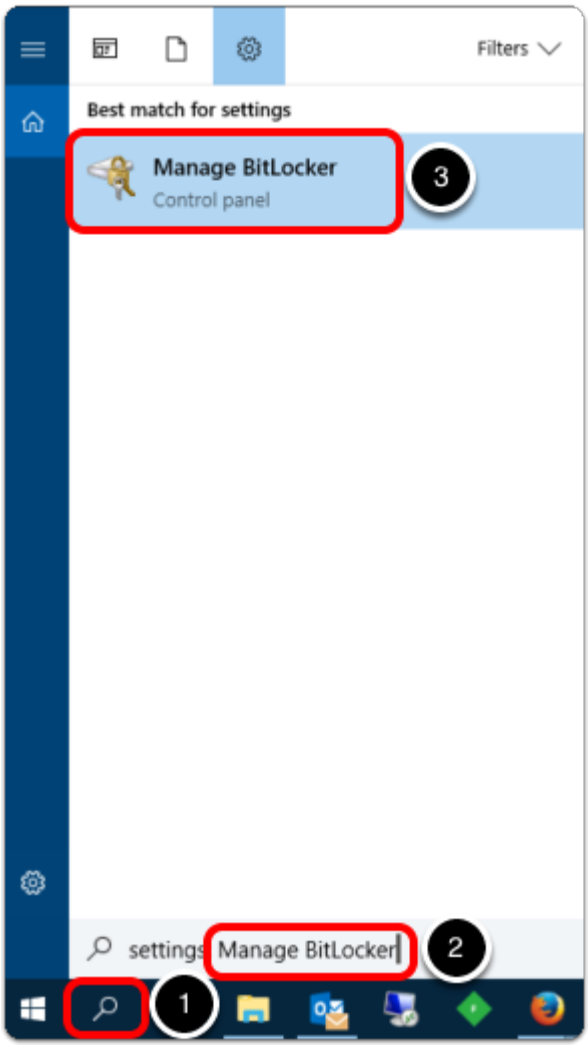


The BitLocker Encryption Profile now appears in the Device Profiles list view.

Verify the Encryption Settings Applied

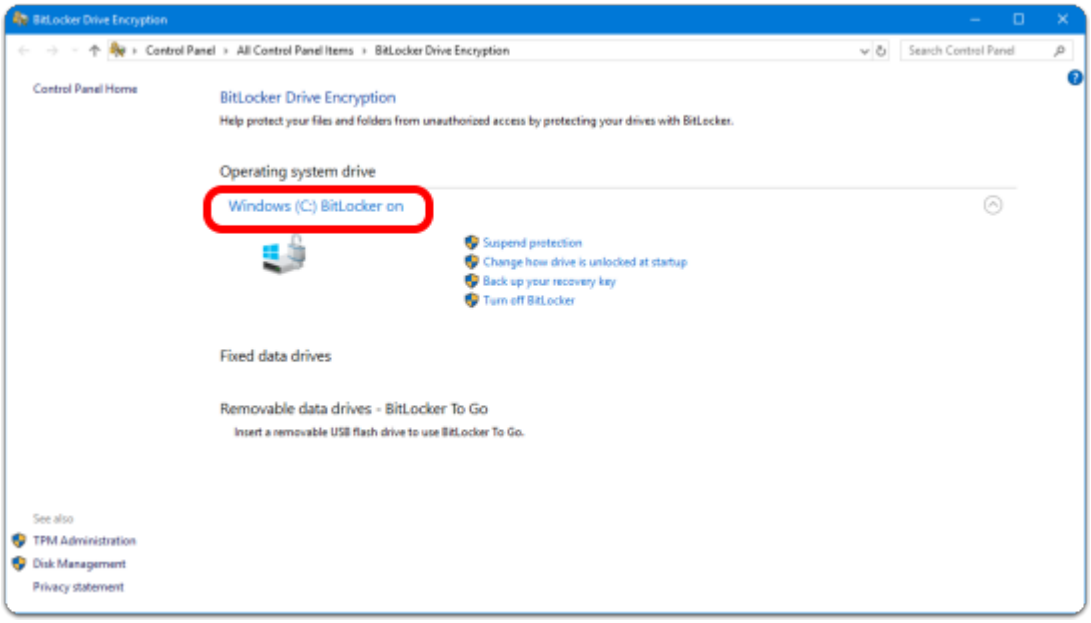
On your Windows 10 device, follow the steps to confirm that the encryption settings are applied.

1. Launch BitLocker Drive Encryption



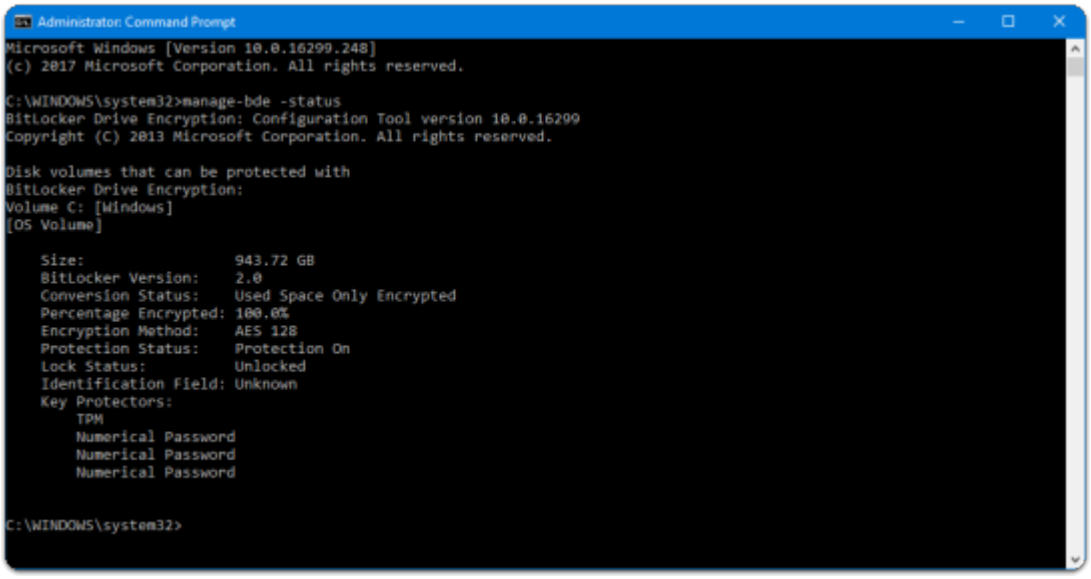
1. Select the search icon.
2. Enter `Manage BitLocker` in the search text box.
3. Select **Manage BitLocker**.

2. Verify BitLocker Encryption is Enabled



Confirm that BitLocker Encryption is on or is still currently encrypting.

3. Confirm Encryption in Elevated Command Prompt (Optional)



For a more detailed view, launch an elevated command prompt and enter `manage-bde -status`.

BitLocker Troubleshooting

This section covers general troubleshooting information for BitLocker migration.

1. BitLocker Drive Preparation Tool

The AirWatch Unified Agent for Windows automatically runs the BitLocker drive preparation tool to ensure the partition requirements are met. You can run this command manually to test if there are compatible partitions. From an elevated command prompt, enter the following command:
`bdehdcfg.exe -driveinfo`

To prepare the drive, run the following commands in an elevated command prompt:

- `bdehdcfg.exe -target c: shrink`
- `Bdehdcfg.exe -target c: merge`
- `Bdehdcfg.exe -target default`

Note: If you manually run these commands, we recommend adding the `-skiphardwaretest` switch so that the system does not require a reboot.

2. Use PowerShell Script to Convert FAT32 to NTFS System Partition

If you have upgraded your Windows 7 systems to Windows 10 and kept them in legacy BIOS mode, the system partition might still be FAT32. You must convert from FAT32 to NTFS for BitLocker to activate.

Note: FAT32 system partition works on Unified Extensible Firmware Interface (UEFI) systems.

To convert, run the following script in PowerShell:

```
 if ($drive = (gwmi win32_volume -Filter "Label = 'System'"))
        {
              Write-Log "Detected a SYSTEM partition...system still in legacy
mode."

             #This finds as available drive letter
              if (!(test-path H:\))
              {
                $driveletter = 'H'
              }
              elseif (!(test-path I:\))
              {
                $driveletter = 'I'
              }
              elseif (!(test-path J:\))
              {
                $driveletter = 'J'
              }
              elseif (!(test-path K:\))
              {
                $driveletter = 'K'
              }
              elseif (!(test-path L:\))
              {
                $driveletter = 'L'
              }

              $newletter = ($driveletter + ":")
              $drive.DriveLetter = "$newletter"
              $drive.Put() #assigning the drive letter
              Write-Log "Attempting to convert system partition to NTFS...reboot
required for changes to take effect."
```

```
            $drive.Label | convert.exe $newletter /FS:NTFS /X #converting
system partition to NTFS
            $drive = (gwmi win32_volume -Filter "Label = 'System'")
            Write-Log "Removing temporary drive letter"
            Get-Volume -Drive $driveletter | Get-Partition | Remove-
PartitionAccessPath -AccessPath "$newletter\" #removing the drive letter so it
doesn't show up in file explorer
           $global:status = 3
       }
```

3. Check Trusted Platform Model (TPM) Health

To check health of TPM on a system, you can launch the TPM snap-in; `tpm.msc`.

Alternatively, run this PowerShell command:
`Get-wmiobject -Namespace ROOT\CIMV2\Security\MicrosoftTpm -Class Win32_Tpm` or
`get-tpm`

4. Export BitLocker Event Viewer Logs

To export BitLocker event viewer logs, enter the following in an elevated command prompt:
`Get-WinEvent -logname 'Microsoft-windows-bitlocker/bitlocker management' -maxevent 30 | export-csv c:\eventviewer.csv`

Summary and Additional Resources

Conclusion

This operational tutorial provided steps to manage the encryption life-cycle for Windows 10 devices using Workspace ONE UEM. Procedures included migrating from McAfee MNE, configuring a BitLocker Encryption profile, and verifying the encryption settings applied.

Terminology Used in This Tutorial

The following terms are used in this tutorial:

application store	A user interface (UI) framework that provides access to a self-service catalog, public examples of which include the Apple App Store, the Google Play Store, and the Microsoft Store.
auto-enrollment	Auto-enrollment simplifies the enrollment process by automatically enrolling registered devices following the Out-of-Box-Experience.
catalog	A user interface (UI) that displays a personalized set of virtual desktops and applications to users and administrators. These resources are available to be launched upon selection.
cloud	Asset of securely accessed, network-based services and applications. A cloud can also host data storage. Clouds can be private or public, as well as hybrid, which is both private and public.
device enrollment	The process of installing the mobile device management agent on an authorized device. This allows access to VMware products with application stores, such as VMware Identity Manager.
identity provider (IdP)	A mechanism used in a single-sign-on (SSO) framework to automatically give a user access to a resource based on their authentication to a different resource.
mobile device management (MDM) agent	Software installed on an authorized device to monitor, manage, and secure end-user access to enterprise resources.
one-touch login	A mechanism that provides single sign-on (SSO) from an authorized device to enterprise resources.
service provider (SP)	A host that offers resources, tools, and applications to users and devices.
virtual desktop	The user interface of a virtual machine that is made available to an end user.
virtual machine	A software-based computer, running an operating system or application environment, that is located in the data center and backed by the resources of a physical computer.

For more information, see the VMware Glossary.

Additional Resources

For more information about Workspace ONE, you can explore the following resources:

- VMware Workspace ONE Action Path
- VMware Workspace ONE product page
- VMware Workspace ONE Documentation
- VMware Identity Manager product page
- VMware Identity Manager Documentation
- VMware Workspace ONE UEM, powered by VMware AirWatch product page
- VMware AirWatch Documentation
- VMware Workspace ONE free trial
- VMware Workspace ONE Cloud-Based Reference Architecture
- VMware Workspace ONE and VMware Horizon 7 Enterprise Edition On-premises Reference Architecture
- VMware End-User-Computing Blogs
- Workspace ONE UEM Hands-On Lab

About the Author

This tutorial was written by:

- Josue Negron, Senior Solutions Architect, End-User-Computing Technical Marketing, VMware

Feedback

The purpose of this tutorial is to assist you. Your feedback is valuable. To comment on this tutorial, contact VMware End-User-Computing Technical Marketing at euc_tech_content_feedback@vmware.com.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com