

# Managing Surface Devices in the Enterprise – BitLocker Management

## Intro to Managing BitLocker on Surface Pro, Surface, and Surface RT Devices

### Surface Pro and Surface

Managing BitLocker on Surface Pro and Surface devices in the enterprise is similar to managing BitLocker on any other Windows 8 or Windows 8.1 Pro or Enterprise device. By taking advantage of the Microsoft Desktop Optimization Pack, IT administrators can easily deploy and monitor BitLocker using the Microsoft BitLocker Administration and Monitoring tool (MBAM). A device can be BitLocker encrypted with the use of Group Policy or with a Configuration Manager task sequence and/or package deployment. Microsoft BitLocker Monitoring and Administration can be set up in a standalone configuration or in an MBAM/Configuration Manager hybrid configuration. The integration of MBAM with Configuration Manager allows IT administrators to use the existing Configuration Manager infrastructure to easily gather compliance data for Surface devices in the enterprise and to deploy BitLocker to newer devices.

Generally, the purpose of using a TPM chip when configuring MBAM drive encryption settings is to handle the keys that unlock the drive and to verify the hardware has not changed. You may have attempted to move a BitLocker encrypted drive to a new machine and noticed that you are still prompted to enter the recovery key when you boot up. This is because the TPM chip is still protecting the data on the drive. Managing pre-boot authentication on Surface Pro and Surface devices is a bit different, because using the TPM plus PIN option does not necessarily make the device more secure. The purpose of enabling a pre-boot PIN is to avoid giving data access to a hacker who connects to your machine via Direct Memory Access or who extracts the memory from your machine to then connect it to a different device to access data. Surface devices, however, do not have any Direct Memory Access ports, and the setup of the hardware makes the memory difficult to remove from the machine. Because of this, enabling TPM plus PIN is not necessary for Surface Pro and Surface devices. However, it can still be enabled via Group Policy. For more detailed information, refer to this blog post:

<http://blogs.technet.com/b/askpfeplat/archive/2014/07/14/bitlocker-pin-on-surface-pro-3-and-other-tablets.aspx>.

### Surface RT

Surface devices running Windows RT offer device encryption, which is based on the same BitLocker drive-encryption technology available in Windows 8 and Windows 8.1 Pro and Enterprise devices. The device encryption feature on Windows RT provides full encryption using AES encryption with 128-bit keys and a TPM protector. Windows RT devices are encrypted automatically upon first startup, but they are not protected with an encryption key until the user provides Microsoft account credentials as an administrator of the device. Once a user provides Microsoft account credentials, the encryption key is *automatically applied and uploaded to the OneDrive associated with the specified Microsoft account*. It is important that an administrative Microsoft account logs on to a Surface running Windows RT at least

once so that the encryption key can be uploaded to OneDrive. To obtain the recovery key, you can go to <https://onedrive.live.com/recoverykey>. For additional information on device encryption specific to Windows RT, go to [https://technet.microsoft.com/en-us/library/dn736041.aspx?f=255&MSPPError=-2147217396#BKMK\\_deviceencryption](https://technet.microsoft.com/en-us/library/dn736041.aspx?f=255&MSPPError=-2147217396#BKMK_deviceencryption).

## Installing and Configuring Microsoft BitLocker Monitoring and Administration

As mentioned earlier in this article, Microsoft BitLocker Monitoring and Administration can be set up in a standalone or Configuration Manager integrated topology. Both topologies have prerequisites for installation, including Group Policy/Active Directory setup. Please look through the following information to set up the necessary prerequisites *before* installing MBAM.

### Standalone Implementation of Microsoft BitLocker Monitoring and Administration

- High-Level Architecture of MBAM 2.5 with Stand-alone Topology  
<https://technet.microsoft.com/en-us/library/dn645312.aspx>
- MBAM 2.5 Installation Prerequisites  
<https://msdn.microsoft.com/en-us/library/dn645331.aspx>
- Planning for MBAM 2.5 Group Policy Requirements  
<https://technet.microsoft.com/en-us/library/dn645338.aspx>
- Planning for MBAM 2.5 Groups and Accounts  
<https://technet.microsoft.com/en-us/library/dn645328.aspx>
- Planning How to Secure the MBAM Websites  
<https://technet.microsoft.com/en-us/library/dn645356.aspx>
- MBAM 2.5 Planning Checklist  
<https://technet.microsoft.com/en-us/library/dn645385.aspx>

### Configuration Manager Integration Implementation

- High-Level Architecture of MBAM 2.5 with Configuration Manager Integration Topology  
<https://technet.microsoft.com/en-us/library/dn656920.aspx>
- MBAM 2.5 Installation Prerequisites  
<https://msdn.microsoft.com/en-us/library/dn645331.aspx>
- MBAM 2.5 Prerequisites Specific to Configuration Manager Integration Topology  
<https://msdn.microsoft.com/en-us/library/dn645334.aspx>
- Planning for MBAM 2.5 Group Policy Requirements  
<https://technet.microsoft.com/en-us/library/dn645338.aspx>

- Planning for MBAM 2.5 Groups and Accounts  
<https://technet.microsoft.com/en-us/library/dn645328.aspx>
- Planning How to Secure the MBAM Websites  
<https://technet.microsoft.com/en-us/library/dn645356.aspx>
- How to Configure the MBAM 2.5 System Center Integration  
<https://msdn.microsoft.com/en-us/library/dn645306.aspx>
- MBAM 2.5 Planning Checklist  
<https://technet.microsoft.com/en-us/library/dn645385.aspx>

Once prerequisites for either stand-alone or Configuration Manager integration topology have been configured, follow the Microsoft BitLocker Administration and Monitoring Deployment Guide (found here: <https://www.microsoft.com/en-us/download/details.aspx?id=38398>) for installation specifics on the server and client side. This document also outlines how to deploy the MBAM 2.5 client via Group Policy and/or Configuration Manager.

## FAQ for Managing BitLocker on Surface Devices

**Q:** I am being prompted for a recovery key on my Surface RT. Where is the recovery key stored?

**A:** The recovery key for a Surface RT device can be obtained at <https://onedrive.live.com/recoverykey>. The key is associated with the Microsoft account that was used to set up the Surface RT. If a Microsoft account is not yet associated with the Surface RT, you will be prompted to enter an email address or phone number where the recovery key can be sent and confirm that you trust the device.

**Q:** How can I get my BitLocker recovery key?

**A:** Depending on how your PC is set up, there are different ways to get your recovery key.

If your PC is connected to a domain

- **Contact your administrator to get your recovery key.**
- **Access a saved copy of the recovery key.** You might have saved a copy of the BitLocker recovery key to a file or a USB flash drive, or printed a hard copy.
  - If you saved the key to a file or printed it, find your copy, follow the instructions on your locked PC, and enter your key when prompted.
  - If you saved the key to a USB flash drive, insert the USB flash drive and follow the instructions on your PC. (If you saved the recovery key as a file on the USB flash drive, you'll need to open the file and manually enter the recovery key.)

- **If your organization has implemented an MBAM self-service portal, you can obtain your key from the portal.**

If your PC isn't connected to a domain, there are several locations where your BitLocker recovery key might have been saved. Here are some places to check:

- **Your Microsoft account online.** This option is available only on PCs that are not joined to a domain. To get your recovery key, go to [BitLocker Recovery Keys](#).
- **A saved copy of the recovery key.** You might have saved a copy of the BitLocker recovery key to a file or a USB flash drive, or printed a hard copy.
  - If you saved the key to a file or printed it, find your copy, follow the instructions on your locked PC, and enter your key when prompted.
  - If you saved the key to a USB flash drive, insert the USB flash drive and follow the instructions on your PC. (If you saved the recovery key as a file on the USB flash drive, you'll need to open the file and manually enter the recovery key.)

**Q:** I do not have a recovery key. What are my other options?

**A:** Unfortunately, if you can't find your key and no other administrator can find a backup copy either, you'll need to restore your Surface to its factory default settings. Choose this option only as a last resort because it will delete your personal data from the Surface. While it helps protect your data against unauthorized access, it also prevents you from ever accessing your data again.

Depending on your Windows configuration, you might be able to restore your Surface to its factory default settings directly from the Windows recovery screen.

If you see a link at the bottom of the recovery screen:

- Select **Learn more about resetting your PC to factory defaults**, and follow the instructions.  
In some Windows configurations, you might need to start the recovery process using a button instead.

If you see buttons at the bottom of the recovery screen:

- Select **Learn more about resetting your PC**, and follow the instructions.  
In other Windows configurations, you might have the option of skipping over certain drives without unlocking them.

If you see an option to skip a drive:

1. Select **Skip this drive** at the bottom of the BitLocker Drive Encryption screen to continue without unlocking the current drive.

If you skip all of the BitLocker-encrypted drives, you'll see a list of advanced repair and startup options to choose from.

2. Select **Repair and Restore > Other repair options > Factory Reset** and follow the instructions.