Microsoft

# Windows: Deploying and Managing BitLocker in the Enterprise

Workshop*PLUS*

*Target Audience:*

*This course is an advanced course for managing BitLocker and is only targeted at IT staff who have designed, deployed, administered and managed Windows Platform or BitLocker encryption or other encryption software.*

*This Premier Workshop is delivered by a Premier Field Engineer. The workshop has a duration of two days at 300 level involving hands-on labs. Participants will learn the internals of BitLocker and how to deploy and manage encrypted volumes.*

## Overview

The Windows Deploying and Managing BitLocker in the Enterprise workshop provides attendees with the deep knowledge and understanding of the implementation, management and troubleshooting techniques needed to manage BitLocker. Through presentations, white-board discussions, and goal-based labs, this two-day workshop covers individual approaches for troubleshooting problems and explores the tools available to monitor, trace and identify the root cause of the issues.

We start by explaining the aspects of BitLocker; from the small, hidden partition at the start of a boot disk, to the integration with Active Directory, to installing an OS on an encrypted disk, to recovering encrypted disks and finally creating a scalable, manageable platform which is enterprise-ready to store the keys using Microsoft BitLocker Administration and Monitoring (MBAM).

## Key Features and Benefits

Data-loss is an ever-growing problem and the consequences of it are numerous and increasing in severity. Being affected by data-loss is becoming a case of “when”, not “if”, sensitive business or personal data is lost. This WorkshopPLUS helps IT pros encrypt their disks, protect their data and keep the encryption keys accessible in a managed way.

## Technical Highlights

After completing this course, you will be able to:

- Understand how BitLocker works
- Understand the tools that can help deploy BitLocker.
- Understand how to approach different troubleshooting scenarios.
- Identify action plans to troubleshoot different components and areas of BitLocker encrypted environments.

*Hardware Requirements:*

*Labs are hosted on Labs on Demand internet platform. Participants need access to the Internet for entire length of the course. For best experience it is recommended to use 2 monitors during using this platform.*

*If no Internet connectivity is possible, participants can use labs hosted locally on premise. In this case notice should be given during scoping and hardware requirements are provided below:*

*Computer running at least Windows 10 or Windows Server 2016 with support for virtualization with 250 GB free drive space, minimum 4GB of RAM (8 GB Recommended).*

*Microsoft Office 2016 or PDF reader needs to be installed.*

# Syllabus

This workshop runs for two full days. Students should anticipate consistent start and end times for each day. Early departure on any day is not recommended.

Module 1: BitLocker Fundamentals: BitLocker Overview and Requirements, TPM (Trusted Platform Module), Protectors, Recovery Method, What's New in Windows 8/10, Security Considerations

Module 2: BitLocker Internals: PCRs (Platform Configuration Registers), Encryption algorithms , Page File and BitLocker, FVE Kernel driver, Decommissioning Old HDD, FIPS compliance

Module 3: BitLocker To Go: What Is BitLocker To Go, BitLocker To Go Requirements, How the BitLocker To Go Reader Works, BitLocker To Go controls

Module 4: Integration with Active Directory and Azure: Storing Recovery Password in Active Directory, Storing TPM Owner Password in Active Directory, Security of BitLocker Information in AD, BitLocker in Azure

Module 5: Branch Offices and Slates: Why BitLocker in the Branch Office, RODC in the Branch Office, BitLocker on Tablets and Mobile Phones

Module 6: Performance Analysis: Hardware Performance, Measuring Performance, Performance Comparison

Module 7: Troubleshooting: BitLocker Logs, Recovery Prompts, TPM Measurements, TPM lockout, DaRT toolset

Module 8: MBAM: **MBAM Fundamentals,** MBAM Agent and Group Policies, MBAM server components, Architecture, MBAM Help Desk and Self Service Portal, Planning for MBAM High Availability, MBAM Security Considerations, Best Practices, Troubleshooting

Module 9: Deployment: Enabling the TPM, BitLocker Deployment Options, TPM AutoProvisioning, MDT and SCCM deployment examples

Microsoft

This data sheet is for informational purposes only.
MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY