Microsoft Security

BITLOCK: Planning and Deploying BitLocker Drive Encryption Training

$1,595.00

- 2 Days
- Helps achieve HIPAA compliance with laptops
- Includes "BitLocker to Go" for USB
- Helps achieve GDPR compliance
- Exclusive course - taught by Mike Danseglio, creator of BitLocker!

Upcoming Dates

Jan 08 - Jan 09
Mar 05 - Mar 06

Course Description

This 2-day instructor-led BitLocker training course teaches you everything you need to know about BitLocker. This course includes hands-on labs. These labs reinforce and expand on the instructor-led portion by having you actually deploy and operate BitLocker. You'll practice techniques for setting up a BitLocker-enabled environment, implementing BitLocker on multiple system configurations, and recovering BitLocker after the detection of a possible compromise.

Data security is an increasingly critical part of IT. More and more organizations require data encryption in order to meet regulatory security requirements. BitLocker Drive Encryption is a popular choice to meet these requirements. BitLocker is a highly effective and low-cost data encryption technology that's built into Windows. But because of this strong protection, your organization must understand and carefully plan for BitLocker deployment to avoid data loss and system downtime.

Although the labs focus primarily on Windows 10 and Windows Server 2012, the class also applies to Windows 7, Windows 8, Windows Server 2008, and Windows Server 2016.

Course Outline

Understanding and Analyzing BitLocker

Analyzing BitLocker

- Context and background
- Understanding BitLocker
- Understanding BitLocker to Go
- Cryptography
- Trusted Platform Module (TPM)

Understanding BitLocker

- Pre-Boot Authentication
- System Tamper Detection\
- System Integrity Verification
- Network Unlock

- Encrypted Drive Support

BitLocker Architecture

- BitLocker Initialization
- BitLocker Operation
- BitLocker Suspend and Resume
- BitLocker to Go Architecture

Planning for BitLocker Deployment and Support

Planning BitLocker Deployment

- Prerequisites
- Examining Hardware Capabilities
- Planning Configuration Options
- Planning Recovery Options

IT Planning

- Planning User Interaction Scenarios
- Planning Recovery Key Access and Use
- Planning BitLocker Deployment Through System Center Configuration Manager (SCCM)
- Planning BitLocker Deployment Through Microsoft Deployment Toolkit (MDT)
- Planning BitLocker Deployment Through Microsoft Baseline Administration and Monitoring (MBAM) and Microsoft Desktop Optimization Pack (MDOP)

User Planning

- Identifying BitLocker Users and Devices
- Educating BitLocker Users

Deploying BitLocker

Single Standalone Device

- Configuring BitLocker Options
- Enabling BitLocker
- Encrypting the Drive
- Verifying BitLocker Operation

Single Domain-Joined Device

- Configuring BitLocker Options
- Enabling BitLocker
- Encrypting the Drive
- Verifying BitLocker Operation

Multiple Devices

- Deploying BitLocker Through Group Policy
- Deploying BitLocker Through PowerShell
- Deploying BitLocker Through SCCM, Altiris, and MBAM

Troubleshooting BitLocker Deployment and Operational Issues

Troubleshooting BitLocker

- Normal BitLocker Use
- Suspending and Resuming BitLocker
- BitLocker Recovery Mode
- Recovering BitLocker Devices
- Preventing BitLocker Recovery Mode
- Managing the Trusted Platform Module (TPM)

Audience

Anyone involved in planning, deploying, or supporting BitLocker. This includes CISOs, IT architects, system administrators, server administrators, disaffected college students, and technical support engineers.

Prerequisites

A strong understanding of Windows deployment and management in an enterprise environment is required. Familiarity with cryptography and data storage technology is highly recommended.

What You Will Learn

After completing this course, student will understand how to:

- Plan for BitLocker deployment for both new and existing computers
- Create a recovery plan for lost encryption keys
- Identify computers that meet BitLocker hardware security requirements
- Determine optimal settings for encryption and data recovery
- Choose a strategy that minimizes BitLocker Recovery events
- Select and implement a BitLocker deployment method
- Implement an organization-wide or limited-scope BitLocker deployment
- Plan BitLocker integration with Microsoft System Center Configuration Manager (SCCM), Active Directory Domain Services, and Microsoft BitLocker Administration and Monitoring (MBAM)
- Support BitLocker systems in the field with minimal downtime