# Microsoft® Official Course

Module 2

## Troubleshooting Startup Issues

Microsoft®

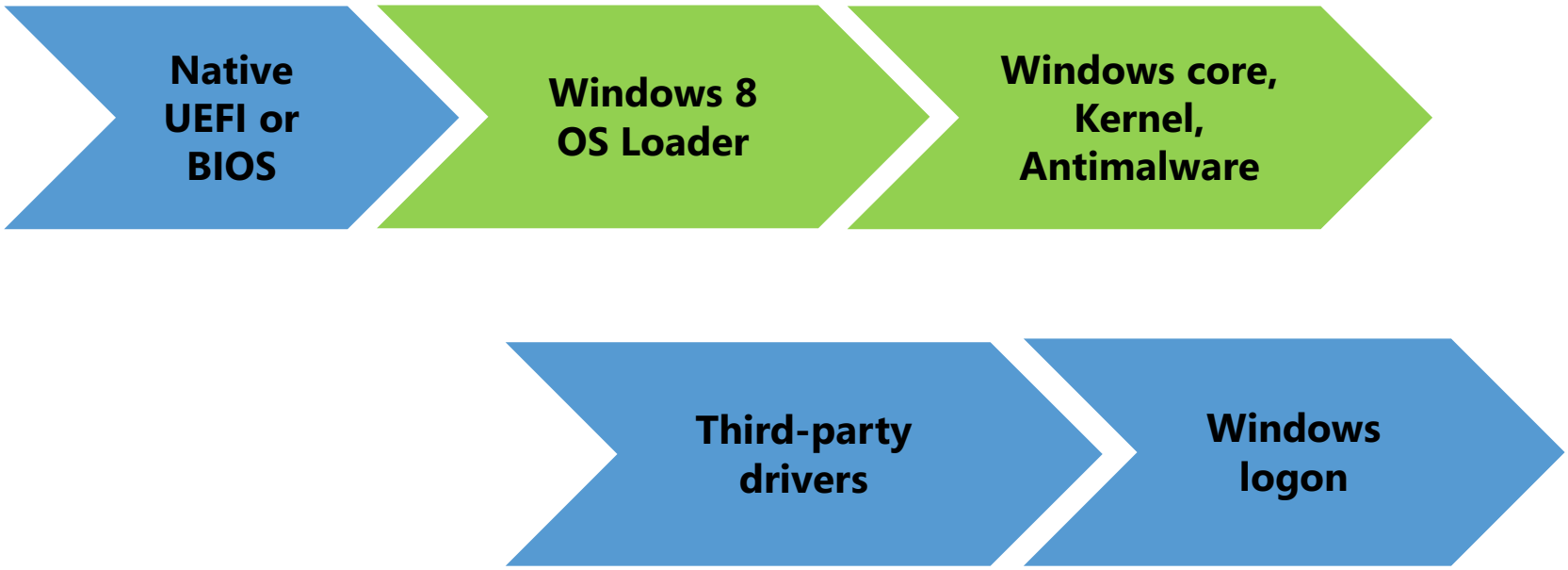
# Module Overview

- Overview of the Windows 8.1 Startup Recovery Environment
- Troubleshooting Startup Settings
- Troubleshooting Operating System Services Issues
- Recovering BitLocker-Protected Drives3

# Lesson 1: Overview of the Windows 8.1 Startup Recovery Environment

- Windows 8.1 Startup Architecture
- Windows Startup Recovery Options
- Recovery Tools Available in Windows RE
- Demonstration: Examining the Advanced Startup Environment
- System Restore
- Demonstration: Accessing System Restore

# Windows 8.1 Startup Architecture



# Windows Startup Recovery Options

Windows 8.1 provides a number of start-up recovery tools:

- Windows RE
- Automatic failover to startup recovery
- Advanced start-up settings

# Recovery Tools Available in Windows RE

- Windows RE provides access to six recovery tools:
  - Refresh your PC
  - Reset your PC
  - System Restore
  - System Image Recovery
  - Startup Repair
  - Command Prompt
- Use Startup Repair first, then try System Restore before attempting any of the more invasive recovery tools listed

# Demonstration: Examining the Advanced Startup Environment

In this practice session, you will:

- Launch Windows RE
- Use the Command Prompt tool
- Use Startup Repair
- Start Windows 8.1 normally
- Examine a Startup Repair log file

# System Restore

- System Restore takes snapshots of your computer system, and then saves them as restore points
- You can use System Restore to:
  - Perform driver rollback
  - Protect against accidental program deletion
  - Roll back the computer's entire configuration

# Demonstration: Accessing System Restore

In this practice session, you will:

- Create a restore point
- Start a computer in Windows RE
- Launch System Restore

# Lesson 2: Troubleshooting Startup Settings

- Windows 8.1 BCD Store
- Configuring the BCD Configuration Settings
- Demonstration: Using Command-Line Tools to Access the BCD Store
- Configuring Environments with the System Configuration Tool
- Advanced Startup Options in Windows 8.1
- Demonstration: Using System Configuration and Advanced Startup Options

# Windows 8.1 BCD Store

- The BCD store is stored as a registry hive
- For BIOS-based systems, the BCD registry file is located in the active partition\Boot directory
- The BCD store is an extensible database of objects and elements that can include information about:
  - The hibernation image
  - Windows 8.1 startup options
  - Alternate start-up options for Windows operating systems

# Configuring the BCD Configuration Settings

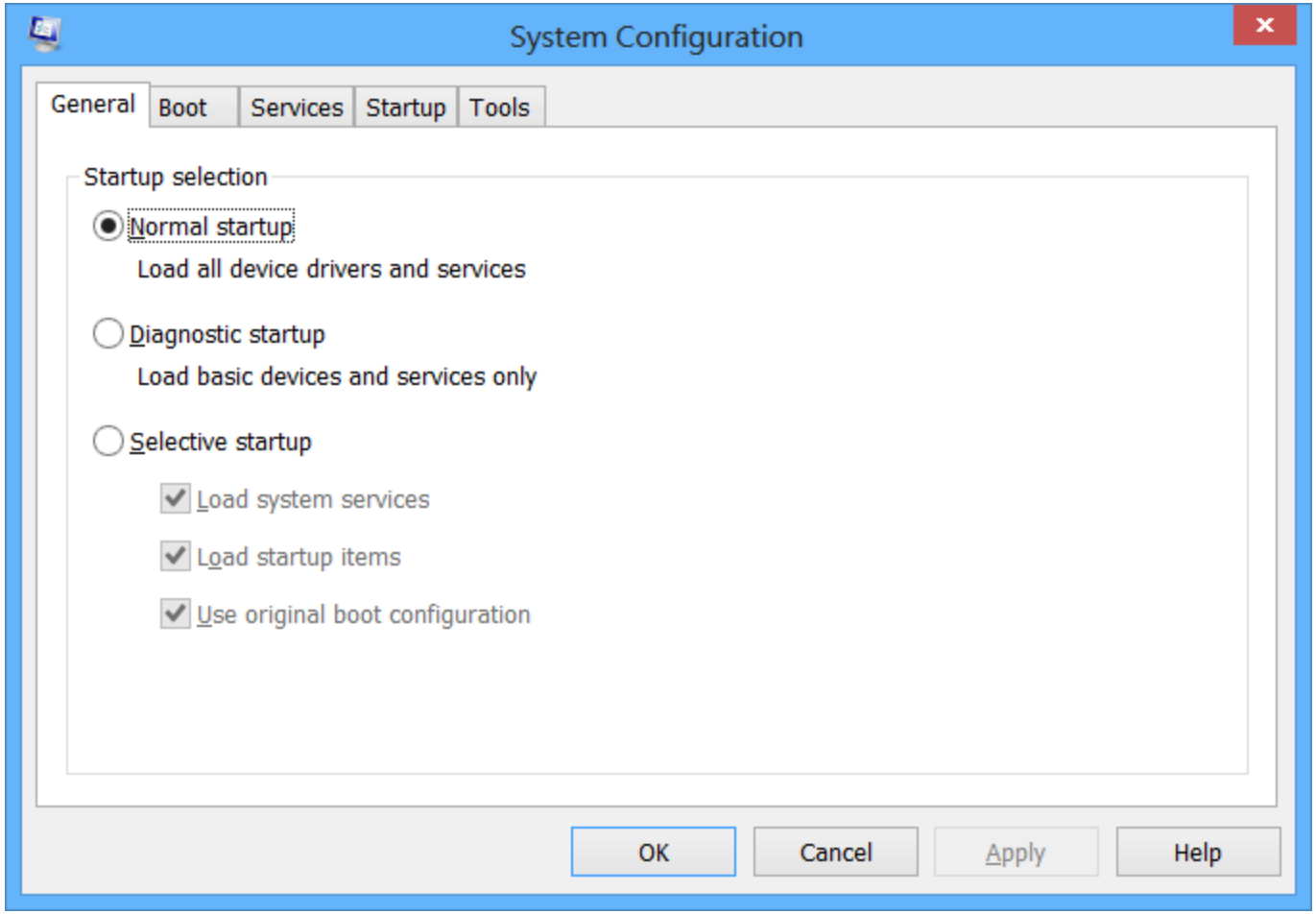
- Use the BCDEdit command-line tool to make changes to the BCD store, such as removing entries from the list of displayed Windows operating systems
- You can use the other following tools to modify the BCD:
  - Startup and recovery
  - Msconfig.exe
  - BootRec.exe

# Demonstration: Using Command-Line Tools to Access the BCD Store

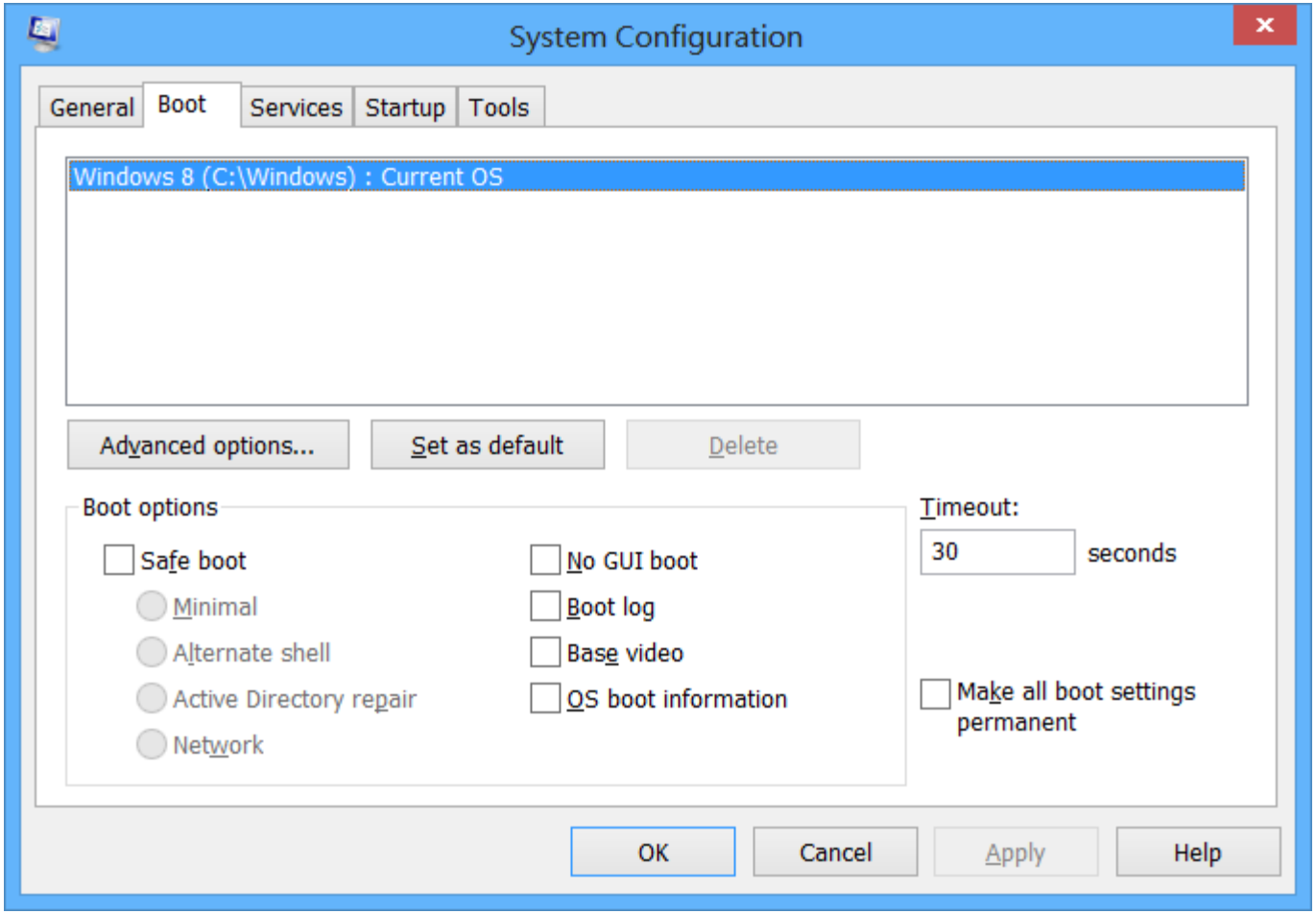
In this practice session, you will:

- Access advanced startup options
- Open the Command Prompt tool
- Work with the boot store
- Restart the Windows operating system normally

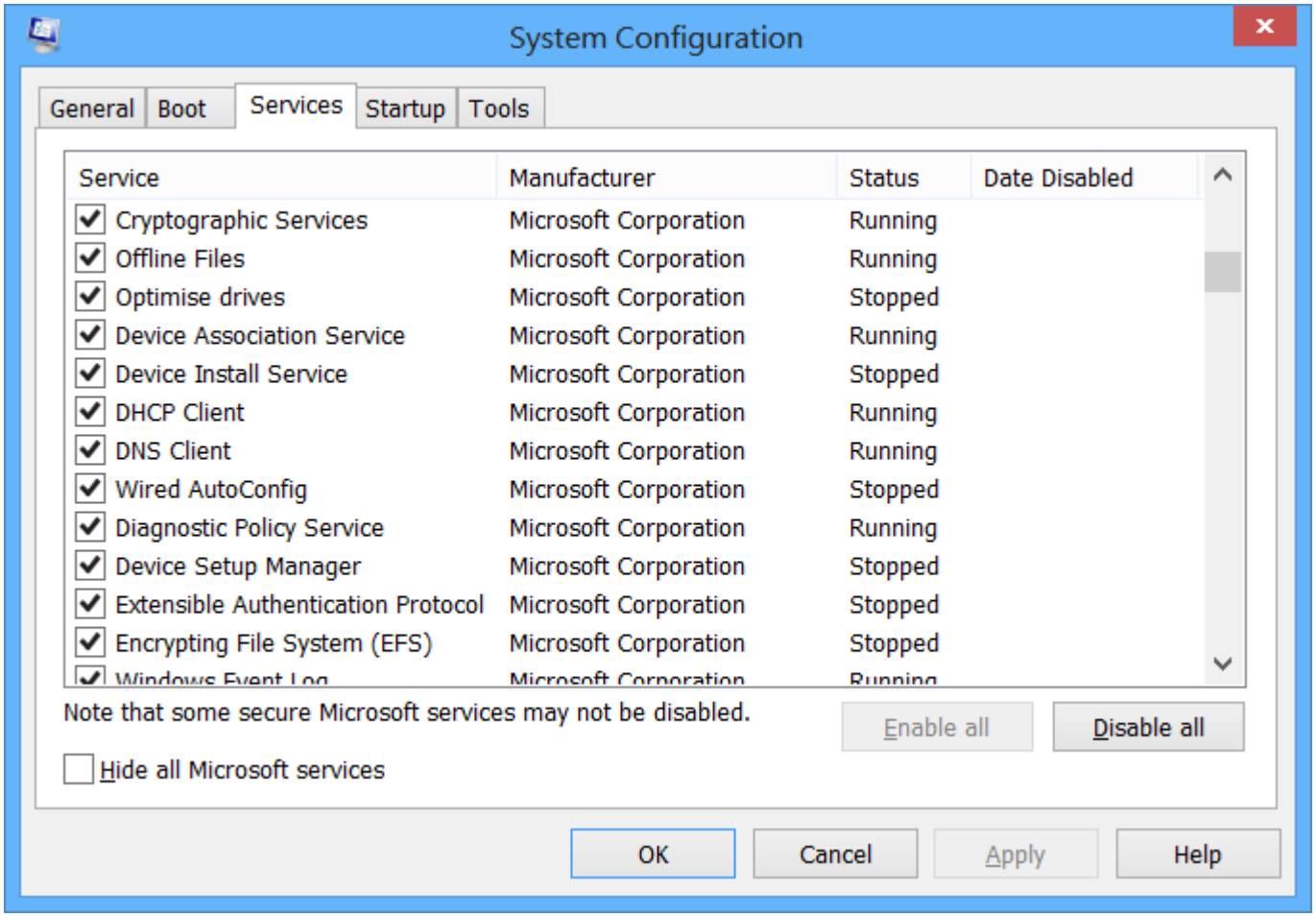
# Configuring Environments with the System Configuration Tool



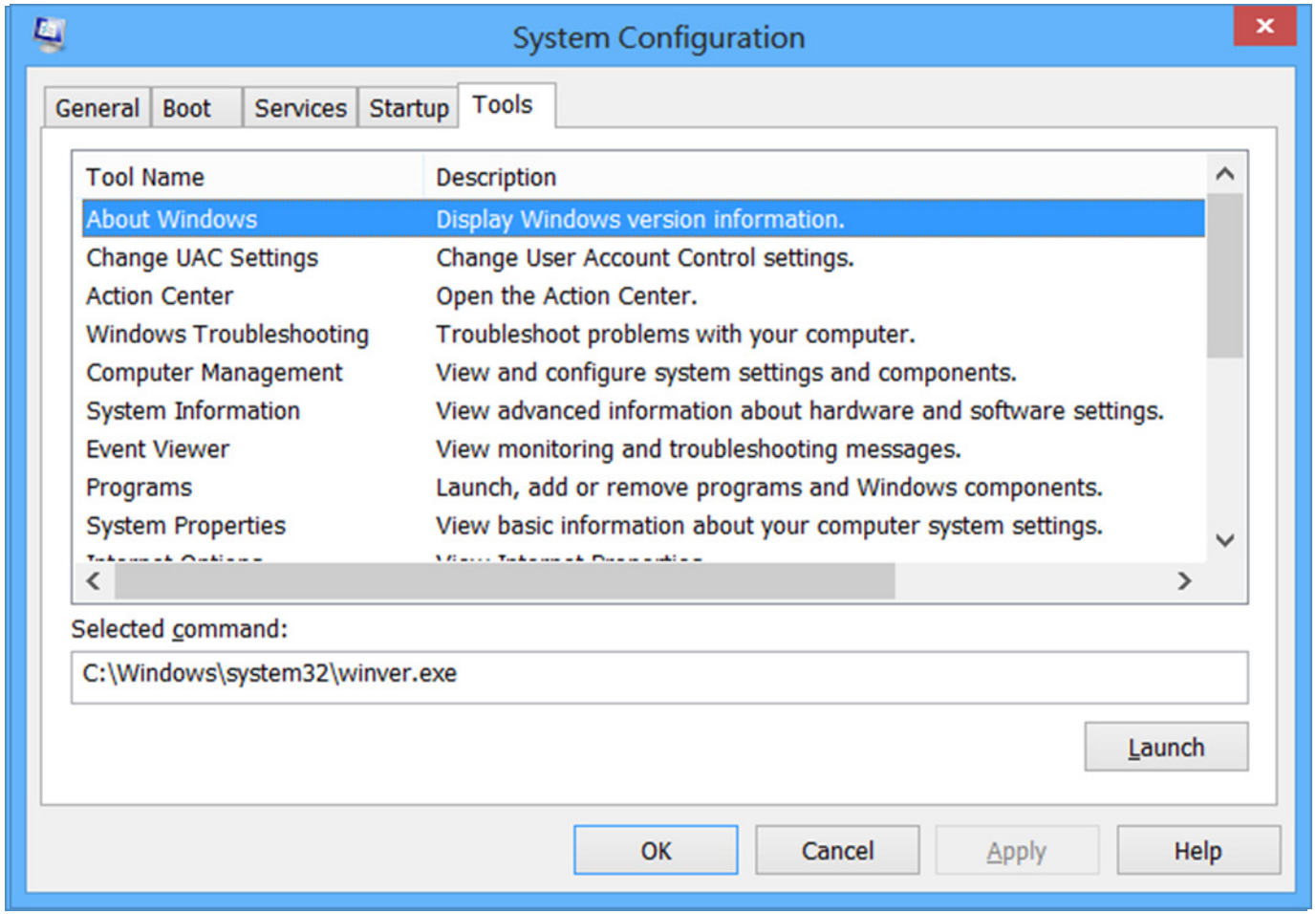
# Configuring Environments with the System Configuration Tool



# Configuring Environments with the System Configuration Tool



# Configuring Environments with the System Configuration Tool



# Advanced Startup Options in Windows 8.1

Windows 8.1 provides the following advanced startup options:

- Enable debugging
- Enable boot logging
- Enable low-resolution video
- Enable safe mode
- Enable safe mode with networking
- Enable safe mode with command prompt
- Disable driver signature enforcement
- Disable early launch anti-malware protection
- Disable automatic restart after failure

# Demonstration: Using System Configuration and Advanced Startup Options

In this practice session, you will:

- Load  the System Configuration tool
- Enable Safe boot, and then restart
- Sign in to safe mode
- Revert to normal start-up
- Access start-up settings

# Lesson 3: Troubleshooting Operating System Services Issues

- Operating System Services
- Identifying Failed Services
- Disabling Services

# Operating System Services

System services:

- Load and run in the background without user intervention
- Support application requests. For example, when an application needs to open a file, it relies on a system service to retrieve that file from the disk
- Can make calls to device drivers when a request is sent to a physical device

# Identifying Failed Services

Windows 8.1 provides a number of ways of locating service-related problems:

- Event Viewer
- Log files
- Stop codes
- Action Center

# Disabling Services

Depending on the circumstances, you can disable a service in one of the following ways:

- Safe mode
- Command prompt
- System Configuration Utility

# Lab A: Troubleshooting Startup Issues

- Exercise 1: Resolving a Startup Problem (1)
- Exercise 2: Resolving a Startup Problem (2)

Logon Information

| | |
|---|---|
| Virtual machines**:** | 20688D-LON-DC1<br>20688D-LON-CL1 |
| User name: | **Adatum\Administrator** |
| Password: | **Pa$$w0rd** |

Estimated Time: 45 minutes

# Lab Scenario

A number of users have reported startup problems to the help desk. You must investigate these problems and attempt resolutions.

# Lab Review

- What was your approach to the first scenario? How did your approach differ from the class?
- What was your approach to the second scenario? How did your approach differ from the class?

# Lesson 4: Recovering BitLocker-Protected Drives

- Overview of BitLocker
- BitLocker and TPMs
- Recovering a BitLocker-Encrypted Drive
- Demonstration: Encrypting a Partition by Using BitLocker
- BitLocker To Go

# Overview of BitLocker

Windows BitLocker Drive Encryption encrypts the computer's operating system and data that is stored on the operating system volume

- Provides offline data protection
- Protects all other applications installed on the encrypted volume
- Includes system integrity verification
- Verifies integrity of early boot components and boot configuration data
- Ensures the integrity of the startup process

# BitLocker and TPMs

BitLocker uses the TPM to verify the integrity of the startup process by:

- Providing a method to verify that early boot file integrity has been maintained
- Enhancing protection to mitigate offline software-based attacks
- Locking the system when it is tampered with

# Recovering a BitLocker-Encrypted Drive

**When a BitLocker-enabled computer starts:**

- BitLocker checks the operating system for conditions indicating a security risk
- If a condition is detected:
  - BitLocker enters recovery mode and keeps the system drive locked
  - The user must enter the correct recovery password to continue

**The BitLocker recovery password is:**

- A 48-digit password used to unlock a system in recovery mode
- Unique to a particular BitLocker encryption
- Can be stored in AD DS
- If in AD DS, search for it by using either the drive label or the computer's password

# Demonstration: Encrypting a Partition by Using BitLocker

In this practice session, you will:

- Configure required GPO settings
- Enable BitLocker
- Complete the process for configuring BitLocker

# BitLocker To Go

Provides enhanced protection against data theft and exposure by extending BitLocker to removable storage devices

When securing a removable drive, you can choose to unlock the drive with either:

- A password
- A smart card

# Lab B: Recovering BitLocker-Encrypted Drives

- Exercise 1: Recovering a BitLocker-Encrypted Drive
- Exercise 2: Creating a New BitLocker Password

Logon Information

| | |
|---|---|
| Virtual machines: | 20688D-LON-DC1<br>20688D-LON-CL1 |
| User name: | **Adatum\Administrator** |
| Password: | **Pa$$w0rd** |

Estimated Time: 25 minutes

# Lab Scenario

A user contacts the help desk explaining that he cannot start his computer. You identify the problem as relating to BitLocker. You must visit the user's computer and attempt to recover the hard drive so that the user can start his computer. After recovery, you must provide new BitLocker keys and passwords.

# Lab Review

- What was your approach to the first scenario? How did your approach differ from the class?

# Module Review and Takeaways

- Review Questions