

# Module 15

Troubleshooting Software

# Objectives

---

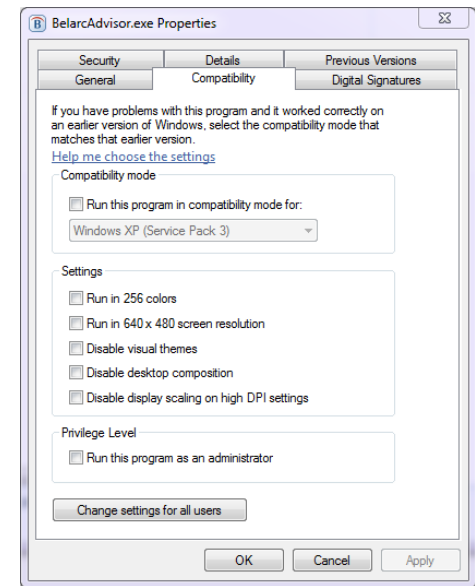
1. 4.6 Troubleshooting Software
2. 4.7 Troubleshooting Security

---

# **TROUBLESHOOTING SOFTWARE**

# Troubleshooting Legacy Software Installation

1. Check Microsoft's web site for updates to Windows or a Microsoft application
2. Check software manufacturer's Web site for updates or suggestions
3. Consider upgrading software
4. Use Windows Compatibility Mode utility to provide an application with the environment it expects from the OS it was designed for



Program Properties

# Blue Screen Of Death (BSOD)

1. Also known as STOP Error or visual fault error
2. Displayed by the operating system upon encountering a critical error that causes the system to crash
3. Can be related to hardware, updates and drivers, causing the computer to stop responding in order to prevent damage to the hardware or data.
4. Not enough free space available on the primary partition
5. The screen presents information for diagnostic purposes
6. Solutions:
  - A. Undo your last procedure
  - B. Free up space on the primary partition
  - C. Undo driver updates and check for new updates
  - D. Scan for viruses
  - E. Apply or remove recent Windows Updates
  - F. Check the System and Application logs in Event Viewer
  - G. Perform diagnostic tests on all hardware

```
***STOP: 0x000000D1 (0x00000000, 0xF73120AE, 0xC0000008, 0xC0000000)
A problem has been detected and Windows has been shut down to prevent damage
to your computer.
DRIVER_IRQL_NOT_LESS_OR_EQUAL
If this is the first time you've seen this Stop error screen, restart your
computer. If this screen appears again, follow these steps:
Check to make sure any new hardware or software is properly installed. If this is a
new installation, ask your hardware or software manufacturer for any Windows updates
you might need.
If problems continue, disable or remove any newly installed hardware or software.
Disable BIOS memory options such as caching or shadowing. If you need to use Safe
Mode to remove or disable components, restart your computer, press F8 to select
Advanced Startup Options, and then select Safe Mode.
*** WXYZ.SYS - Address F73120AE base at C0000000, DateStamp 36b072a3
Kernel Debugger Using: COM2 (Port 0x2f8, Baud Rate 19200)
Beginning dump of physical memory
Physical memory dump complete. Contact your system administrator or
technical support group.
```

Visual Fault Error

# OS Problems

---

- 1. Improper Shutdown** - Can cause some harmful effects for your OS and software
  - Only use when no other option is available
- 2. Spontaneous Shutdown/Restart** – Usually caused by overheating issues or driver issues
- 3. Slow System Performance** – Caused by too little RAM or virtual memory

# Startup Problems

---

- 1. RAID not Detected During Startup** – RAID controller or drive not configured
  - Power on the device at least 15 second before start the computer
- 2. Missing DLL Message** – Causes: a damaged hal.dll file, a damaged or missing boot.ini file, or a physically damaged hard drive
- 3. Services Fail to Start** – Causes: child service not started, authentication error
- 4. Boots to Safe Mode** – Boot option set incorrectly, registry errors
- 5. Failure to Boot** – Missing boot.ini or other startup file
- 6. Missing NTLDR or Boot.ini** – Repair using the Recovery Console
- 7. Invalid Boot Disk** – Causes include: virus, drive marked as inactive
- 8. Missing OS** – Change boot order, run recovery disk, repair MBR
- 9. Missing GUI** – Missing file, turned off, registry error

# Tools and Recovery Console Options

---

1. Bootrec.exe /fixmbr, /fixboot, /rebuildbcd
2. SFC
3. Repair Disks
4. Msconfig
5. Defrag
6. Regsrv32
7. Regedit
8. Event Viewer
9. Safe Mode
10. Command Prompt
11. Emergency Repair Disk
12. ASR



---

# **TROUBLESHOOTING SECURITY**

# Security Issues

---

1. Pop-ups
2. Browser Redirection
3. Security Alerts
4. Slow Performance
5. PC Locks up
6. Windows Update Failure
7. Rogue Antivirus
8. Spam
9. Renamed System Files
10. Files Disappearing
11. File Permission Changes
12. Hi-Jacked email
13. Access Denied

# Tools

---

1. Antivirus
2. Anti-malware
3. Anti-Spyware
4. Recovery Console
5. System Restore
6. Event Viewer
7. Administrator access and tools

# Security Removal Techniques

---

1. Schedule frequent scans and updates
2. Identify Malware Symptoms
3. Quarantine infected system
4. Enable system restore
5. Create Restore point
6. Educate end user

# Summary

---

In this module we discussed:

1. Legacy Software troubleshooting
2. Visual Fault Errors
3. OS troubleshooting and tools
4. Startup troubleshooting
5. Security troubleshooting and tools
6. Removal techniques