(https://www.crowdstrike.com/)

BitLocker recovery in Microsoft environment…

Solution: Sensors - Windows OS Platforms | Cloud Security Modules (CSPM & CWP)

Published Date: Jul 19, 2024

Objective

- BitLocker recovery in Microsoft environments using ManageEngine Desktop Central

Applies To

- Supported versions of the Falcons sensor for Windows
- Supported versions of Microsoft Windows
- ManageEngine Desktop
- May be related to Tech Alert | Windows crashes related to Falcon Sensor | 2024-07-19 (/s/article/Tech-Alert-Windows-crashes-related-to-Falcon-Sensor-2024-07-19)

Procedure

1. **Retrieve BitLocker Recovery Keys** – Use ManageEngine Desktop Central to retrieve BitLocker recovery keys:

   a. Open the ManageEngine Desktop Central console.

   b. Navigate to **Inventory > BitLocker Management**.

   c. Select the specific device and view the recovery key.

2. **Develop a PowerShell Script** – The script will handle booting into safe mode, changing the registry key, and rebooting into normal mode. However, since BitLocker is enabled, you'll need to ensure you have the recovery key.

```
# CrowdStrikeFix.ps1
# This script deletes the problematic CrowdStrike driver file causing
BSODs and reverts Safe Mode

$filePath = "C:\Windows\System32\drivers\C-00000291*.sys"
$files = Get-ChildItem -Path $filePath -ErrorAction SilentlyContinue

foreach ($file in $files) {
    try {
        Remove-Item -Path $file.FullName -Force
        Write-Output "Deleted: $($file.FullName)"
    } catch {
        Write-Output "Failed to delete: $($file.FullName)"
    }
}

# Revert Safe Mode Boot after Fix
bcdedit /deletevalue {current} safeboot
Restart-Computer -Force
```

3. Retrieve BitLocker Recovery Keys:

   a. Use Azure AD to retrieve BitLocker recovery keys

   b. Navigate to **Azure AD > Devices > All Devices**

   c. Click on the specific device and select "**Show Recovery Key**"

   d.
   ```
   # Example of retrieving BitLocker recovery key
   $bitLockerKey = Get-BitLockerVolume | Select-Object -ExpandProperty
   KeyProtector | Where-Object { $_.KeyProtectorType -eq
   'RecoveryPassword' } | Select-Object -ExpandProperty
   RecoveryPassword
   ```

4. **Deploy the Script Using ManageEngine Desktop Central**

   a. **Create a Configuration:**

      i. In the ManageEngine Desktop Central console, go to Configurations > Script Configuration.

      ii. Create a new script configuration and add the PowerShell script.

   b. **Deploy the Configuration** – Choose the target devices and deploy the configuration.

5. **Monitor and Validate**
    a. Monitor the deployment process through the ManageEngine console.
    b. Validate that the machines boot correctly into normal mode after the script runs.

Additional Information

- **ManageEngine Compliance Settings**: Use ManageEngine Compliance Settings to monitor and ensure BitLocker compliance.
- **Windows Admin Center**: Use Windows Admin Center for easier management and monitoring of your devices.
- **Backup**: Ensure you have backups of important data before making changes to registry and system files.

See Also

- BitLocker recovery in Microsoft Azure (/s/article/ka16T000001tlmZQAQ)
- BitLocker recovery in Microsoft environments using SCCM (/s/article/ka16T000001tlmeQAA)
- BitLocker recovery in Microsoft environments using Active Directory and GPOs (/s/article/ka16T000001tlmjQAA)
- BitLocker recovery in Microsoft environments using Ivanti Endpoint Manager (/s/article/ka16T000001tlmtQAA)
- BitLocker recovery in Microsoft environments using IBM BigFix (/s/article/ka16T000001tlnSQAQ)