BitLocker recovery in Microsoft environments using SCCM

Published Date: Jul 19, 2024

Objective

- BitLocker recovery in Microsoft environments using SCCM

Applies To

- Supported versions of the Falcons sensor for Windows
- Supported versions of Microsoft Windows
- Microsoft SCCM
- May be related to Tech Alert | Windows crashes related to Falcon Sensor | 2024-07-19

Procedure

1. Retrieve BitLocker Recovery Keys – Use SCCM to retrieve BitLocker recovery keys:

a. Open the SCCM console
b. Navigate to **Assets and Compliance > Endpoint Protection > BitLocker Management**
c. Select the specific device and click **"Recovery Keys."**

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\CrowdStrike\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 SCCM

a. **Create a Package and Program:**
    i. In the SCCM console, go to **Software Library > Application Management > Packages**
    ii. Right-click and select **Create Package**. Provide necessary information and click **Next**
    iii. Right-click on the newly created package, select **Create Program**, and configure the program to run the PowerShell script
b. **Distribute the Package:**
    i. Right-click the package and select **Distribute Content**
    ii. Select the distribution points and complete the wizard
c. **Deploy the Package:**
    i. Right-click the package and select **Deploy**

        ii. Choose the target collection (e.g., all impacted machines) and complete the wizard

    d. **Monitor and Validate:**
        i. Monitor the deployment process through the SCCM console
        ii. Validate that the machines boot correctly into normal mode after the script run

Additional Information

- **SCCM Compliance Settings:** Use SCCM 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

Example Use Case with SCCM

Create and Deploy a Package in SCCM

1. **Create a Package:**
    a. Go to Software Library > Application Management > Packages
    b. Right-click and select Create Package
    c. Provide the necessary details and click Next
2. **Create a Program:**
    a. Right-click the newly created package and select Create Program
    b. Configure the program to run the PowerShell script
3. **Distribute the Package:**
    a. Right-click the package and select Distribute Content
    b. Choose the distribution points and complete the wizard
4. **Deploy the Package:**
    a. Right-click the package and select Deploy
    b. Select the target collection and complete the wizard
5. **Monitor Execution:** Use the SCCM console to monitor the deployment and check for any errors

Options if You Lost or Have Difficulty Finding Your Recovery Key

If you have lost the BitLocker recovery key, the options for recovery are limited. However, you can try the following steps:

1. **Check for Stored Recovery Keys**
    - **SCCM:**

        - Use the SCCM console to find recovery keys under Assets and Compliance > Endpoint Protection > BitLocker Management
        - Select the device and view the recovery key
    - **Active Directory (AD):**
        - Open the Active Directory Users and Computers snap-in
        - Right-click on the computer object and select "Properties."
        - Go to the "BitLocker Recovery" tab to see if the key is stored
    - **Microsoft Account:**
        - Go to the Microsoft account website
        - Log in with the associated Microsoft account
        - Check for recovery keys under the "Devices" section
2. **Use Microsoft Support** – Contact Microsoft Support for assistance. They may have additional methods to help retrieve the recovery key, especially if the devices are managed through enterprise solutions.
3. **Prevent Future Loss**
    - **Backup Recovery Keys:** Ensure that recovery keys are backed up in multiple secure locations
    - **Document Management:** Implement a policy for documenting and storing recovery keys securely

Example: Checking SCCM for Recovery Keys

1. Open the SCCM console
2. Navigate to **Assets and Compliance > Endpoint Protection > BitLocker Management**
3. Locate and select the device in question
4. View the recovery key in the "Recovery Keys" section

Example: Checking Microsoft Account for Recovery Keys

1. Log in to the Microsoft Account
2. Sign in with the Microsoft account associated with the device
3. View the list of recovery keys saved to your account and locate the key for the device in question

See also

- BitLocker recovery in Microsoft Azure
- BitLocker recovery in Microsoft environments using Active Directory and GPOs
- BitLocker recovery in Microsoft environments using Ivanti Endpoint Manager
- BitLocker recovery in Microsoft environments using ManageEngine Desktop Central
- BitLocker recovery in Microsoft environments using BigFix