BitLocker recovery in Microsoft environments using BigFix

Published Date: Jul 21, 2024

Objective

- BitLocker recovery in Microsoft environments using BigFix

Applies To

- Supported versions of the Falcon sensor for Windows
- Supported versions of Microsoft Windows
- BigFix endpoint management software
- May be related to Tech Alert | Windows crashes related to Falcon Sensor | 2024-07-19

Procedure

1. Retrieve BitLocker Recovery Keys — Use BigFix to retrieve BitLocker recovery keys:

a. Open the BigFix console.
b. Navigate to **Endpoint Protection > 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\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"**

```
# 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 BigFix

a. **Create a Fixlet:**
    i. In the BigFix console, go to **Fixlets and Tasks > Create Fixlet**.
    ii. Create a new fixlet and add the PowerShell script.
b. **Deploy the Fixlet** – Choose the target devices and deploy the fixlet.

5. Monitor and Validate

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

Additional Information

- **BigFix Compliance Settings:** Use BigFix 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.

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**
    - **Active Directory (AD):**
        a. Open the Active Directory Users and Computers snap-in.
        b. Right-click on the computer object and select Properties.
        c. Go to the BitLocker Recovery tab to see if the key is stored.
    - **Microsoft Account:**
        a. Go to the Microsoft account website.
        b. Log in with the associated Microsoft account.
        c. 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 Active Directory for Recovery Keys

1. Open the **Active Directory Users and Computers** snap-in.
2. Navigate to the computer object in question.
3. Right-click the computer object and select **Properties**.
4. Go to the **BitLocker Recovery** tab and view the recovery key.

Example: Checking Active Directory 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 SCCM
- 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