CROWDSTRIKE

BitLocker recovery in Microsoft environments using Active Directory and GPOs

Published Date: July 19, 2024

Objective

» BitLocker recovery in Microsoft environments using Active Directory and GPOs

Applies To

» Supported versions of the Falcons sensor for Windows

» Supported versions of Microsoft Windows

» Microsoft Active Directory and GPOs

» 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 Active Directory to retrieve BitLocker recovery keys:
   a. Open the **Active Directory Users and Computers** snap-in
   b. Navigate to the computer object
   c. Right-click on the computer object and select **Properties**
   d. Go to the **BitLocker Recovery** tab 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 Group Policy**
   a. **Create a GPO:**
      i. Open the **Group Policy Management Console** (GPMC)
      ii. Right-click on the desired Organizational Unit (OU) and select **Create a GPO in this domain, and Link it here**
      iii. Name the GPO and click **OK**
   b. **Edit the GPO:**
      i. Right-click on the newly created GPO and select **Edit**
      ii. Navigate to **Computer Configuration > Policies > Windows Settings > Scripts (Startup/Shutdown)**
      iii. Double-click **Startup** or **Shutdown** depending on when you want the script to run
      iv. Click **Add**, then **Browse** to the location of your PowerShell script and add it
   c. **Apply the GPO:**
      i. Link the GPO to the appropriate OU containing the target machines
      ii. Ensure the GPO is enforced and has the correct security filtering to apply to the intended machines

5. **Monitor and Validate**
   a. Monitor the deployment process through the **Event Viewer** on target machines
   b. Validate that the machines boot correctly into normal mode after the script runs

Additional Information

» **GPO Compliance Settings:** Use GPO 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

» **CrowdStrike Support Portal Link:** https://supportportal.crowdstrike.com/s/article/ka16T000001tImjQAA

Example Use Case with Active Directory and GPO

Create and Deploy a GPO in Active Directory

1. **Create a GPO:**
   a. Open the **Group Policy Management Console** (GPMC)
   b. Right-click the desired OU and select **Create a GPO** in this domain, and Link it here
   c. Name the GPO and click **OK**

2. **Edit the GPO:**
   a. Right-click the newly created GPO and select **Edit**
   b. Navigate to Computer Configuration > Policies > Windows Settings > Scripts (Startup/Shutdown)
   c. Double-click **Startup** or **Shutdown**
   d. Click **Add**, browse to the PowerShell script, and add it

3. **Apply the GPO:**
   a. Link the GPO to the appropriate OU
   b. Ensure the GPO is enforced and has the correct security filtering

4. **Monitor Execution:**
   a. Use the Event Viewer on target machines to monitor the script execution and check for 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:**
   - **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 therecovery 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 Microsoft Account for Recovery Keys

1. Log in to the Microsoft Account (https://account.microsoft.com/devices/recoverykey)
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