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

BitLocker recovery in Microsoft environments using Active Directory a...

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

Published Date: Jul 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** – Create a script that handles the following tasks:
   - Booting into Safe Mode
   - Changing the registry key
   - Rebooting into Normal Mode
   - Ensure you have the BitLocker recovery key
3. **Prepare the PowerShell Script** – Create a PowerShell script that performs these actions:

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

# Set the registry key
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Services\<YourService>' -Name '<YourKey>' -Value
'<NewValue>'

# Restart into Safe Mode
bcdedit /set {current} safeboot minimal
Restart-Computer -Force

# (In Safe Mode) Change the file and the registry key

# Restart back into Normal Mode
bcdedit /deletevalue {current} safeboot
Restart-Computer -Force
```

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

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 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 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

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 Ivanti Endpoint Manager (/s/article/ka16T000001tlmtQAA)
- BitLocker recovery in Microsoft environments using ManageEngine Desktop Central (/s/article/ka16T000001tln8QAA)
- BitLocker recovery in Microsoft environments using IBM BigFix (/s/article/ka16T000001tlnSQAQ)