



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

## BitLocker recovery in Microsoft environments using Ivanti Endpoint M...

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

Published Date: Jul 19, 2024

### Objective

- BitLocker recovery in Microsoft environments using Ivanti Endpoint Manager

### Applies To

- Supported versions of the Falcons sensor for Windows
- Supported versions of Microsoft Windows
- Ivanti Endpoint Manager
- 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 Ivanti Endpoint Manager to retrieve BitLocker recovery keys:

- a. Open the Ivanti Endpoint Manager console
- b. Navigate to **Security and Compliance > BitLocker**.
- c. Select the specific device and view the recovery key.

2. **Develop a PowerShell Script** – Create a script that handles the following tasks:

- a. Booting into Safe Mode
- b. Changing the registry key
- c. Rebooting into Normal Mode
- d. 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\' -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 Ivanti Endpoint Manager**

- a. **Create a Software Distribution Package:**

- i. In the Ivanti Endpoint Manager console, go to **Software Distribution > Packages**.
- ii. Create a new package and add the PowerShell script.

**b. Distribute the Package:**

- i. Right-click the package and select **Distribute**.
- ii. Choose the target devices and distribute the package.

**c. Deploy the Package** – Schedule the deployment to run on the target devices.

**5. Monitor and Validate**

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

## Additional Information

- **Ivanti Compliance Settings:** Use Ivanti 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 \(/s/article/ka16T000001tImZQAQ\)](/s/article/ka16T000001tImZQAQ).
- [BitLocker recovery in Microsoft environments using SCCM \(/s/article/ka16T000001tImeQAA\)](/s/article/ka16T000001tImeQAA).
- [BitLocker recovery in Microsoft environments using Active Directory and GPOs \(/s/article/ka16T000001tImjQAA\)](/s/article/ka16T000001tImjQAA).
- [BitLocker recovery in Microsoft environments using ManageEngine Desktop Central \(/s/article/ka16T000001tIn8QAA\)](/s/article/ka16T000001tIn8QAA).
- [BitLocker recovery in Microsoft environments using IBM BigFix \(/s/article/ka16T000001tInSQAQ\)](/s/article/ka16T000001tInSQAQ).

Copyright © 2024

[Privacy \(https://www.crowdstrike.com/privacy-notice/\)](https://www.crowdstrike.com/privacy-notice/)

[Cookies \(https://www.crowdstrike.com/cookie-notice/\)](https://www.crowdstrike.com/cookie-notice/)

[Your Privacy Choices](#)

[Terms & Conditions \(https://www.crowdstrike.com/terms-conditions/\)](https://www.crowdstrike.com/terms-conditions/)