Intune Device BitLocker & LAPS Reporting using Microsoft Graph

Overview

This automation produces a consolidated report for Windows devices in Intune. It combines device compliance information with BitLocker recovery key metadata and Local Administrator Password Solution (LAPS) rotation data. The output is a PowerShell object list that is ready for export or further filtering in scripts and runbooks.

What It Does

The script first queries Intune for all managed Windows devices. For each device, it retrieves the most recent BitLocker recovery key backup timestamp and checks whether a recovery key exists. It then retrieves the last LAPS password rotation timestamp for the same Entra device ID. Finally, it merges these values with the device name, Intune device ID, and compliance state into a single per-device record.

How It Works

1. **Managed device inventory**
   The script calls the Microsoft Graph `deviceManagement/managedDevices` endpoint with a Windows filter. It selects only the fields required to link the device to Entra and to report compliance.
2. **BitLocker recovery keys**
   For each device, the script queries the BitLocker recovery key collection using a device ID filter. It sorts by `createdDateTime` and keeps the newest entry as the backup timestamp for that device.

3. **LAPS credentials**
   For each device, the script calls `directory/deviceLocalCredentials/{deviceId}` and reads `lastPasswordRotationDateTime`. The lookup uses the Entra device ID to align with Graph directory objects.
4. **Report assembly**
   The script joins all values by Entra device ID and outputs a PowerShell object with consistent property names.

Requirements

You must run the script in PowerShell 5.1 or PowerShell 7+ and provide a valid Microsoft Graph access token in `$Global:MicrosoftEntraIDAccessToken`. The environment must be able to reach `https://graph.microsoft.com`.

Graph Permissions (minimum)

The access token must include delegated or app-only permissions that cover both Intune and directory data. The minimum set is:

- `Device.Read.All`
- `DeviceManagementManagedDevices.Read.All`
- `BitLockerKey.Read.All` (or `BitLockerKey.ReadBasic.All` if you do not need key material)
- `DeviceLocalCredential.Read.All`

If you are using delegated permissions, the signed-in user must also hold a directory role that allows reading these resources, such as Intune Administrator, Security Administrator, Helpdesk Administrator, or Global Administrator.

Usage

Set the access token, run the script, and capture the output if desired.

```
$Global:MicrosoftEntraIDAccessToken = "<GraphAccessToken>"
$results = .\Bitlocker&LAPSReporting.ps1
```

The script returns objects with the following properties:

- `DeviceName`
- `IntuneDeviceId`

- `ComplianceStatus`
- `BitlockerRecoveryKeyStatus`
- `BitlockerRecoveryKeyBackupTimestamp`
- `LocalAdminPasswordLastRotationTimestamp`

Logging

The script writes progress messages to the host for each device. These messages include BitLocker processing, LAPS processing, and report assembly so you can trace the flow and identify any device that fails to return data.

Notes and Limitations

BitLocker recovery keys must be queried per device because the API requires a collection query with a device ID filter. LAPS data is retrieved from the Entra directory endpoint and therefore depends on the device being registered and the caller having directory permissions. The script only targets Windows devices by design and does not include macOS or mobile platforms. The REST client retries transient Graph failures and rate limits, but very large tenants may still need staggered runs.

Troubleshooting

Authorization error
Confirm that the access token is minted for Microsoft Graph and that it contains the required scopes or roles. The `aud` claim must be `https://graph.microsoft.com/`, and the `scp` (delegated) or `roles` (app-only) claim must include the permissions listed above. For app-only permissions, ensure admin consent is granted and that a new token has been issued after consent.

Connection closed by remote host
This usually indicates a transient network or throttling issue. The script retries those errors, but you can also reduce request volume by adding delays or running during off-peak hours.

Files

The automation consists of the following files:

- Script: Microsoft Intune\Bitlocker&LAPSReporting.ps1

Revision #2
Created 2026-01-19 12:28:19 UTC by Luca Noah Caprez
Updated 2026-01-19 13:27:59 UTC by Luca Noah Caprez