Defender for Endpoint DLP on macOS: Troubleshooting Runbook

macOS 版 Defender for Endpoint DLP トラブルシューティング ランブック

April 11, 2026 / 2026 年 4 月 11 日

English Version

See page 16 →

日本語版

3 ページへ →

eSolia

macOS 版 Defender for Endpoint DLP トラブルシューティング ランブック

2026 年 4 月 11 日

目次

> eSolia INTERNAL — Not for distribution outside eSolia

eSolia 管理下の macOS デバイスで Microsoft Defender for Endpoint および Endpoint DLP の問題が起きたときの実践ランブックです。特に、2026 年 4 月に 4 時間溶かした落とし穴（**Defender Organization ID は Entra Tenant ID ではない**）を最優先で覚えておいてください。

このランブックを使う場面

以下のいずれかに該当する場合、このドキュメントを開いてください。

- Microsoft Purview → Device onboarding → Devices で macOS デバイスの **Endpoint DLP status が Disabled** と表示される
- Accessibility または Full Disk Access の Configuration status が「Not updated」のまま動かない
- Mac 上で `mdatp health` を実行すると、期待と異なる `org_id` が返ってくる
- Defender が間違ったテナントにオンボードされているように見えて、ワイプを検討している
- tamper protection が `sudo` での Defender daemon 操作をブロックしている

破壊的な作業を始める前に、必ず次のセクションを読んでください。 混乱の最も多い原因は、設定ミスではなく「思い込み」です。

これだけは覚えておきたい

Microsoft は、同じ組織に対して 2 つの異なる GUID を並行して使っています。

識別子	意味	確認できる場所	eSolia の値
Entra Tenant ID	Microsoft Entra のディレクトリ ID。組織ごとに 1 つ。	Entra admin center、Azure portal、M365 管理ツールの URL の `tid=` パラメータ	`436f19ac-627e-4ec1-bfcb-7404d06a5b46`
Defender Organization ID	Microsoft Defender XDR 内部で使われるワークスペース識別子。これも組織ごとに 1 つ。	`mdatp health --field org_id` の出力、Defender portal の attack map、onboarding XML のペイロード	`9cf9ad79-f064-42b8-b551-0bd97d6a9efe`

この 2 つの GUID は、両方とも eSolia を指しています。 同じ識別子ではありません。Mac 上で `mdatp health --field org_id` を実行して、Purview ポータルの `tid=` と一致しない GUID が返ってきても、**それは正常な挙動です。** クロステナント汚染と解釈しないでください。

出典: Microsoft Q&A — Updating Organization Name in Microsoft Defender。Microsoft スタッフの説明によれば、Defender portal では Tenant ID と Organization ID は別の識別子であり、Tenant ID は Entra と一致するが、Organization ID はセキュリティコンテキスト専用の識別子である、とのこと。

このランブックから 1 つだけ持ち帰るなら、上の表です。

診断手順

Intune や Purview で何かを変更する前に、影響を受けている Mac で以下のコマンドを実行し、期待値と照合してください。

Step 1: Defender が動作しライセンスが有効か確認

```
mdatp health
```

出力の以下のフィールドを確認します。

フィールド	期待値	期待値と違う場合
`healthy`	`true`	Defender に問題あり。`health_issues` 配列を確認
`licensed`	`true`	ライセンス割り当ての問題、またはオンボードされていない
`org_id`	eSolia の Defender Org ID（上の表を参照）	**パニックする前に必ず表と照合**
`real_time_protection_enabled`	`true [managed]`	Preferences profile が未展開または未適用
`tamper_protection`	`block [managed]` または `block`	想定通り。誰か（eSolia または過去のオンボーディング）がロックしている
`data_loss_prevention_status`	`active`	Preferences profile から DLP feature flag が欠落。下の Fix 1 を参照
`managed_by`	`MDM`	設定が Intune から来ていない。プロファイル展開を確認

Step 2: インストール済みプロファイルの確認

```
sudo profiles list | grep -iE "wdav|dlp|defender|microsoft"
```

完全に設定された Mac では、最低限以下が必要です。

- `com.microsoft.wdav` preferences profile（例: `eSolia-Defender-Preferences-Baseline-INTERNAL`）
- `com.microsoft.wdav.atp` onboarding profile（例: `eSolia-Purview-macOS-Onboarding-INTERNAL`）
- `com.microsoft.wdav` および `com.microsoft.dlp.daemon` に対して Full Disk Access、Accessibility、Notifications、Background Services を付与するバンドル（または個別プロファイル）

Step 3: Purview ポータルでのデバイス状態確認

Purview ポータル（次の Step でテナントを必ず確認）で Settings → Device onboarding → Devices を開き、対象 Mac を見つけます。詳細ペインで以下が全て緑になっているべきです。

- **Configuration status:** Updated

- **Policy sync status:** Updated
- **Accessibility:** Updated
- **Full disk access:** Updated
- **Endpoint DLP status:** Enabled

どれかが赤い場合、次のセクションのいずれかが該当します。

Step 4: 正しい Purview テナントにサインインしているか確認

変更を加える前に、委任アクセスのある顧客テナントではなく、eSolia の Purview にサインインしていることを確認します。以下の 3 つを独立に確認してください。

1. **URL:** Purview ポータルの URL にある `tid=` が、eSolia の Entra Tenant ID（`436f19ac-627e-4ec1-bfcb-7404d06a5b46`）と一致すること。
2. **アバターメニュー:** 右上のユーザーアイコンをクリック。表示される組織名が「eSolia Inc 株式会社イソリア」であること。
3. **オンボーディングパッケージの内容:** オンボーディング/オフボーディングのパッケージをダウンロード済みなら、XML に含まれる org ID を確認します。

```
grep -oE "[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}" \
  ~/Downloads/DeviceComplianceOnboardingPackage/intune/DeviceComplianceOnboarding.xml \
  | sort -u
```

期待される出力には eSolia の Defender Org ID が含まれているはずです。もし eSolia の Org ID と一致しなければ、ダウンロード時に別のテナントにサインインしていたことになります。

修正手順（可能性の高い順）

上から順に試してください。前のステップを試さずに破壊的なオプションに飛ばないこと。

Fix 1: Preferences profile に DLP feature flag が欠落

症状: `mdatp health` で `data_loss_prevention_status: "disabled"`。Defender は健全でライセンスも MDM 管理も正常。それ以外は全て緑。最も多い DLP 無効化の原因で、2026 年 4 月に eSolia が踏んだのもこれ。

原因: Intune 経由で展開された `com.microsoft.wdav` preferences profile に、DLP daemon を有効化する `dlp.features` キーが含まれていない。

クイックフィックス（ランタイム、次のプロファイル同期まで持続）:

```
sudo mdatp config data-loss-prevention --value enabled
mdatp health --field data_loss_prevention_status

# 期待値: "active"
```

恒久対応（preferences profile）: baseline preferences profile の `com.microsoft.wdav` ペイロード内に以下のブロックを追加し、Intune 経由で再展開します。

```
<key>dlp</key>
<dict>
    <key>features</key>
    <array>
        <dict>
            <key>name</key>
            <string>DLP_feature_enabled</string>
            <key>state</key>
            <string>enabled</string>
        </dict>
    </array>
</dict>
```

完成版のリファレンスプロファイルは、本ランブックと同じ場所にある `eSolia-Defender-Preferences-Baseline-v2-INTERNAL.mobileconfig` です。

Fix 2: Company Portal がアプリ変更をブロックされている（macOS 15 以降）

症状: Intune からプロファイルは展開されるが、Defender の状態が変わらない。macOS に「Company Portal was prevented from modifying apps on your Mac」という通知が出る。

原因: macOS 15（Sequoia）で追加された App Management プライバシー制御。他のアプリを変更するアプリに対して明示的な承認が必要で、Company Portal はまさにそのカテゴリに該当します。オフだと、Intune はアプリインストール、更新、一部のプロファイル駆動の状態変更を実行できません。

対処: Mac 上で System Settings → Privacy & Security → App Management → **Company Portal** をオンにする。その後 Company Portal から policy sync を実行し、`mdatp health` を再確認。

これは macOS 15 以降の新規 Mac 向けの eSolia 標準オンボーディングチェックリストに追加すべき項目です。

Fix 3: PPPC 権限の不足、またはユーザー付与（MDM 管理でない）

症状: Purview ポータルで Accessibility や Full Disk Access が「Not updated」と表示される。Mac 上で Defender は動いている。macOS System Settings で手動で権限を有効化しても改善しない。

原因: Purview は、MDM 経由で push された PPPC profile によって付与された TCC 権限（Accessibility、Full Disk Access など）のみを認識します。ユーザーが手動でトグルした権限は認識しません。特に `com.microsoft.dlp.daemon` は Defender エージェント本体とは別のアプリケーションであり、権限を個別に付与する必要があります。

対処: Microsoft の combined `mdatp.mobileconfig` バンドルを Intune の Custom profile として展開します。このバンドルには Full Disk Access、Accessibility、Notifications、Background Service Management、Network Filter、System Extensions の PPPC ペイロードが含まれており、`com.microsoft.wdav` と `com.microsoft.dlp.daemon` の両方に対して事前設定されています。

ダウンロード元：https://raw.githubusercontent.com/microsoft/mdatp-xplat/master/macos/mobileconfig/combined/mdatp.mobileconfig

Intune での展開: Devices → macOS → Configuration profiles → New Policy → Templates → **Custom** → `.mobileconfig` をアップロード → Device channel → 対象 Mac に割り当て。

プロファイル適用後、Mac を再起動してください。実行中の daemon に対する TCC 権限の付与は、daemon 起動時が最も確実です。

Fix 4: Tamper protection がテナント変更またはアンインストールをブロック

症状: 本当に別テナントに再オンボードしたい（Org ID の読み間違いではなく）、あるいは Defender をアンインストールしたい。uninstall スクリプトを実行すると「Defender is in the strict tamper protected mode, change it to either disabled or audit mode and repeat uninstallation」と表示される。

原因: Tamper protection が設計通りに動いている。正常な挙動です。

推奨の対処 — 現在のテナントからオフボーディングパッケージを取得する。 Defender は、現在の `org_id` 用に署名されたオフボーディングペイロードのみを受け入れます。オフボーディング plist を Intune の Custom profile として展開し、適用させる。これが唯一のサポートされた方法で、残留物もありません。

オフボーディングパッケージが入手できない場合（まれですが、完全性のために記載）：

1. `tamperProtection.status = disabled` を設定する一時的な `com.microsoft.wdav` preferences profile を展開する。リファレンステンプレートは `eSolia-Defender-Tamper-Disable-TEMPORARY-INTERNAL.mobileconfig` にあります。
2. 他に `com.microsoft.wdav` profile が割り当てられていないことを確認する。macOS は競合する managed preferences を「厳しい値が勝つ」ルールでマージするため、baseline profile が tamper protection を `block` に設定していると、disable profile は黙って上書きされます。
3. Company Portal → sync → 再起動 → `mdatp health --field tamper_protection` が `disabled` を返すことを確認。
4. uninstall スクリプトを実行。
5. **直後に tamper-disable profile を Intune から削除する。** 管理対象の Mac に tamper protection 無効の状態を残してはいけません。

Plan B — managed preference が効かない場合（まれ）： macOS Recovery で起動し、data volume から Defender を手動で削除する。Defender が動いていないため、tamper protection を含む全てのランタイム保護をバイパスできます。巻末の Recovery Mode 付録を参照。**使うのは Org ID の問題が本物であることを確認してから。** 2026 年 4 月のインシデントでは、Org ID と Tenant ID の混同により不要な Recovery Mode 実行に至りました。

Fix 5: 別の原因

Fix 1 から 4 を試しても症状が改善しない場合、以下のいずれかの可能性があります。

- **古いデバイスレコード**が Purview に残っている。いずれ自動で reconcile されますが、Purview → Device onboarding → Offboarding から手動オフボードも可能。
- **サードパーティ製セキュリティソフトの競合**（BlockBlock、RansomWhere など）。`mdatp health --field conflicting_applications` で確認。通常 Defender の機能は妨げませんが、ノイズの原因にはなります。
- **ネットワーク egress** が Defender のクラウドエンドポイント到達をブロックしている。`mdatp health --field cloud_enabled` および Defender テレメトリエンドポイントへの到達性を確認。
- **Defender ビルドが古く**、新しい managed preference キーを認識していない。Intune アプリ展開から更新。

2026 年 4 月のインシデント、教訓版

実際に何が起きたか、失敗談として記録します。

1. Mac の Endpoint DLP が Purview で Disabled と表示された。真の原因は Fix 1 の DLP feature flag 欠落。本来なら 15 分で解決する問題。
2. 診断中に `mdatp health --field org_id` が `9cf9ad79-f064-42b8-b551-0bd97d6a9efe` を返した。その時点で Purview ポータルの URL は `tid=436f19ac-627e-4ec1-bfcb-7404d06a5b46`。
3. この 2 つの GUID を同じ識別子（Entra Tenant ID）だと思い込み、不一致を「過去の顧客プロジェクトによるクロステナント汚染」と解釈した。
4. その後 4 時間、誤った方向にトラブルシューティングを進めた。tamper-disable profile の展開、複数回の sync 試行、Recovery Mode での Defender 完全ワイプ、そして完全な再オンボーディング。
5. 再オンボーディング後、`org_id` は同じ `9cf9ad79...` の GUID を返した。そこで Microsoft ドキュメントを検索し、Defender Organization ID が Entra Tenant ID とは別の識別子であることが判明。最初から正常な状態だった。
6. 当初の症状に対する実際の修正（上記 Fix 1）は 1 分もかからなかった。

教訓:

- 2 つの GUID が一致しないとき、それらが「一致すべきものかどうか」を先に確認する。
- 驚きがあったら、破壊的な手順を始める前にドキュメントを検索する。
- 診断手順（Step 1 ～ Step 4）をチェックリストとして目の前に置く。特に Step 4 を飛ばさない。

「急がば回れ」という言葉は、トラブルシューティングでもそのまま効きます。

Appendix A: リファレンスプロファイルテンプレート

以下のテンプレートは本ランブックと一緒に管理されており、Microsoft の Defender for Endpoint managed preference スキーマの更新に追随させるべきものです。

テンプレート	用途	展開タイミング
`eSolia-Defender-Preferences-Baseline-v2-INTERNAL.mobileconfig`	Baseline Defender preferences。DLP feature flag、real-time protection、cloud protection、network protection、tamper protection (block) を含む	eSolia 管理下の全 macOS に恒久展開
`eSolia-Defender-Tamper-Disable-TEMPORARY-INTERNAL.mobileconfig`	Tamper protection を disabled に設定。アンインストール作業用	一時的。使用後に即削除
`eSolia-Purview-macOS-Onboarding-INTERNAL.mobileconfig`	eSolia テナント用の Defender Organization ID およびオンボーディングペイロードを含む。Purview からダウンロードしたオンボーディングパッケージ由来	eSolia 管理下の全 macOS に恒久展開
`mdatp.mobileconfig`（Microsoft GitHub）	Full Disk Access、Accessibility、Notifications、Background Services、Network Filter、System Extensions の PPPC 付与	eSolia 管理下の全 macOS に恒久展開

Appendix B: Recovery Mode ワイプ（最終手段）

Tamper protection が正当なアンインストールを本当にブロックしており、managed preference の対処も失敗している場合のみ使用してください。実行前に Org ID の問題が本物であることを必ず確認してください。

事前準備

1. 最新の Time Machine バックアップ（または同等のバックアップ）があることを確認。
2. Mac のデータボリューム名を控える。`diskutil list` を実行し、`/Library/Application Support` を含む APFS ボリュームを確認。通常は `Macintosh HD - Data` または `Data`。
3. 管理者パスワードを用意（Recovery で FileVault のアンロックに必要）。
4. 本ランブックをスマートフォンまたは別デバイスで開いておく。Recovery からブラウザは使えません。

手順（Apple Silicon）

1. Apple メニュー → シャットダウン。完全に電源オフするまで待つ。
2. 電源ボタンを「Loading startup options…」が表示されるまで長押し。**Options** → **Continue** → 認証。
3. メニューバー → Utilities → Terminal。
4. データボリュームがマウントされていることを確認:

```
ls /Volumes/
```

データボリュームが表示されていない場合はアンロック：5. データボリュームのパスを変数にセットし、Defender が存在することを確認：`bash DATA="/Volumes/Data" # 自環境のボリューム名に合わせる ls -la "$DATA/Library/Application Support/Microsoft/"`

6. Defender と DLP を削除：

```
bash rm -rf "$DATA/Library/Application Support/Microsoft/Defender" rm -rf "$DATA/Library/Application Support/Microsoft/DLP" rm -rf "$DATA/Applications/Microsoft Defender.app" rm -f "$DATA/Library/LaunchDaemons/com.microsoft.fresno.plist" rm -f "$DATA/Library/LaunchDaemons/com.microsoft.fresno.uninstall.plist" rm -f "$DATA/Library/LaunchDaemons/com.microsoft.dlp.install_monitor.plist" rm -f "$DATA/Library/LaunchAgents/com.microsoft.wdav.tray.plist" rm -rf "$DATA/Library/SystemExtensions/"*wdav* 2>/dev/null rm -rf "$DATA/Library/SystemExtensions/"*microsoft* 2>/dev/null
```

7. Defender 関連ファイルが残っていないことを確認：

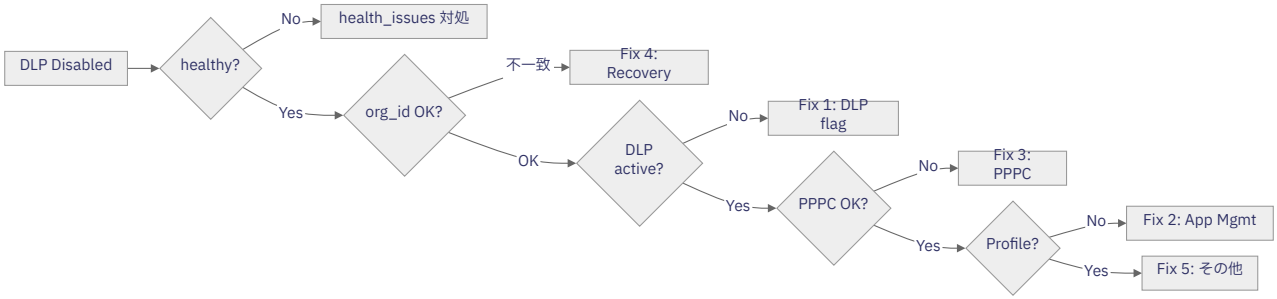
```
bash find "$DATA" -iname "*defender*" 2>/dev/null find "$DATA" -iname "*wdav*" 2>/dev/null find "$DATA" -iname "*mdatp*" 2>/dev/null
```

8. Apple メニュー → 再起動。

再起動後

Defender は削除されているはずです（`mdatp health` が command not found を返す）。Intune 経由で baseline preferences profile、PPPC バンドル、onboarding profile を再割り当てします。Defender は Intune Apps → macOS で必須アプリとして割り当てられていれば自動的に再インストールされます。エージェント再起動後に `mdatp health --field org_id` で確認。そして **Org ID は Entra Tenant ID ではない**ことを忘れずに。

Appendix C: 診断フローチャート



Diagram

関連ドキュメント

- Microsoft: Onboard macOS devices into Microsoft Purview solutions using Intune (MDE customers)
- Microsoft: Troubleshoot Endpoint DLP configuration and policy sync
- Microsoft: mdatp-xplat GitHub リポジトリ — `.mobileconfig` テンプレートの一次ソース

お問い合わせ

株式会社イソリア 〒105-7105 東京都港区東新橋 1-5-2 汐留シティセンター 5 階 (Workstyling)

電話	**03-4577-3380**
メール	hello@esolia.co.jp
Web	https://esolia.co.jp
営業時間	月～金、9:00～18:00

eSolia

Defender for Endpoint DLP on macOS: Troubleshooting Runbook

April 11, 2026

Contents

> eSolia INTERNAL — Not for distribution outside eSolia

A practical runbook for diagnosing and fixing Microsoft Defender for Endpoint and Endpoint DLP issues on eSolia-managed macOS devices, with special attention to the gotcha that cost us four hours: **Defender Organization ID is NOT the Entra Tenant ID**.

When to use this runbook

Reach for this document when any of the following is true:

- A macOS device in Microsoft Purview → Device onboarding → Devices shows **Endpoint DLP status: Disabled**
- Configuration status is stuck on "Not updated" for Accessibility or Full Disk Access
- `mdatp health` on a Mac returns an `org_id` that doesn't match what you expect
- You're considering wiping Defender because it seems onboarded to the wrong tenant
- Tamper protection is blocking `sudo` commands against the Defender daemon

Stop and read the next section before doing anything destructive. The most common cause of confusion is a mental model error, not a real configuration problem.

The one thing that could save you hours

Microsoft uses two different GUIDs for the same organization, and they live side by side:

Identifier	What it is	Where you see it	Example (eSolia)
Entra Tenant ID	The Directory ID for Microsoft Entra. One per organization.	Entra admin center, Azure portal, `tid=` URL parameter in M365 admin centers	`436f19ac-627e-4ec1-bfcb-7404d06a5b46`
Defender Organization ID	A separate workspace identifier used inside Microsoft Defender XDR. Also one per organization.	`mdatp health --field org_id` output, Defender portal attack map, onboarding XML payloads	`9cf9ad79-f064-42b8-b551-0bd97d6a9efe`

Both of these GUIDs point to eSolia. They are not interchangeable. When you check `mdatp health --field org_id` on a Mac and see a GUID that doesn't match the `tid=` in your Purview portal URL, **this is expected and correct**. Do not interpret it as cross-tenant contamination.

Source: Microsoft Q&A — Updating Organization Name in Microsoft Defender. Quote from Microsoft staff: in the Defender portal, the Tenant ID and Organization ID are distinct; the Tenant ID matches Entra, but the Organization ID is a separate identifier used specifically within the security context.

If you remember only one thing from this runbook, remember this table.

Diagnostic sequence

Run these commands on the affected Mac and compare the output against the expected state before touching anything in Intune or Purview.

Step 1: Confirm Defender is running and licensed

```
mdatp health
```

Look for these fields in the output:

Field	Expected	If wrong
`healthy`	`true`	Defender has issues — check `health_issues` array
`licensed`	`true`	License assignment problem, or Defender not onboarded
`org_id`	eSolia Defender Org ID (see gotcha table above)	**Verify against the table before panicking**
`real_time_protection_enabled`	`true [managed]`	Preferences profile missing or not applied
`tamper_protection`	`block [managed]` or `block`	Expected — means someone (eSolia or prior onboarding) locked it
`data_loss_prevention_status`	`active`	DLP feature flag missing from preferences profile — see fix below
`managed_by`	`MDM`	Config isn't coming from Intune — check profile deployment

Step 2: Check installed configuration profiles

```
sudo profiles list | grep -iE "wdav|dlp|defender|microsoft"
```

For a fully-configured Mac, you should see at minimum:

- `com.microsoft.wdav` preferences profile (e.g., `eSolia-Defender-Preferences-Baseline-INTERNAL`)
- `com.microsoft.wdav.atp` onboarding profile (e.g., `eSolia-Purview-macOS-Onboarding-INTERNAL`)
- A bundle or individual profiles granting Full Disk Access, Accessibility, Notifications, and Background Services to `com.microsoft.wdav` and `com.microsoft.dlp.daemon`

Step 3: Check Purview portal device status

In the Purview portal (confirm tenant first — see next step), go to Settings → Device onboarding → Devices and find the Mac. The detail pane should show:

- **Configuration status:** Updated (green)

- **Policy sync status:** Updated (green)
- **Accessibility:** Updated
- **Full disk access:** Updated
- **Endpoint DLP status:** Enabled

If any of these are red, the fix is usually one of the steps in the next section.

Step 4: Verify you are in the correct Purview tenant

Before making any changes, confirm you are signed in to eSolia's Purview and not a customer tenant you have delegated access to. Three independent checks:

1. **URL:** The `tid=` parameter in the Purview portal URL should be eSolia's Entra Tenant ID (`436f19ac-627e-4ec1-bfcb-7404d06a5b46`).
2. **Avatar menu:** Click your user icon at the top right. The organization name shown should be "eSolia Inc 株式会社イソリア".
3. **Onboarding package content:** If you have downloaded an onboarding or offboarding package, run the following against the XML file to see which org ID it is signed for:

```
grep -oE "[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}" \
  ~/Downloads/DeviceComplianceOnboardingPackage/intune/DeviceComplianceOnboarding.xml \
  | sort -u
```

Expected output includes eSolia's Defender Org ID. A Defender Org ID that does not match eSolia means you were signed into a different tenant when you downloaded the package.

Fixes, in order of likelihood

Work through these in order. Do not skip ahead to destructive options until the earlier steps have been tried and verified.

Fix 1: DLP feature flag missing from preferences profile

Symptom: `data_loss_prevention_status: "disabled"` in `mdatp health`, even though Defender is otherwise healthy, licensed, and managed. Everything else green. This is the most common cause of a disabled DLP status and is the issue eSolia hit in April 2026.

Cause: The `com.microsoft.wdav` preferences profile deployed via Intune does not include the `dlp.features` key that enables the DLP daemon.

Quick fix (runtime, survives until next profile sync):

```
sudo mdatp config data-loss-prevention --value enabled
mdatp health --field data_loss_prevention_status

# Expect: "active"
```

Durable fix (preferences profile): Add the following block inside the `com.microsoft.wdav` payload of your baseline preferences profile, then redeploy via Intune:

```
<key>dlp</key>
<dict>
    <key>features</key>
    <array>
        <dict>
            <key>name</key>
            <string>DLP_feature_enabled</string>
            <key>state</key>
            <string>enabled</string>
        </dict>
    </array>
</dict>
```

A complete reference profile is kept at `eSolia-Defender-Preferences-Baseline-v2-INTERNAL.mobileconfig` in the eSolia shared docs location for this runbook.

Fix 2: Company Portal blocked from modifying apps (macOS 15+)

Symptom: Profiles deploy from Intune but Defender state does not change. You see a macOS system notification like “Company Portal was prevented from modifying apps on your Mac.”

Cause: macOS 15 (Sequoia) added an App Management privacy control that requires explicit approval for apps that modify other apps. Company Portal is exactly such an app. If the toggle is off, Intune cannot push app installs, updates, or certain profile-driven state changes.

Fix: On the Mac, System Settings → Privacy & Security → App Management → toggle **Company Portal** on. Force a policy sync from Company Portal afterwards and re-check `mdatp health`.

This should be added to the standard eSolia macOS onboarding checklist for any new Mac on macOS 15+.

Fix 3: PPPC permissions missing or user-granted instead of MDM-managed

Symptom: Purview portal shows Accessibility and/or Full Disk Access as "Not updated" even though you can see Defender running on the Mac. Toggling the permissions manually in macOS System Settings does not help.

Cause: Purview only recognizes TCC permissions (Accessibility, Full Disk Access, etc.) that were granted by an MDM-pushed PPPC profile, not permissions toggled manually by the user. The `com.microsoft.dlp.daemon` binary in particular is a separate application from the main Defender agent, and its permissions need to be granted explicitly.

Fix: Deploy Microsoft's combined `mdatp.mobileconfig` bundle as a Custom profile in Intune. It includes the PPPC payloads for Full Disk Access, Accessibility, Notifications, Background Service Management, Network Filter, and System Extensions, all pre-configured for both `com.microsoft.wdav` and `com.microsoft.dlp.daemon`.

Download from: https://raw.githubusercontent.com/microsoft/mdatp-xplat/master/macos/mobileconfig/combined/mdatp.mobileconfig

Deploy in Intune: Devices → macOS → Configuration profiles → New Policy → Templates → **Custom** → upload the `.mobileconfig` → Device channel → assign to the target Mac.

After the profile lands, reboot the Mac. TCC grants for running daemons are most reliably applied at daemon startup.

Fix 4: Tamper protection blocking a tenant change or uninstall

Symptom: You need to re-onboard Defender to a different tenant (genuinely — not because you misread the Org ID), or you need to uninstall Defender. Running the uninstall script returns "Defender is in the strict tamper protected mode, change it to either disabled or audit mode and repeat uninstallation."

Cause: Tamper protection is doing exactly what it was designed to do. This is correct behavior.

Preferred fix — get an offboarding package from the current tenant. Defender will accept an offboarding payload signed for its current `org_id`. Deploy the offboarding plist as a Custom profile in Intune and let it run. This is the only supported method and leaves no residue.

If you cannot obtain an offboarding package (uncommon, but the path is documented for completeness):

1. Deploy a temporary `com.microsoft.wdav` preferences profile that sets `tamperProtection.status = disabled`. A reference template is kept at `eSolia-Defender-Tamper-Disable-TEMPORARY-INTERNAL.mobileconfig`.
2. Ensure no other `com.microsoft.wdav` profile is also assigned — macOS merges conflicting managed preferences with the stricter value winning, so a baseline profile setting tamper protection to `block` will override your disable profile silently.

3. Company Portal → sync → reboot → verify `mdatp health --field tamper_protection` returns `disabled`.
4. Run the uninstall script.
5. **Immediately delete the tamper-disable profile from Intune.** Never leave tamper protection disabled on a managed Mac.

Plan B if the managed preference does not take effect (rare): Boot into macOS Recovery and manually delete Defender from the data volume. This bypasses every runtime protection, including tamper protection, because Defender is not running. See the Recovery Mode appendix at the end of this runbook. **Only use this path after confirming the org ID is genuinely wrong** (i.e., you have verified against the eSolia Defender Org ID and the Mac is truly pointing to a different organization). In the April 2026 incident, we reached for Recovery Mode unnecessarily because of the Org ID vs Tenant ID confusion.

Fix 5: The problem is actually elsewhere

If you have worked through fixes 1 through 4 and the symptom persists, the problem is likely:

- **Stale device record** in Purview from a previous onboarding attempt, which will eventually reconcile but can be manually offboarded from Purview → Device onboarding → Offboarding.
- **Conflicting third-party security software** such as BlockBlock or RansomWhere listed in `mdatp health --field conflicting_applications`. These typically do not prevent Defender from functioning but may cause noise.
- **Network egress** blocking Defender from reaching its cloud endpoints. Check `mdatp health --field cloud_enabled` and Defender telemetry endpoints are reachable from the Mac.
- **Outdated Defender build** that does not recognize newer managed preference keys. Update via Intune app deployment.

The April 2026 incident, condensed

What actually happened, as a cautionary tale:

1. A Mac showed Endpoint DLP as “Disabled” in Purview. The real cause was Fix 1 — the DLP feature flag was not in the preferences profile. Fifteen-minute fix.
2. During diagnosis, `mdatp health --field org_id` returned `9cf9ad79-f064-42b8-b551-0bd97d6a9efe`. The Purview portal URL at the time showed `tid=436f19ac-627e-4ec1-bfcb-7404d06a5b46`.
3. The two GUIDs were assumed to be the same identifier (Entra Tenant ID), and the mismatch was interpreted as the Mac being cross-tenant contaminated from a prior client project.
4. Four hours of misdirected troubleshooting followed: a tamper-disable profile, multiple sync attempts, a full Recovery Mode wipe of Defender, and a complete re-onboarding sequence.
5. After the re-onboarding, `org_id` came back as the same `9cf9ad79...` GUID. A search of Microsoft documentation revealed that the Defender Organization ID is a separate identifier from the Entra Tenant ID, and the original state had been correct the entire time.
6. The actual fix for the original symptom (Fix 1 above) took under a minute.

Lessons:

- When two GUIDs do not match, verify what each one represents before concluding they should match.
- Search the documentation as soon as a surprise appears, not after several destructive steps.
- Keep the diagnostic sequence (Step 1 through Step 4) in front of you as a checklist. Do not skip Step 4.

Appendix A: Reference profile templates

The following templates are maintained alongside this runbook and should be kept in sync with any updates to Microsoft's Defender for Endpoint managed preference schema.

Template	Purpose	When to deploy
`eSolia-Defender-Preferences-Baseline-v2-INTERNAL.mobileconfig`	Baseline Defender preferences including DLP feature flag, real-time protection, cloud protection, network protection, and tamper protection in block mode	Permanent assignment to all eSolia macOS devices
`eSolia-Defender-Tamper-Disable-TEMPORARY-INTERNAL.mobileconfig`	Sets tamper protection to disabled for uninstall scenarios	Temporary — delete immediately after use
`eSolia-Purview-macOS-Onboarding-INTERNAL.mobileconfig`	Contains the Defender Organization ID and onboarding payload for eSolia's tenant. Derived from the onboarding package downloaded from Purview.	Permanent assignment to all eSolia macOS devices
`mdatp.mobileconfig` (from Microsoft GitHub)	PPPC grants for Full Disk Access, Accessibility, Notifications, Background Services, Network Filter, System Extensions	Permanent assignment to all eSolia macOS devices

Appendix B: Recovery Mode wipe (last-resort procedure)

Use this only if tamper protection is genuinely blocking a legitimate uninstall and the managed-preference path has failed. Verify the Org ID problem is real before proceeding.

Pre-flight

1. Confirm a current Time Machine backup or equivalent.
2. Record the Mac's data volume name: `diskutil list` and note the APFS volume containing `/Library/Application Support`. Typically named `Macintosh HD - Data` or just `Data`.
3. Have the admin password available (required to unlock FileVault in Recovery).
4. Access this runbook from a phone or second device — you will not have browser access from Recovery.

Procedure (Apple Silicon)

1. Apple menu → Shut Down. Wait for full power-off.
2. Press and hold the power button until "Loading startup options…" appears. Click **Options** → **Continue** → authenticate.
3. Menu bar → Utilities → Terminal.
4. Verify the data volume is mounted:

```
ls /Volumes/
```

If the data volume is not listed, unlock it: 5. Set a variable for the data volume path and verify Defender is present:

```
bash DATA="/Volumes/Data" # Adjust to match your volume name ls -la "$DATA/Library/Application Support/Microsoft/"
```

6. Delete Defender and DLP:

```
bash rm -rf "$DATA/Library/Application Support/Microsoft/Defender" rm -rf "$DATA/Library/Application Support/Microsoft/DLP" rm -rf "$DATA/Applications/Microsoft Defender.app" rm -f "$DATA/Library/LaunchDaemons/com.microsoft.fresno.plist" rm -f "$DATA/Library/LaunchDaemons/com.microsoft.fresno.uninstall.plist" rm -f "$DATA/Library/LaunchDaemons/com.microsoft.dlp.install_monitor.plist" rm -f "$DATA/Library/LaunchAgents/com.microsoft.wdav.tray.plist" rm -rf "$DATA/Library/SystemExtensions/"*wdav* 2>/dev/null rm -rf "$DATA/Library/SystemExtensions/"*microsoft* 2>/dev/null
```

7. Verify nothing Defender-related remains:

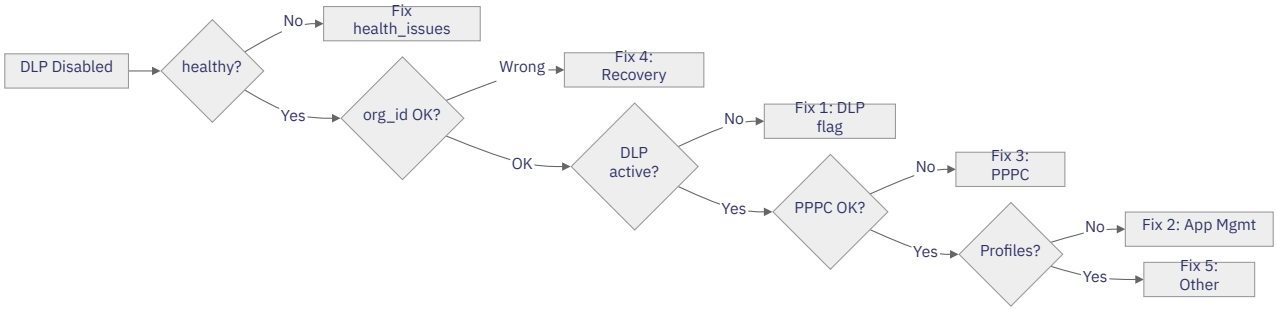
```
bash find "$DATA" -iname "*defender*" 2>/dev/null find "$DATA" -iname "*wdav*" 2>/dev/null find "$DATA" -iname "*mdatp*" 2>/dev/null
```

8. Apple menu → Restart.

After reboot

Defender should be gone (`mdatp health` returns "command not found"). Reassign the baseline preferences profile, the PPPC bundle, and the onboarding profile via Intune. Defender will reinstall automatically if assigned as a required app in Intune Apps → macOS. Verify with `mdatp health --field org_id` once the agent is running again — and remember the Org ID is NOT the Entra Tenant ID.

Appendix C: Diagnostic flowchart



Diagram

Related documents

- Microsoft: Onboard macOS devices into Microsoft Purview solutions using Intune (MDE customers)
- Microsoft: Troubleshoot Endpoint DLP configuration and policy sync
- Microsoft: mdatp-xplat GitHub repository — source for `.mobileconfig` templates

Contact Us

eSolia Inc. Shiodome City Center 5F (Workstyling) 1-5-2 Higashi-Shimbashi, Minato-ku Tokyo 105-7105, Japan

Phone	03-4577-3380
Email	hello@esolia.co.jp
Web	https://esolia.co.jp/en
Hours	Monday-Friday, 9:00-18:00 JST