# セキュアエンドポイントのWindowsイベントIDのリストのエクスポート

## 内容



## はじめに

このドキュメントでは、Cisco Secure EndpointのすべてのイベントIDについて説明し、効果的なモニタリングとインシデント対応を支援します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Windowsイベントログ
- Cisco Secure Endpoint

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアバージョンに基づくものです。

- Cisco Secureエンドポイント8.4.0.30201
- Windows Server 2019

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 問題

Cisco Secure EndpointのWindowsイベントIDは、効果的なモニタリングとトラブルシューティングに不可欠です。これらのイベントIDにアクセスできることは、問題の診断、運用効率の確保、および全体的なセキュリティの強化に不可欠です。

# 解決方法

ファイルエクスプローラを開き、C:\Program Files\Cisco\AMP\<バージョン番号>\AMPEvents.man ファイルに移動します。このファイルをメモ帳で開くと、Cisco Secure Endpointによって生成されたWindowsイベントに関連するすべての情報が表示されます。

AMPEvents.manファイルからエクスポートされたイベントIDのリスト：

| イベントID | [Event] | エンジン/タスク | レベル |
|---|---|---|---|
| 100 | EXPREV_ATTACK_WITHOUT_SUSPICIOUS_FILES_V1/V2/V3/V4 | 不正利用の防止 | 情報 |
| 101 | EXPREV_ATTACK_WITH_SUSPICIOUS_FILES_V1/V2/V3/V4 | 不正利用の防止 | 情報 |
| 102 | EXPREV_ATTACK_WITHOUT_SUSPICIOUS_FILES_V3/V4_監査 | 不正利用の防止 | 情報 |
| 103 | EXPREV_ATTACK_WITH_SUSPICIOUS_FILES_V3/V4_監査 | 不正利用の防止 | 情報 |
| 104 | EXPREV_SCRIPT_CONTROL_ATTACK_V4 | 不正利用の防止 | 情報 |
| 105 | EXPREV_SCRIPT_CONTROL_ATTACK_V4_監査 | 不正利用の防止 | 情報 |
| 200 | MALICIOUS_ACTIVITY_PROTECTION_V1/V2 | 悪意のある活動の保護 | 情報 |
| 300 | SD_BLOCK_PROCESS_ACTION_V1 | システムプロセス保護 | 情報 |
| 400 | CCMS_JOB_STARTED_V1 | CCMS（必須） | 情報 |
| 401 | JANUS_EVENT_V1 | | 情報 |
| 500 | エンドポイント_分離_開始_V1 | エンドポイント分離 | 情報 |
| 501 | エンドポイント分離停止中V1 | エンドポイント分離 | 情報 |
| 502 | エンドポイントの分離の開始に失敗しました | エンドポイント分離 | エラー |
| 503 | エンドポイント_分離_停止失敗_V1 | エンドポイント分離 | エラー |
| 504 | エンドポイント分離アップデートV1 | エンドポイント分離 | 情報 |
| 505 | ENDPOINT_ISOLATION_UPDATEFAILED_V1 | エンドポイント分離 | エラー |
| 600 | ORBITAL_INSTALL_SUCCESS_V1 | 軌道 | 情報 |
| 601 | ORBITAL_INSTALL_FAILED_V1 | 軌道 | エラー |

| | | | |
|---|---|---|---|
| 602 | ORBITAL_UPDATE_SUCCESS_V1 | 軌道 | 情報 |
| 603 | ORBITAL_UPDATE_FAILED_V1（オプション） | 軌道 | エラー |
| 700 | ENDPOINT_ISOLATION_BRUTE_FORCE_ATTEMPT（エンドポイントの分離のブルートフォース試行） | エンドポイント分離 | warning |
| 800 | SCRIPT_PROTECTION_DETECTION_V1（スクリプト保護検出V1） | スクリプト保護 | 情報 |
| 801 | SCRIPT_PROTECTION_QUARANTINE_V1（スクリプト_保護_検疫_V1） | スクリプト保護 | 情報 |
| 900 | エンジン_検出_処理 | 動作保護 | 情報 |
| 901 | ENGINE_DETECTION_NOT_処理 | 動作保護 | エラー |
| 902 | エンジン_検出_監査 | 動作保護 | 情報 |
| 903 | ENGINE_DETECTION_NO_アクション | 動作保護 | 情報 |
| 904 | エンジン_クリーンアップが必要です | 動作保護 | 情報 |
| 1248 | SCAN_COMPLETED_CLEAN_V1（スキャン完了クリーンV1） | スキャン | 情報 |
| 1249 | SCAN_COMPLETED_DIRTY_V1（スキャン完了ダーティV1） | スキャン | 情報 |
| 1250 | SCAN_FAILED_V1 | スキャン | エラー |
| 1300 | 検出_V1 | 検出 | 情報 |
| 1310 | 検疫_成功_V1 | Quarantine | 情報 |
| 1311 | QUARANTINE_FAILED_V1（隔離エラーV1） | Quarantine | エラー |
| 1320 | EXECUTION_BLOCK_V1（実行ブロック数） | 実行ブロック | 情報 |
| 1321 | EXECUTION_BLOCK_BAD_PARENT_V1（実行ブロックの不正な親のバージョン） | 実行ブロック | 情報 |
| 1700 | WMI_RECON_V1 | WMIReconの略 | 情報 |

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。