# 高度な脅威ソリューションのトラブルシューティングリファレンスガイド

## 内容

## はじめに

このドキュメントでは、Cisco Secure Endpoint、Cisco Secure Malware Analytics、Cisco Threat Response(CTR)、Cisco SecureXなどの製品のAdvanced Threat Solutions(ATS)ドキュメントのリンクについて説明します。

## 前提条件

### 要件

このドキュメントに関する固有の要件はありません。

### 使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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。

## 背景説明

次の記事は、高度な脅威ソリューション製品の設定およびトラブルシューティングに関するリファレンスガイドです。この記事は、Cisco TACに問い合わせる前に参照できます。

## Cisco Secure Endpointドキュメントのリンク

| 製品ポータル | 関連記事 | タグ |
|---|---|---|
| パブリッククラウド<br><br>USクラウド<br>EUクラウド<br>APJCクラウド | 一般文書 | Documentation |
| | 適切なSecure EndpointおよびSecure Malware Analytics操作に必要なサーバアドレス | Configuration |
| | セキュアエンドポイントコネクタのサポートポリシー | Documentation |
| | シスコセキュリティアカウントユーザガイド | Documentation |
| | セキュアエンドポイントでの2要素認証の設定 | Configuration |
| | セキュアなエンドポイントの導入方法とベストプラクティス | Configuration |

| | | | |
|---|---|---|---|
| | セキュアエンドポイントの権限 | | Configuration |
| | シスコセキュリティアカウントのセキュアサインオンの有効化 | | Configuration |
| | セキュアなエンドポイント通知Eメール | | Configuration |
| | Secure Endpointでの除外の設定と管理 | ビデオ | Configuration |
| | シスコが保持するセキュアエンドポイントコンソールの除外リストの変更 | | Configuration |
| | Secure Endpoint の除外に関するベストプラクティス | | Configuration |
| | セキュアエンドポイントポータルでの簡単なカスタム検出リストの設定 | | Configuration |
| | エンドポイントコンソールと最後に確認したフィルタの保護 | | Troubleshooting |
| | APIを使用したSecure Endpoint Portalからのアプリケーションブロックリストのエクスポート | | Configuration |
| | セキュアエンドポイントAPIを使用したイベントストリームの作成方法 | | Configuration |
| | Secure Endpoint PortalからSecure Malware Analyticsにファイルを送信する方法 | | Troubleshooting |
| | セキュアなエンドポイントの導入でOrbitalの高度な検索をオプトインして有効にする | | Documentation |
| | TETRA定義の更新失敗のトラブルシューティング | | Troubleshooting |
| | Splunkによるセキュアなエンドポイントの統合 | | Configuration |
| | セキュアエンドポイントでのポップアップ通知の設定 | | Configuration |
| | Secure Endpointでの誤検出ファイル分析イベントのトラブルシューティング | | Troubleshooting |
| | セキュアエンドポイント – エラーで満たされる軌道ログ – CSCwh73163 | | Documentation |
| | Secure Endpoint on AWS Workspaces – ゴールデンイメージのスタートアップおよびセットアップスクリプト | | Configuration |

| | | |
|---|---|---|
| | 安全なエンドポイント調査スナップショット情報 | Configuration |
| | セキュアエンドポイント(CSE)Windowsスキャンの確認 | Documentation |

| | | |
|---|---|---|
| | | |
| | | |
| Android コネクタ | Androidデバイスでセキュアエンドポイントのトラブルシューティングデータを取得する | Troubleshooting |
| | セキュアエンドポイントのAndroidコネクタのOS互換性 | Documentation |
| | | |
| iOSの明確さ | CiscoセキュリティコネクタApple iOSとの互換性 | Documentation |
| | セキュアエンドポイントCisco Security Connectorからの問題/診断レポートの作成 | Troubleshooting |
| | Cisco Security Connector(CSC)で使用するiOSデバイスを監視する方法 | Troubleshooting |
| | | |
| Windowsコネクタ | Windows上で動作するセキュアエンドポイントコネクタからの診断データの収集 | Troubleshooting |
| | セキュアエンドポイントWindows Connector OSの互換性 | Documentation |
| | セキュアエンドポイントのWindows Connector更新プログラムの再起動の要件 | Documentation |
| | セキュアエンドポイントコネクタバージョンのサポート終了のお知らせ | Documentation |
| | Secure Endpoint Connectorに関するWindows XP、Windows Vista、およびWindows 2003のサポート終了のお知らせ | Documentation |
| | 新しいSecure Endpoint Packageに関する2020年1月8日現在の既存のお客様に対するFAQ | Documentation |
| | セキュアエンドポイントでのWindowsポリシーの設定 ビデオ | Configuration |
| | [外部] – セキュアエンドポイントコネクタインストーラのコマンドラインスイッチ | Configuration |

| | | | |
|---|---|---|---|
| | 安全なエンドポイントコマンドラインスイッチ | | Configuration |
| | TETRA定義の更新を手動で強制実行 – セキュアエンドポイント | ビデオ | Troubleshooting |
| | Secure Endpoint Update Serverの設定手順 | | Configuration |
| | 起動時のセキュアエンドポイントの問題をトラブルシューティングするためのProcMon口グの収集方法 | | Troubleshooting |
| | Cisco Secure Endpointでの高度なカスタム検出リストの作成 | | Troubleshooting |
| | セキュアなエンドポイントの診断バンドルを分析してCPU使用率を高くする | | Troubleshooting |
| | セキュアエンドポイントのWindowsコネクタをセーフモードでアンインストールする方法 | | Troubleshooting |
| | パスワードを忘れた場合にセキュアエンドポイントコネクタをアンインストールする手順 | | Troubleshooting |
| | セキュアエンドポイントコネクタの回避策 – セキュアエンドポイントの前にWindowsプロセスが開始される | | Configuration |
| | EMETとのセキュアエンドポイントの悪用の防止エンジンの互換性 | | Configuration |
| | 不正利用の防止 | | Documentation |
| | ID永続化に関するCisco Secure Endpointガイド | | Configuration |
| | Windowsでのセキュアエンドポイントのインストールに必要なルート証明書のリスト | | Troubleshooting |
| | Secure Endpoint Windows Connectorインストーラーの終了コード | | Documentation |
| | セキュアエンドポイントでのスクリプト保護のトラブルシューティング | | Troubleshooting |
| | VMWare環境におけるデバイス制御の制限 | | Troubleshooting |
| | 3000エラーを伴うTETRA定義の更新エラーのトラブルシューティング | | Troubleshooting |
| | カスタム検出の設定 – WindowsのClamAV | | Configuration |

| | | | |
|---|---|---|---|
| | SIGTOOL.EXEによる高度な検出 | | |
| | Secure Client Full\|Network Installウィザードのインストールに関する問題のトラブルシューティング | | Troubleshooting |
| | | | |
| Linuxコネクタ | Secure Endpoint Linuxコネクタからの診断データの収集 | | Troubleshooting |
| | セキュアエンドポイントLinuxコネクタOSの互換性 | | Documentation |
| | セキュアエンドポイントLinuxコネクタの更新リブート要件 | | Documentation |
| | セキュアエンドポイントLinuxコネクタのインストール | ビデオ | Configuration |
| | LinuxのセキュアエンドポイントClamAVウイルス定義オプション | | Configuration |
| | Cisco Secure Endpoint Mac/LinuxのCLI | | Configuration |
| | セキュアエンドポイントLinuxコネクタの障害 | | Troubleshooting |
| | セキュアエンドポイントLinuxコネクタの基本的なトラブルシューティングガイド | | Troubleshooting |
| | セキュアエンドポイントLinux入門 | | Documentation |
| | Ubuntu上のセキュアエンドポイントLinuxコネクタ | | Configuration |
| | Ubuntu 20.04.0 LTSおよびUbuntu 20.04.1 LTS上のセキュアエンドポイントLinuxコネクタ1.15.0に関するアドバイザリ | | Documentation |
| | Linuxカーネル開発の障害 | | Troubleshooting |
| | セキュアエンドポイントLinuxコネクタの長期サポート | | Documentation |
| | セキュアエンドポイントLinuxコネクタ障害のトラブルシューティング18 | | Troubleshooting |
| | | | |
| Macコネクタ | Mac診断データ収集用セキュアエンドポイントコネクタ | | Troubleshooting |
| | セキュアエンドポイントのMacコネクタの | | Documentation |

| | | |
|---|---|---|
| | OS互換性 | |
| | macOS Secure Endpoint Diagnosticバンドルのcpu高使用率の分析 | Troubleshooting |
| | macOSおよびLinuxでのセキュアエンドポイントプロセスの除外 | Configuration |
| | セキュアエンドポイントMacコネクタのパフォーマンスチューニングガイド | Troubleshooting |
| | コンソールでのMACカーネルとフルディスクアクセス – セキュアエンドポイント | Troubleshooting |
| | セキュアエンドポイントMacコネクタの手動アンインストール手順 | Configuration |
| | macOS 11(Big Sur)、macOS 10.15(Catalina)、およびmacOS 10.14(Mojave)でのセキュアエンドポイントMacコネクタ1.14に関するアドバイザリ | Configuration |
| | セキュアエンドポイントMacコネクタの障害 | Troubleshooting |
| | | |
| プライベートクラウド | 一般文書 | Documentation |
| | セキュアエンドポイントプライベートクラウドサポートポリシー | Documentation |
| | セキュアエンドポイント仮想プライベートクラウドのインストールと設定 | Documentation |
| | セキュアエンドポイントのプライベートクラウドPC3000の再イメージングとバックアップの復元 | Configuration |
| | セキュアエンドポイントプライベートクラウド3.x以降のインストールに必要な証明書の生成と追加 | Configuration |
| | AirGapped Secure Endpoint Private Cloud（仮想およびアプライアンス）のアップグレード手順 | Configuration |
| | セキュアエンドポイントのプライベートクラウドサポートスナップショットを生成し、ライブサポートセッションを有効にする | Troubleshooting |
| | SSH経由でのSecure Endpoint Private CloudのCLIへのアクセスおよびSCP経由でのファイル転送 | Configuration |
| | Secure Endpoint Private Cloud 3.0.1のアップグレード手順 | Documentation |

| | | |
|---|---|---|
| | | |
| | Secure Endpoint Private Cloud 3.1.1へのアップグレード – ディスク領域とメモリの追加 | Documentation |
| | セキュアエンドポイントプライベートクラウドバージョンの販売終了のお知らせ | Documentation |
| | | |
| 有効性/修復/コンプライアンス | アウトブレイク/感染（インシデント対応） | Documentation |
| | | |

## Cisco Secure Malware Analyticsアプライアンス

| 製品ポータル | 関連記事 | タグ |
|---|---|---|
| Cisco Secure Malware Analyticsアプライアンス | 設定ガイド | Documentation |
| | インストールおよびアップグレード ガイド | Documentation |
| | Secure Malware Analyticsアプライアンスシステムバージョン | Documentation |
| | 販売終了とサポート終了の通知 | Documentation |
| | クラスタ運用のためのセキュアなマルウェア分析アプライアンスの設定 | Configuration |
| | セキュアマルウェア分析サポートスナップショットを生成し、ライブサポートセッションを有効にする | Troubleshooting |
| | Cisco Secure Malware AnalyticsアプライアンスのSSHクライアントのセットアップ | Configuration |
| | セキュアマルウェア分析アプライアンスのエアギャップモードの更新 | Configuration |
| | セキュアマルウェア分析サポートスナップショットを生成し、ライブサポートセッションを有効にする | Configuration |
| | Prometheusモニタリングソフトウェアを使用したセキュアマルウェア分析アプライアンスの設定 | Configuration |
| | EFIシェルを使用してセキュアマルウェア分析アプライアンスをリカバリモードに起動し、リカバリモードをブートオプションに追加す | Configuration |

| | | |
|---|---|---|
| | る方法 | |
| | セキュアマルウェア分析アプライアンスのエアギャップモードの更新 | Configuration |
| | コンソールおよびOPadminポータルのDTLS認証でのセキュアマルウェア分析RADIUSの設定 | Configuration |
| | セキュアなマルウェア分析アプライアンスのサードパーティ統合の設定 | Configuration |
| | Secure Malware Analyticsアプライアンスダッシュボードに表示されないサンプルとデバイスのトラブルシューティング | Configuration |
| | Secure Malware AnalyticsアプライアンスとFMCの統合のトラブルシューティング | Configuration |
| | セキュアマルウェア分析のビデオ再生リスト | Video |
| | | |

## Cisco SecureX

| 製品ポータル | 関連記事 | タグ |
|---|---|---|
| Cisco SecureX<br><br>USクラウド<br>EUクラウド<br>APJCクラウド | 設定ガイド | Documentation |
| | SecureXリファレンスガイド | Configuration |
| | SecureXブログ | Documentation |
| | SecureXに関するFAQ | Documentation |
| | Cisco Live On-Demandライブラリ | Video |
| | Cisco SecureXのビデオ再生リスト | Video |
| | | |
| SecureX脅威対応 | CTRとセキュアなマルウェア分析の統合 | Configuration |
| | Cisco Threat ResponseとFirepowerの統合 | Configuration |
| | FMCとCTRの統合に関するトラブルシュー | |

| | | | |
|---|---|---|---|
| [旧称Cisco Threat Response(CTR)]<br><br>USクラウド<br>EUクラウド<br>APJCクラウド | ティング | | Configuration |
| | Cisco Threat Response(CTR)とESAの統合 | ビデオ | Configuration |
| | ESA：ファイルレピュテーションとファイル分析 | | Configuration |
| | WSAとCTRの統合 | | Configuration |
| | CTRに関するFAQ | | Configuration |
| | Cisco Threat Response設定のチュートリアル | | Configuration |
| | Cisco Threat Responseビデオプレイリスト | | Video |
| | | | |
| SecureXオーケストレータ<br><br>USクラウド<br>EUクラウド<br>APJCクラウド | SecureXオーケストレーションチュートリアル | | Documentation |
| | 自動化の検討：シスココミュニティ | | Configuration<br>Troubleshooting |
| | ActionOrchestratorContent - Github | | Documentation |
| | | | |

## 統合に関する記事

| 製品ポータル | 関連記事 | タグ |
|---|---|---|
| Cisco Secure Endpoint<br><br>USクラウド<br>EUクラウド<br>APJCクラウド | セキュアエンドポイントのFMCへの統合 | Configuration |
| | AnyConnect 4.x および AMP イネーブラを介した AMP モジュールのインストールと設定 | Configuration |
| | ESA/CES – クラスタ化アプライアンスをセキュアエンドポイントに登録する手順 | Configuration |

| | | |
|---|---|---|
| | セキュアエンドポイントとセキュアマルウェア分析をWSAと統合 | Configuration |
| | | |
| Cisco SecureX Malware Analytics<br><br>USクラウド<br>EUクラウド | 包括的でセキュアなマルウェア分析の統合 | Configuration |
| | コンテンツセキュリティアプライアンス(ESA、SMA、WSA)およびDC/FMCのファイル分析クライアントID | Troubleshooting |
| | | |
| 認識脅威分析/<br><br>グローバル脅威アラート<br><br>(CTA) | セキュアエンドポイントを使用したCTAデモ | Configuration |
| | セキュアエンドポイントグローバル脅威アラート(GTA)サービス終了に関するFAQ | Documentation |
| | | |

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。