Guide de référence de dépannage Advanced Threat Solutions

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Liens vers la documentation Cisco Secure Endpoint
  - Portails de produits
  - Articles associés
  - Étiquettes
  - Cloud public
  - Connecteur Android
  - Clarté de Cisco IOS®
  - Connecteur Windows
  - Connecteur Linux
  - Connecteur Mac
  - Cloud privé
  - Efficacité/Correction/Conformité
- Appareil Cisco Secure Malware Analytics
  - Portails de produits
  - Articles associés
  - Étiquettes
  - Appareil Cisco Secure Malware Analytics
- Articles associés aux intégrations
  - Portails de produits
  - Articles associés
  - Étiquettes
    - Terminaux sécurisés Cisco
    - Analyse des programmes malveillants sécurisés Cisco

Introduction

Ce document décrit les liens de la documentation Advanced Threat Solutions (ATS) pour plusieurs produits de sécurité.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Ce document couvre des produits de sécurité tels que Cisco Secure Endpoint, Cisco Secure Malware Analytics, Cisco Threat Response (CTR) et Cisco SecureX. Il s'agit d'un guide de référence pour la configuration et le dépannage des produits Advanced Threat Solutions. Utilisez cette ressource avant d'engager le TAC Cisco.

Liens vers la documentation Cisco Secure Endpoint

Portails de produits	Articles associés	Étiquettes
Cloud public nuage US nuage de l'UE Cloud APJC	Documentation générale	Documentation
	Installation, configuration et désinstallation de Secure Endpoint Connector pour Windows	Configuration
	Adresses de serveur requises pour des opérations d'analyse sécurisées des terminaux et des programmes malveillants	Configuration
	Politique de prise en charge du connecteur Secure Endpoint	Documentation
	Méthodologie et bonnes pratiques de déploiement des terminaux sécurisés	Configuration

	Autorisation pour Secure Endpoint	Configuration
	E-mails de notification de terminal sécurisé	Configuration
	Configuration et gestion des exclusions dans Secure Endpoint - Vidéo	Configuration Video
	Modifications apportées à la liste d'exclusion de Cisco pour Secure Endpoint Console	Configuration
	Meilleures pratiques pour les exclusions de terminaux sécurisés	Configuration
	Configurer une liste de détection personnalisée simple sur le portail Secure Endpoint	Configuration
	Secure Endpoint Console et le dernier filtre visible	Troubleshooting
	Exporter une liste de blocage d'application depuis Secure Endpoint Portal avec des API	Configuration Troubleshooting
	Création d'un flux d'événements avec des API Secure Endpoint	Configuration Troubleshooting
	Comment envoyer un fichier dans Secure Malware Analytics à partir du portail Secure Endpoint ?	Troubleshooting
	Opt-In et Enable Orbital Advanced Search dans votre déploiement de terminaux sécurisés	Documentation
	Dépannage des échecs de mise à jour des définitions TETRA	Troubleshooting
	Intégration sécurisée des terminaux avec Splunk	Configuration
	Configuration de la notification contextuelle dans Secure Endpoint	Configuration
	Dépannage des événements d'analyse de fichiers faux positifs dans Secure Endpoint	Troubleshooting
	Point d'accès sécurisé - Journaux orbitaux remplis d'erreurs - ID de bogue Cisco CSCwh73163	Documentation
	Secure Endpoint sur les espaces de travail AWS - Scripts de démarrage et de configuration pour Golden Images	Configuration
	Informations sur le snapshot de	Configuration

	sécurité des terminaux	
	Analyse des analyses Windows de Secure Endpoint (CSE)	Documentation
	Identifier les conditions de déclenchement des actions automatisées sur les terminaux sécurisés	Documentation
Connecteur Android	Obtenir des données de dépannage sur un appareil Android pour un terminal sécurisé	Troubleshooting
	Compatibilité du SE avec Secure Endpoint Android Connector	Documentation
Clarté de Cisco IOS®	Connecteur de sécurité Cisco Compatibilité Apple iOS	Documentation
	Créer un rapport de problème / des données de diagnostic à partir de Secure Endpoint Cisco Security Connector	Troubleshooting
	Comment superviser un périphérique iOS à utiliser avec le connecteur de sécurité Cisco (CSC) ?	Troubleshooting
Connecteur Windows	Collecte de données de diagnostic à partir d'un connecteur de terminal sécurisé exécuté sous Windows	Troubleshooting
	Compatibilité du système d'exploitation du connecteur Windows Secure Endpoint	Documentation
	Configuration requise pour le redémarrage de Secure Endpoint Windows Connector Update	Documentation
	Annonce de fin de prise en charge des versions Secure Endpoint Connector	Documentation
	Annonce de fin de prise en charge de Windows XP, Windows Vista et Windows 2003 pour le connecteur de terminal sécurisé	Documentation
	FAQ pour les clients existants à partir du 8 janvier 2020 concernant les nouveaux packages de terminaux sécurisés	Documentation

	Configuration de la stratégie Windows dans Secure Endpoint - Vidéo	Configuration Video
	[Externe] - Commutateurs de ligne de commande pour le programme d'installation du connecteur Secure Endpoint	Configuration
	Commutateurs de ligne de commande Secure Endpoint	Configuration
	Forcer manuellement la mise à jour des définitions TETRA - Terminaux sécurisés - Vidéo	Troubleshooting Video
	Étapes de configuration du serveur Secure Endpoint Update	Configuration
	Comment collecter les journaux ProcMon pour résoudre les problèmes liés aux terminaux sécurisés au démarrage	Troubleshooting
	Créer une liste de détection personnalisée avancée dans Cisco Secure Endpoint	Troubleshooting
	Analyser le bundle de diagnostic Secure Endpoint pour une CPU élevée	Troubleshooting
	Comment désinstaller le connecteur Windows Secure Endpoint en mode sans échec	Troubleshooting
	Procédure de désinstallation du connecteur Secure Endpoint si le mot de passe est oublié	Troubleshooting
	Processus Windows démarre avant la solution de contournement Secure Endpoint Connector - Secure Endpoint	Configuration
	Compatibilité du moteur Secure Endpoint Exploit Prevention Engine avec EMET	Configuration
	Prévention des exploits	Documentation
	Guide Cisco Secure Endpoint sur la persistance de l'identité	Configuration
	Liste des certificats racine requis pour l'installation de Secure Endpoint sous Windows	Troubleshooting
	Codes de sortie du programme d'installation du connecteur Windows Secure Endpoint	Documentation
	Dépannage de la protection des scripts	Troubleshooting

	dans Secure Endpoint	
	Limites du contrôle des périphériques dans les environnements VMWare	Troubleshooting
	Dépannage de l'échec de mise à jour des définitions TETRA avec erreur 3000	Troubleshooting
	Configuration de détections personnalisées - Avancé avec ClamAV SIGTOOL.EXE sous Windows	Configuration
	Résolution des problèmes d'installation de Secure Client Full|Network Install Wizard	Troubleshooting
	Configurer une heure personnalisée pour les téléchargements TETRA	Configuration
Connecteur Linux	Collecte de données de diagnostic à partir du connecteur Linux Secure Endpoint	Troubleshooting
	Compatibilité du système d'exploitation avec Secure Endpoint Linux Connector	Documentation
	Configuration requise pour le redémarrage du connecteur Secure Endpoint Linux	Documentation
	Installation du connecteur Linux pour terminal sécurisé - Vidéo	Configuration Video
	Options de définition de virus ClamAV Secure Endpoint sous Linux	Configuration
	CLI pour Mac/Linux Cisco Secure Endpoint	Configuration
	Défaillances du connecteur Linux du terminal sécurisé	Troubleshooting
	Résoudre le problème de stratégie Linux Connector SE Linux	Troubleshooting
	Guide de dépannage de base du connecteur Linux pour terminal sécurisé	Troubleshooting
	Initiation Linux sur les terminaux sécurisés	Documentation Configuration
	Connecteur Linux de terminal sécurisé sur Ubuntu	Configuration
	Conseil pour le connecteur Linux Secure Endpoint 1.15.0 sur Ubuntu 20.04.0 LTS et Ubuntu 20.04.1 LTS	Documentation

	Défaillance du noyau Linux	Troubleshooting
	Prise en charge à long terme du connecteur Linux pour terminal sécurisé	Documentation
	Dépannage de la défaillance du connecteur Linux Secure Endpoint 18	Troubleshooting
	Dépannage de l'ID de panne 11 sur le terminal sécurisé SUSE Linux	Troubleshooting
Connecteur Mac	Connecteur de terminal sécurisé pour la collecte de données de diagnostic Mac	Troubleshooting
	Compatibilité du système d'exploitation du connecteur Mac pour terminal sécurisé	Documentation
	Analyser l'offre groupée de diagnostic macOS Secure Endpoint pour CPU élevé	Troubleshooting
	Exclusions des processus de terminaux sécurisés dans macOS et Linux	Configuration
	Guide de réglage des performances du connecteur Mac pour terminal sécurisé	Troubleshooting
	Noyau MAC et accès complet au disque dans la console - point d'extrémité sécurisé	Troubleshooting
	Procédure de désinstallation manuelle du connecteur Mac de terminal sécurisé	Configuration
	Conseil pour le connecteur Mac Secure Endpoint 1.14 sur macOS 11 (Big Sur), macOS 10.15 (Catalina) et macOS 10.14 (Mojave)	Configuration Troubleshooting
	Défaillances du connecteur Mac du terminal sécurisé	Troubleshooting
	Configuration des autorisations pour le connecteur Mac et l'orbite des terminaux sécurisés avec MDM : Accès complet au disque, extensions système	Configuration
	Guide d'installation de Secure Endpoint Mac Proxy Automatic	Configuration

	Configuration (PAC)	
Cloud privé	Documentation générale	Documentation
	Politique de support du cloud privé Secure Endpoint	Documentation
	Installation et configuration d'un cloud privé virtuel pour terminaux sécurisés	Documentation
	Re-image du cloud privé de point de terminaison sécurisé PC3000 et restauration de la sauvegarde	Configuration
	Générer et ajouter les certificats requis pour l'installation du cloud privé Secure Endpoint à partir de 3.x	Configuration
	Procédure de mise à niveau pour le cloud privé AirGapped Secure Endpoint (virtuel et matériel)	Configuration
	Générer un snapshot de prise en charge du cloud privé Secure Endpoint et activer la session de prise en charge dynamique	Troubleshooting
	Accès à l'interface de ligne de commande du cloud privé Secure Endpoint via SSH et transfert de fichiers via SCP	Configuration
	Procédure de mise à niveau de Secure Endpoint Private Cloud 3.0.1	Documentation
	Mise à niveau vers Secure Endpoint Private Cloud 3.1.1 - ajout d'espace disque et de mémoire	Documentation
	Annonce EOS pour les versions de cloud privé Secure Endpoint	Documentation
	Cloud privé de terminal sécurisé - Expiration des certificats d'authentification 2024	Documentation
	Dépannage du flux d'événements sur le cloud privé	Troubleshooting
	Point de terminaison sécurisé - Expiration du certificat CA racine du cloud privé 2023	Documentation
	Installation et configuration d'un cloud privé virtuel de point de terminaison	Configuration

	sécurisé	
Efficacité/Correction/Conformité	Épidémie/Infection (Réponse à l'incident)	Documentation Troubleshooting

Appareil Cisco Secure Malware Analytics

Portails de produits	Articles associés	Étiquettes
Appareil Cisco Secure Malware Analytics	Guides de configuration	Documentation Configuration
	Guides d'installation et de mise à niveau	Documentation
	Version du système Secure Malware Analytics Appliance	Documentation
	Annonce de fin de commercialisation et de fin de vie	Documentation
	Configurer l'appliance Secure Malware Analytics pour les opérations de cluster	Configuration
	Générer un snapshot de support Secure Malware Analytics et activer la session de support en direct	Troubleshooting
	Configuration du client SSH pour Cisco Secure Malware Analytics Appliance	Configuration
	Mettre à jour le mode Secure Malware Analytics Appliance Air-Gap	Configuration
	Générer un snapshot de support Secure Malware Analytics et activer la session de support en direct	Configuration
	Configurer l'appliance Secure Malware Analytics avec le logiciel de surveillance Prometheus	Configuration
	Comment démarrer l'appliance Secure Malware Analytics en mode de récupération avec EFI Shell et ajouter le mode de récupération aux options de démarrage	Configuration
	Mettre à jour le mode Secure Malware Analytics Appliance Air-Gap	Configuration Troubleshooting
	Configurer l'authentification RADIUS Secure Malware Analytics sur DTLS pour la console	Configuration

	et le portail OPadmin	
	Configuration des intégrations tierces de l'appliance Secure Malware Analytics	Configuration
	Dépannage des exemples et des périphériques absents du tableau de bord du dispositif Secure Malware Analytics	Configuration Troubleshooting
	Dépannage de l'intégration de Secure Malware Analytics Appliance avec FMC	Configuration Troubleshooting
	Liste de lecture vidéo Secure Malware Analytics	Video
	Configurer l'appliance Secure Malware Analytics avec Umbrella	Configuration
	Résolution du problème de configuration initiale de Secure Malware Analytics Appliance	Troubleshooting
	L'appliance Secure Malware Analytics n'accepte pas le certificat CA	Troubleshooting
	Secure Malware Analytics Appliance indique qu'une réinitialisation requise doit être effectuée avant l'installation de la version 3.0	Troubleshooting
	Comment télécharger les certificats à partir de l'appliance Secure Malware Analytics (auto-signée) à des fins d'intégration ?	Configuration
	Utilisation d'un équilibreur de charge externe avec un cluster Secure Malware Analytics Appliance	Configuration

Articles associés aux intégrations

Portails de produits	Articles associés	Étiquettes
Terminaux sécurisés Cisco nuage US nuage de l'UE Cloud APJC	Intégration de Secure Endpoint avec FMC	Configuration
	Installation et configuration du module AMP via AnyConnect 4.x et AMP Enabler	Configuration
	ESA/CES - Procédure d'enregistrement des appliances en cluster sur Secure Endpoint	Configuration
	Intégration du cloud privé virtuel AMP et de l'appliance Threat Grid	Configuration

	Intégrer Secure Endpoint et Secure Malware Analytics avec WSA	Configuration
Analyse des programmes malveillants sécurisés Cisco nuage US nuage de l'UE	Intégration d'Umbrella et Secure Malware Analytics	Configuration
	ID client d'analyse de fichiers sur les dispositifs de sécurité du contenu (ESA, SMA, WSA) et DC/FMC	Troubleshooting
	IP et ports requis pour Secure Malware Analytics	Configuration

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.