

# 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 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](#)

[Cisco SecureX](#)

[Portails de produits](#)

[Articles associés](#)

[Étiquettes](#)

[Cisco SecureX](#)

[Réponse aux menaces SecureX](#)

[SecureX Orchestrator](#)

[Articles associés aux intégrations](#)

[Portails de produits](#)

[Articles associés](#)

[Étiquettes](#)

[Terminaux sécurisés Cisco](#)

[Analyse des programmes malveillants sécurisés Cisco](#)

[Analyse cognitive des menaces /](#)

[Alertes de menaces globales](#)

# Introduction

Ce document décrit les liens de la documentation Advanced Threat Solutions (ATS) pour des produits tels que Cisco Secure Endpoint, Cisco Secure Malware Analytics, Cisco Threat Response (CTR) et Cisco SecureX.

## 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

L'article suivant est un guide de référence pour la configuration et le dépannage des produits Advanced Threat Solutions. Vous pouvez consulter cet article avant d'engager le TAC Cisco.

## Liens vers la documentation Cisco Secure Endpoint

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

	<a href="#">E-mails de notification de terminal sécurisé</a>	Configuration
	<a href="#">Configuration et gestion des exclusions dans Secure Endpoint</a>	<a href="#">Vidéo</a> Configuration
	<a href="#">Modifications apportées à la liste d'exclusion de Cisco pour Secure Endpoint Console</a>	Configuration
	<a href="#">Meilleures pratiques pour les exclusions de terminaux sécurisés</a>	Configuration
	<a href="#">Configurer une liste de détection personnalisée simple sur le portail Secure Endpoint</a>	Configuration
	<a href="#">Secure Endpoint Console et le dernier filtre visible</a>	Troubleshooting
	<a href="#">Exporter une liste de blocage d'application depuis Secure Endpoint Portal avec des API</a>	Configuration
	<a href="#">Création d'un flux d'événements avec des API Secure Endpoint</a>	Configuration
	<a href="#">Comment envoyer un fichier dans Secure Malware Analytics à partir du portail Secure Endpoint ?</a>	Troubleshooting
	<a href="#">Opt-In et Enable Orbital Advanced Search dans votre déploiement de terminaux sécurisés</a>	Documentation
	<a href="#">Dépannage des échecs de mise à jour des définitions TETRA</a>	Troubleshooting
	<a href="#">Intégration sécurisée des terminaux avec Splunk</a>	Configuration
	<a href="#">Configuration de la notification contextuelle dans Secure Endpoint</a>	Configuration
	<a href="#">Dépannage des événements d'analyse de fichiers faux positifs dans Secure Endpoint</a>	Troubleshooting
	<a href="#">Terminal sécurisé - Les journaux orbitaux se remplissent d'erreurs - CSCwh73163</a>	Documentation
	<a href="#">Secure Endpoint sur les espaces de travail AWS - Scripts de démarrage et de</a>	Configuration

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

<a href="#">Windows dans Secure Endpoint</a>	<a href="#">Vidéo</a>	
<a href="#">[Externe] - Commutateurs de ligne de commande pour le programme d'installation du connecteur Secure Endpoint</a>		Configuration
<a href="#">Commutateurs de ligne de commande Secure Endpoint</a>		Configuration
<a href="#">Forcer manuellement la mise à jour des définitions TETRA - Secure Endpoint</a>	<a href="#">Vidéo</a>	Troubleshooting
<a href="#">Étapes de configuration du serveur Secure Endpoint Update</a>		Configuration
<a href="#">Comment collecter les journaux ProcMon pour résoudre les problèmes liés aux terminaux sécurisés au démarrage</a>		Troubleshooting
<a href="#">Créer une liste de détection personnalisée avancée dans Cisco Secure Endpoint</a>		Troubleshooting
<a href="#">Analyser le bundle de diagnostic Secure Endpoint pour une CPU élevée</a>		Troubleshooting
<a href="#">Comment désinstaller le connecteur Windows Secure Endpoint en mode sans échec</a>		Troubleshooting
<a href="#">Procédure de désinstallation du connecteur Secure Endpoint si le mot de passe est oublié</a>		Troubleshooting
<a href="#">Processus Windows démarre avant la solution de contournement Secure Endpoint Connector - Secure Endpoint</a>		Configuration
<a href="#">Compatibilité du moteur Secure Endpoint Exploit Prevention Engine avec EMET</a>		Configuration
<a href="#">Prévention des exploits</a>		Documentation

	<a href="#">Guide Cisco Secure Endpoint sur la persistance de l'identité</a>	Configuration	
	<a href="#">Liste des certificats racine requis pour l'installation de Secure Endpoint sous Windows</a>	Troubleshooting	
	<a href="#">Codes de sortie du programme d'installation du connecteur Windows Secure Endpoint</a>	Documentation	
	<a href="#">Dépannage de la protection des scripts dans Secure Endpoint</a>	Troubleshooting	
	<a href="#">Limites du contrôle des périphériques dans les environnements VMWare</a>	Troubleshooting	
	<a href="#">Dépannage de l'échec de mise à jour des définitions TETRA avec erreur 3000</a>	Troubleshooting	
	<a href="#">Configuration de détections personnalisées - Avancé avec ClamAV SIGTOOL.EXE sous Windows</a>	Configuration	
	<a href="#">Résolution des problèmes d'installation de Secure Client Full Network Install Wizard</a>	Troubleshooting	
	<a href="#">Configurer une heure personnalisée pour les téléchargements TETRA</a>	Configuration	
Connecteur Linux	<a href="#">Collecte de données de diagnostic à partir du connecteur Linux Secure Endpoint</a>	Troubleshooting	
	<a href="#">Compatibilité du système d'exploitation avec Secure Endpoint Linux Connector</a>	Documentation	
	<a href="#">Configuration requise pour le redémarrage du connecteur Secure Endpoint Linux</a>	Documentation	
	<a href="#">Installation du connecteur Linux Secure Endpoint</a>	Vidéo	Configuration
	<a href="#">Options de définition de virus ClamAV Secure Endpoint sous Linux</a>	Configuration	
	<a href="#">CLI pour Mac/Linux Cisco Secure Endpoint</a>	Configuration	
	<a href="#">Défaillances du connecteur Linux du terminal sécurisé</a>	Troubleshooting	

	<a href="#">Résoudre le problème de stratégie Linux Connector SE Linux</a>	Troubleshooting
	<a href="#">Guide de dépannage de base du connecteur Linux pour terminal sécurisé</a>	Troubleshooting
	<a href="#">Initiation Linux sur les terminaux sécurisés</a>	Documentation
	<a href="#">Connecteur Linux de terminal sécurisé sur Ubuntu</a>	Configuration
	<a href="#">Conseil pour le connecteur Linux Secure Endpoint 1.15.0 sur Ubuntu 20.04.0 LTS et Ubuntu 20.04.1 LTS</a>	Documentation
	<a href="#">Défaillance du noyau Linux</a>	Troubleshooting
	<a href="#">Prise en charge à long terme du connecteur Linux pour terminal sécurisé</a>	Documentation
	<a href="#">Dépannage de la défaillance du connecteur Linux Secure Endpoint 18</a>	Troubleshooting
	<a href="#">Dépannage de l'ID de panne 11 sur le terminal sécurisé SUSE Linux</a>	Troubleshooting
Connecteur Mac	<a href="#">Connecteur de terminal sécurisé pour la collecte de données de diagnostic Mac</a>	Troubleshooting
	<a href="#">Compatibilité du système d'exploitation du connecteur Mac pour terminal sécurisé</a>	Documentation
	<a href="#">Analyser l'offre groupée de diagnostic macOS Secure Endpoint pour CPU élevé</a>	Troubleshooting
	<a href="#">Exclusions des processus de terminaux sécurisés dans macOS et Linux</a>	Configuration
	<a href="#">Guide de réglage des performances du connecteur Mac pour terminal sécurisé</a>	Troubleshooting
	<a href="#">Noyau MAC et accès complet au disque dans la console - point d'extrémité sécurisé</a>	Troubleshooting
	<a href="#">Procédure de désinstallation manuelle du connecteur Mac de terminal sécurisé</a>	Configuration
	<a href="#">Conseil pour le connecteur Mac Secure Endpoint 1.14 sur macOS 11 (Big Sur), macOS 10.15 (Catalina) et macOS 10.14 (Mojave)</a>	Configuration
	<a href="#">Défaillances du connecteur Mac du terminal</a>	Troubleshooting

	<a href="#">sécurisé</a>	
	<a href="#">Configuration des autorisations pour le connecteur Mac et l'orbite des terminaux sécurisés avec MDM : accès complet au disque, extensions système</a>	Configuration
	<a href="#">Guide d'installation de Secure Endpoint Mac Proxy Automatic Configuration (PAC)</a>	Configuration
Cloud privé	<a href="#">Documentation générale</a>	Documentation
	<a href="#">Politique de support du cloud privé Secure Endpoint</a>	Documentation
	<a href="#">Installation et configuration d'un cloud privé virtuel pour terminaux sécurisés</a>	Documentation
	<a href="#">Re-image du cloud privé de point de terminaison sécurisé PC3000 et restauration de la sauvegarde</a>	Configuration
	<a href="#">Générer et ajouter les certificats requis pour l'installation du cloud privé Secure Endpoint à partir de 3.x</a>	Configuration
	<a href="#">Procédure de mise à niveau pour le cloud privé AirGapped Secure Endpoint (virtuel et matériel)</a>	Configuration
	<a href="#">Générer un snapshot de prise en charge du cloud privé Secure Endpoint et activer la session de prise en charge dynamique</a>	Troubleshooting
	<a href="#">Accès à l'interface de ligne de commande du cloud privé Secure Endpoint via SSH et transfert de fichiers via SCP</a>	Configuration
	<a href="#">Procédure de mise à niveau de Secure Endpoint Private Cloud 3.0.1</a>	Documentation
	<a href="#">Mise à niveau vers Secure Endpoint Private Cloud 3.1.1 - ajout d'espace disque et de mémoire</a>	Documentation
	<a href="#">Annonce EOS pour les versions de cloud privé Secure Endpoint</a>	Documentation
	<a href="#">Cloud privé de terminal sécurisé - Expiration des certificats d'authentification 2024</a>	Documentation
	<a href="#">Dépannage du flux d'événements sur le cloud privé</a>	Troubleshooting
	<a href="#">Point de terminaison sécurisé - Expiration du</a>	Documentation



	<a href="#">certificat CA racine du cloud privé 2023</a>	
	<a href="#">Installation et configuration d'un cloud privé virtuel de point de terminaison sécurisé</a>	Configuration
Efficacité/Correction/Conformité	<a href="#">Épidémie/Infection (Réponse à l'incident)</a>	Documentation

## Appareil Cisco Secure Malware Analytics

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




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

## Cisco SecureX







Portails de produits	Articles associés	Étiquettes
Cisco SecureX <a href="#">nuage US</a> <a href="#">nuage de l'UE</a>	<a href="#">Guides de configuration</a>	Documentation
	<a href="#">Guide de référence SecureX</a>	Configuration
	<a href="#">Blogs SecureX</a>	Documentation

[FAQ SecureX](#)

<a href="#">Cloud APJC</a>		<a href="#">Documentation</a>
	<a href="#">Bibliothèque Cisco Live On-Demand</a>	<a href="#">Video</a>
	<a href="#">Liste de lecture vidéo Cisco SecureX</a>	<a href="#">Video</a>
	<a href="#">Cisco Live 2023 ! Sessions Secure Endpoint et SecureX</a>	<a href="#">Documentation</a>
Réponse aux menaces SecureX [anciennement Cisco Threat Response (CTR)] <a href="#">nuage US</a> <a href="#">nuage de l'UE</a> <a href="#">Cloud APJC</a>	<a href="#">Intégrer CTR et Secure Malware Analytics</a>	<a href="#">Configuration</a>
	<a href="#">Intégrer Cisco Threat Response et Firepower</a>	<a href="#">Configuration</a>
	<a href="#">Dépannage de l'intégration FMC et CTR</a>	<a href="#">Configuration</a>
	<a href="#">Intégration de Cisco Threat Response (CTR) et ESA</a>	<a href="#">Vidéo</a>
	<a href="#">ESA : Réputation des fichiers et analyse des fichiers</a>	<a href="#">Configuration</a>
	<a href="#">Intégration de WSA avec CTR</a>	<a href="#">Configuration</a>
	<a href="#">FAQ CTR</a>	<a href="#">Configuration</a>
	<a href="#">Didacticiels de configuration de Cisco Threat Response</a>	<a href="#">Configuration</a>
	<a href="#">Liste de lecture vidéo Cisco Threat Response</a>	<a href="#">Video</a>
SecureX Orchestrator	<a href="#">Didacticiel d'orchestration SecureX</a>	<a href="#">Documentation</a>

<a href="#">nuage US</a> <a href="#">nuage de l'UE</a> <a href="#">Cloud APJC</a>	<a href="#">Communauté Cisco</a>	  
	<a href="#">ContenuActionOrchestrator - Github</a>	

## Articles associés aux intégrations

Portails de produits	Articles associés	Étiquettes
Terminaux sécurisés Cisco  <a href="#">nuage US</a> <a href="#">nuage de l'UE</a> <a href="#">Cloud APJC</a>	<a href="#">Intégration de Secure Endpoint avec FMC</a>	
	<a href="#">Installation et configuration du module AMP via AnyConnect 4.x et AMP Enabler</a>	
	<a href="#">ESA/CES - Procédure d'enregistrement des appliances en cluster sur Secure Endpoint</a>	
	<a href="#">Intégration du cloud privé virtuel AMP et de l'appliance Threat Grid</a>	
	<a href="#">Intégrer Secure Endpoint et Secure Malware Analytics avec WSA</a>	
Analyse des programmes malveillants sécurisés Cisco  <a href="#">nuage US</a> <a href="#">nuage de l'UE</a>	<a href="#">Intégration d'Umbrella et Secure Malware Analytics</a>	
	<a href="#">ID client d'analyse de fichiers sur les dispositifs de sécurité du contenu (ESA, SMA, WSA) et DC/FMC</a>	
	<a href="#">IP et ports requis pour Secure Malware Analytics</a>	
Analyse cognitive des menaces /	<a href="#">Démo CTA avec Secure Endpoint</a> <a href="#">FAQ sur les alertes de fin de service pour les terminaux sécurisés (GTA)</a>	

Alertes de menaces  
globales

[\(CTA\)](#)

Documentation

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.