

# Advanced Threat Solutions Troubleshooting Reference Guide

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Background Information](#)

### [Cisco Secure Endpoint Documentation links](#)

[Product Portals](#)

[Related Articles](#)

[Tags](#)

[Public Cloud](#)

[Android Connector](#)

[iOS Clarity](#)

[Windows Connector](#)

[Linux Connector](#)

[Mac Connector](#)

[Private Cloud](#)

[Efficacy/Remediation/Compliance](#)

### [Cisco Secure Malware Analytics Appliance](#)

[Product Portals](#)

[Related Articles](#)

[Tags](#)

[Cisco Secure Malware Analytics Appliance](#)

### [Cisco SecureX](#)

[Product Portals](#)

[Related Articles](#)

[Tags](#)

[Cisco SecureX](#)

[SecureX Threat Response](#)

[SecureX Orchestrator](#)

### [Integrations related articles](#)

[Product Portals](#)

[Related Articles](#)

[Tags](#)

[Cisco Secure Endpoint](#)

[Cisco Secure Malware Analytics](#)

[Cognitive Threat Analytics /](#)

[Global Threat Alerts](#)

---

# Introduction

This document describes the Advanced Threat Solutions (ATS) documentation links for products like Cisco Secure Endpoint, Cisco Secure Malware Analytics, Cisco Threat Response (CTR), and Cisco SecureX.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

This document is not restricted to specific software and hardware versions.

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. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

The following article is a reference guide for the configuration/troubleshooting of Advanced Threat Solutions products. This article can be referred to before engaging Cisco TAC.

## Cisco Secure Endpoint Documentation links

Product Portals	Related Articles	Tags
<b>Public Cloud</b> <a href="#">US Cloud</a> <a href="#">EU Cloud</a> <a href="#">APJC Cloud</a>	<a href="#">General Documentation</a>	Documentation
	<a href="#">Install, Configure and Uninstall Secure Endpoint Connector for Windows</a>	Configuration
	<a href="#">Required Server Addresses for Proper Secure Endpoint &amp; Secure Malware Analytics Operations</a>	Configuration
	<a href="#">Secure Endpoint Connector Support Policy</a>	Documentation
	<a href="#">Secure Endpoint Deployment Methodology and Best Practices</a>	Configuration
	<a href="#">Entitlement for Secure Endpoint</a>	Configuration
	<a href="#">Secure Endpoint Notification Emails</a>	Configuration
	<a href="#">Configure and Manage Exclusions in Secure Endpoint</a>	Video Configuration

	<a href="#">Cisco-Maintained Exclusion List Changes for Secure Endpoint Console</a>	Configuration
	<a href="#">Best Practices for Secure Endpoint Exclusions</a>	Configuration
	<a href="#">Configure a Simple Custom Detection List on the Secure Endpoint Portal</a>	Configuration
	<a href="#">Secure Endpoint Console and the Last Seen Filter</a>	Troubleshooting
	<a href="#">Export an Application Blocklists from the Secure Endpoint Portal with APIs</a>	Configuration
	<a href="#">How to Create an Event Stream with Secure Endpoint APIs</a>	Configuration
	<a href="#">How to Submit a File in Secure Malware Analytics from the Secure Endpoint Portal?</a>	Troubleshooting
	<a href="#">Opt-In and Enable Orbital Advanced Search in your Secure Endpoint Deployment</a>	Documentation
	<a href="#">Troubleshooting TETRA definitions update failures</a>	Troubleshooting
	<a href="#">Secure Endpoint Integration with Splunk</a>	Configuration
	<a href="#">Configure Pop-Up Notification in Secure Endpoint</a>	Configuration
	<a href="#">Troubleshoot False Positive File Analysis Events in Secure Endpoint</a>	Troubleshooting
	<a href="#">Secure Endpoint - Orbital Logs Filling Up with Errors - CSCwh73163</a>	Documentation
	<a href="#">Secure Endpoint on AWS Workspaces - Startup and Setup scripts for Golden Images</a>	Configuration
	<a href="#">Secure Endpoint Forensic Snapshot Information</a>	Configuration
	<a href="#">Review Secure Endpoint (CSE) Windows Scans</a>	Documentation
	<a href="#">Identify Conditions to Trigger Automated Actions in Secure Endpoint</a>	Documentation
	<a href="#">Obtain Troubleshoot Data on an Android</a>	Troubleshooting

<b>Android Connector</b>	<a href="#">Device for Secure Endpoint</a>		
	<a href="#">Secure Endpoint Android Connector OS Compatibility</a>		Documentation
<b>iOS Clarity</b>	<a href="#">Cisco Security Connector Apple iOS Compatibility</a>		Documentation
	<a href="#">Create Report Problem / Diagnostic data from Secure Endpoint Cisco Security Connector</a>		Troubleshooting
	<a href="#">How to Supervise an iOS Device for Use with Cisco Security Connector (CSC)?</a>		Troubleshooting
<b>Windows Connector</b>	<a href="#">Collection of Diagnostic Data from a Secure Endpoint Connector Running on Windows</a>		Troubleshooting
	<a href="#">Secure Endpoint Windows Connector OS Compatibility</a>		Documentation
	<a href="#">Secure Endpoint Windows Connector Update Reboot Requirements</a>		Documentation
	<a href="#">End-of-Support Announcement for Secure Endpoint Connector Versions</a>		Documentation
	<a href="#">End-of-Support Announcement for Windows XP, Windows Vista, and Windows 2003 for the Secure Endpoint Connector</a>		Documentation
	<a href="#">FAQ for Existing Customers as of January 8, 2020 Regarding New Secure Endpoint Packages</a>		Documentation
	<a href="#">Configure Windows Policy in Secure Endpoint</a>	Video	Configuration
	<a href="#">[External] - Command Line Switches for Secure Endpoint Connector Installer</a>		Configuration
	<a href="#">Secure Endpoint Command Line Switches</a>		Configuration
	<a href="#">Force Manually the TETRA Definitions</a>	Video	Troubleshooting




<a href="#">Update - Secure Endpoint</a>	
<a href="#">Secure Endpoint Update Server Configuration Steps</a>	Configuration
<a href="#">How to collect ProcMon logs to troubleshoot Secure Endpoint issues at startup</a>	Troubleshooting
<a href="#">Create an Advanced Custom Detection List in Cisco Secure Endpoint</a>	Troubleshooting
<a href="#">Analyze Secure Endpoint Diagnostic Bundle for High CPU</a>	Troubleshooting
<a href="#">How to Uninstall Secure Endpoint Windows Connector with Safe Mode</a>	Troubleshooting
<a href="#">Procedure to uninstall the Secure Endpoint connector if the password is forgotten</a>	Troubleshooting
<a href="#">Windows Process Starts Before Secure Endpoint Connector Workaround - Secure Endpoint</a>	Configuration
<a href="#">Secure Endpoint Exploit Prevention Engine Compatibility with EMET</a>	Configuration
<a href="#">Exploit Prevention</a>	Documentation
<a href="#">Cisco Secure Endpoint Guide to Identity Persistence</a>	Configuration
<a href="#">List of Root Certificates Required for Secure Endpoint Installation on Windows</a>	Troubleshooting
<a href="#">Secure Endpoint Windows Connector Installer Exit Codes</a>	Documentation
<a href="#">Troubleshoot Script Protection in Secure Endpoint</a>	Troubleshooting
<a href="#">Device Control limitations in VMWare Environments</a>	Troubleshooting
<a href="#">Troubleshoot TETRA Definitions Update Failure with 3000 Error</a>	Troubleshooting
<a href="#">Configure Custom Detections - Advanced with ClamAV SIGTOOL.EXE on Windows</a>	Configuration

[Troubleshoot Secure Client Full|Network  
Install Wizard Installation Issues](#)

Troubleshooting

[Configure a Custom Time for TETRA  
Downloads](#)

Configuration

<b>Linux Connector</b>	<a href="#">Collection of Diagnostic Data from Secure Endpoint Linux Connector</a>	
	<a href="#">Secure Endpoint Linux Connector OS Compatibility</a>	
	<a href="#">Secure Endpoint Linux Connector Update Reboot Requirements</a>	
	<a href="#">Installation of the Secure Endpoint Linux Connector</a>	<a href="#">Video</a>

	<a href="#">Secure Endpoint ClamAV Virus Definition Options in Linux</a>	Configuration
	<a href="#">Cisco Secure Endpoint Mac/Linux CLI</a>	Configuration
	<a href="#">Secure Endpoint Linux Connector Faults</a>	Troubleshooting
	<a href="#">Resolve Linux Connector SE Linux Policy Fault</a>	Troubleshooting
	<a href="#">Basic Troubleshoot Guide for Secure Endpoint Linux Connector</a>	Troubleshooting
	<a href="#">Secure Endpoint Linux Primer</a>	Documentation
	<a href="#">Secure Endpoint Linux Connector on Ubuntu</a>	Configuration
	<a href="#">Advisory for Secure Endpoint Linux Connector 1.15.0 on Ubuntu 20.04.0 LTS and Ubuntu 20.04.1 LTS</a>	Documentation
	<a href="#">Linux Kernel-Devel Fault</a>	Troubleshooting
	<a href="#">Secure Endpoint Linux Connector Long Term Support</a>	Documentation
	<a href="#">Troubleshoot Secure Endpoint Linux Connector Fault 18</a>	Troubleshooting
	<a href="#">Troubleshoot Fault ID 11 on SUSE Linux Secure Endpoint</a>	Troubleshooting
<b>Mac Connector</b>	<a href="#">Secure Endpoint Connector for Mac Diagnostic Data Collection</a>	Troubleshooting
	<a href="#">Secure Endpoint Mac Connector OS Compatibility</a>	Documentation
	<a href="#">Analyze macOS Secure Endpoint Diagnostic Bundle for High CPU</a>	Troubleshooting
	<a href="#">Secure Endpoint Process Exclusions in macOS and Linux</a>	Configuration
	<a href="#">Secure Endpoint Mac Connector Performance Tuning Guide</a>	Troubleshooting
	<a href="#">MAC Kernel and Full Disk Access in the Console - Secure Endpoint</a>	Troubleshooting
	<a href="#">Manual Uninstall Procedure for Secure Endpoint Mac Connector</a>	Configuration



	<a href="#">Advisory for Secure Endpoint Mac Connector 1.14 on macOS 11 (Big Sur), macOS 10.15 (Catalina), and macOS 10.14 (Mojave)</a>	Configuration
	<a href="#">Secure Endpoint Mac Connector Faults</a>	Troubleshooting
	<a href="#">Configure Permissions for Secure Endpoint Mac Connector and Orbital with MDM: Full Disk Access, System Extensions</a>	Configuration
	<a href="#">Secure Endpoint Mac Proxy Automatic Configuration (PAC) Setup Guide</a>	Configuration
<b>Private Cloud</b>	<a href="#">General Documentation</a>	Documentation
	<a href="#">Secure Endpoint Private Cloud Support Policy</a>	Documentation
	<a href="#">Installation and Configuration of Secure Endpoint Virtual Private Cloud</a>	Documentation
	<a href="#">Re-Image the Secure Endpoint Private Cloud PC3000 and Restore the Backup</a>	Configuration
	<a href="#">Generate and Add Certificates that are Required for Installation of Secure Endpoint Private Cloud 3.x Onwards</a>	Configuration
	<a href="#">Upgrade Procedure for AirGapped Secure Endpoint Private Cloud (Virtual and Appliance)</a>	Configuration
	<a href="#">Generate Secure Endpoint Private Cloud Support Snapshot and Enable Live Support Session</a>	Troubleshooting
	<a href="#">Accessing the CLI of Secure Endpoint Private Cloud via SSH and Transferring Files via SCP</a>	Configuration
	<a href="#">Secure Endpoint Private Cloud 3.0.1 upgrade procedure</a>	Documentation
	<a href="#">Upgrading to Secure Endpoint Private Cloud 3.1.1 - adding disk space and memory</a>	Documentation
	<a href="#">EOS Announcement for Secure Endpoint Private Cloud Versions</a>	Documentation

<b>Efficacy/Remediation/Compliance</b>	<a href="#">Outbreak/Infection (Incident Response)</a>	Documentation

## Cisco Secure Malware Analytics Appliance

Product Portals	Related Articles	Tags
<b>Cisco Secure Malware Analytics Appliance</b>	<a href="#">Configuration Guides</a>	Documentation
	<a href="#">Install and Upgrade Guides</a>	Documentation
	<a href="#">Secure Malware Analytics Appliance System Version</a>	Documentation
	<a href="#">End-of-Sale and End-of-Life Announcement</a>	Documentation
	<a href="#">Configure Secure Malware Analytics Appliance for Cluster Operations</a>	Configuration
	<a href="#">Generate Secure Malware Analytics Support Snapshot and Enable Live Support Session</a>	Troubleshooting
	<a href="#">Setting up SSH client for Cisco Secure Malware Analytics Appliance</a>	Configuration
	<a href="#">Update Secure Malware Analytics Appliance Air-Gap mode</a>	Configuration
	<a href="#">Generate Secure Malware Analytics Support Snapshot and Enable Live Support Session</a>	Configuration
	<a href="#">Configure Secure Malware Analytics Appliance with Prometheus Monitoring Software</a>	Configuration
	<a href="#">How to Boot Secure Malware Analytics Appliance into Recovery Mode with EFI Shell and Add Recovery Mode to Boot Options</a>	Configuration
	<a href="#">Update Secure Malware Analytics Appliance Air-Gap mode</a>	Configuration
	<a href="#">Configure Secure Malware Analytics RADIUS over DTLS Authentication for Console and OPadmin Portal</a>	Configuration
	<a href="#">Configure Secure Malware Analytics Appliance Third-Party Integrations</a>	Configuration
	<a href="#">Troubleshoot Samples and Devices Not Present in Secure Malware Analytics Appliance Dashboard</a>	Configuration

	<a href="#">Troubleshoot of Secure Malware Analytics Appliance Integration with FMC</a>	Configuration
	<a href="#">Secure Malware Analytics Video Playlist</a>	Video




## Cisco SecureX

Product Portals	Related Articles	Tags
<b>Cisco SecureX</b>  <a href="#">US Cloud</a> <a href="#">EU Cloud</a> <a href="#">APJC Cloud</a>	<a href="#">Configuration Guides</a>	Documentation
	<a href="#">SecureX Reference Guide</a>	Configuration
	<a href="#">SecureX Blogs</a>	Documentation
	<a href="#">SecureX FAQs</a>	Documentation
	<a href="#">Cisco Live On-Demand Library</a>	Video
	<a href="#">Cisco SecureX Video Playlist</a>	Video
	<a href="#">Cisco Live 2023! Secure Endpoint and SecureX Sessions</a>	Documentation
<b>SecureX Threat Response</b>  [formerly Cisco Threat Response(CTR)]  <a href="#">US Cloud</a> <a href="#">EU Cloud</a> <a href="#">APJC Cloud</a>	<a href="#">Integrate CTR and Secure Malware Analytics</a>	Configuration
	<a href="#">Integrate Cisco Threat Response and Firepower</a>	Configuration
	<a href="#">Troubleshoot on the FMC and CTR Integration</a>	Configuration
	<a href="#">Cisco Threat Response (CTR) and ESA Integration</a>	Video
	<a href="#">ESA: File Reputation and File Analysis</a>	Configuration

	<a href="#">Integrate WSA with CTR</a>	Configuration
	<a href="#">CTR FAQs</a>	Configuration
	<a href="#">Cisco Threat Response Configuration Tutorials</a>	Configuration
	<a href="#">Cisco Threat Response Video Playlist</a>	Video
<b>SecureX Orchestrator</b>		
<a href="#">US Cloud</a> <a href="#">EU Cloud</a> <a href="#">APJC Cloud</a>	<a href="#">SecureX Orchestration Tutorial</a>	Documentation
	<a href="#">Pondering Automations - Cisco Community</a>	Configuration
		Troubleshooting
	<a href="#">ActionOrchestratorContent - Github</a>	Documentation

## Integrations related articles

Product Portals	Related Articles	Tags
	<a href="#">Integrating Secure Endpoint with FMC</a>	Configuration
	<a href="#">Installation and Configuration of AMP Module Through AnyConnect 4.x and AMP Enabler</a>	Configuration
	<a href="#">ESA/CES - Procedure to register clustered appliances to Secure Endpoint</a>	Configuration
	<a href="#">Integration of AMP Virtual Private Cloud and Threat Grid Appliance</a>	Configuration
	<a href="#">Integrate Secure Endpoint and Secure Malware Analytics with WSA</a>	Configuration
<b>Cisco Secure Endpoint</b> <a href="#">US Cloud</a> <a href="#">EU Cloud</a> <a href="#">APJC Cloud</a>		

<b>Cisco Secure Malware Analytics</b>  <a href="#">US Cloud</a> <a href="#">EU Cloud</a>	<a href="#">Umbrella and Secure Malware Analytics Integration</a>	
	<a href="#">File Analysis Client ID on Content Security Appliances (ESA, SMA, WSA) and DC/FMC</a>	
<b>Cognitive Threat Analytics</b> / <b>Global Threat Alerts</b> <a href="#">(CTA)</a>	<a href="#">CTA Demo with Secure Endpoint</a>	
	<a href="#">Secure Endpoint Global Threat Alerts (GTA) End of Service FAQ</a>	