Advanced Threat Solutions Troubleshooting Reference Guide

Contents

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
Public Cloud US Cloud EU Cloud APJC Cloud	General Documentation	Documentation
	Required Server Addresses for Proper Secure Endpoint & Secure Malware Analytics Operations	Configuration
	Secure Endpoint Connector Support Policy	Documentation
	Cisco Security Account User Guide	Documentation
	Configure Two-Factor Authentication in Secure Endpoint	Configuration
	Secure Endpoint Deployment Methodology and Best Practices	Configuration
	Entitlement for Secure Endpoint	Configuration
	Enable Secure Sign-On for Cisco Security Accounts	Configuration
	Secure Endpoint Notification Emails	Configuration
	Configure and Video	

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

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

Secure Endpoint Update Server

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

Linux Connector	Endpoint Linux Connector		
	Secure Endpoint Linux Connector OS Compatibility		Documentation
	Secure Endpoint Linux Connector Update Reboot Requirements		Documentation
	Installation of the Secure Endpoint Linux Connector	Video	Configuration
	Secure Endpoint ClamAV Virus Definition Options in Linux		Configuration
	Cisco Secure Endpoint Mac/Linux CLI		Configuration
	Secure Endpoint Linux Connector Faults		Troubleshooting
	Basic Troubleshoot Guide for Secure Endpoint Linux Connector		Troubleshooting
	Secure Endpoint Linux Primer		Documentation
	Secure Endpoint Linux Connector on Ubuntu		Configuration
	Advisory for Secure Endpoint Linux Connector 1.15.0 on Ubuntu 20.04.0 LTS and Ubuntu 20.04.1 LTS		Documentation
	Linux Kernel-Devel Fault		Troubleshooting
	Secure Endpoint Linux Connector Long Term Support		Documentation
	Troubleshoot Secure Endpoint Linux Connector Fault 18		Troubleshooting
	Troubleshoot Fault ID 11 on SUSE Linux Secure Endpoint		Troubleshooting
Mac Connector	Secure Endpoint Connector for Mac Diagnostic Data Collection		Troubleshooting
	Secure Endpoint Mac Connector OS Compatibility		Documentation
	Analyze macOS Secure Endpoint Diagnostic Bundle for High CPU		Troubleshooting
	Secure Endpoint Process Exclusions in macOS and Linux		Configuration
	Secure Endpoint Mac Connector		Troubleshooting

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

Efficacy/Remediation/Compliancy	Outbreak/Infection (Incident Response)	Documentation

Cisco Secure Malware Analytics Appliance

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

	Secure Malware Analytics Appliance Dashboard	Configuration
	Troubleshoot of Secure Malware Analytics Appliance Integration with FMC	Configuration
	Secure Malware Analytics Video Playlist	Video

Cisco SecureX

Product Portals	Related Articles	Tags
Cisco SecureX US Cloud EU Cloud APJC Cloud	Configuration Guides	Documentation
	SecureX Reference Guide	Configuration
	SecureX Blogs	Documentation
	SecureX FAQs	Documentation
	Cisco Live On-Demand Library	Video
	Cisco SecureX Video Playlist	Video
SecureX Threat Response [formerly Cisco Threat Response(CTR)] US Cloud EU Cloud APJC Cloud	Integrate CTR and Secure Malware Analytics	Configuration
	Integrate Cisco Threat Response and Firepower	Configuration
	Troubleshoot on the FMC and CTR Integration	Configuration
	Cisco Threat Response (CTR) and ESA Integration | Video	Configuration
	ESA: File Reputation and File Analysis	Configuration
	Integrate WSA with CTR	Configuration
	CTR FAQs	Configuration

Cisco Threat Response Configuration Tutorials

		Configuration
	Cisco Threat Response Video Playlist	Video
SecureX Orchestrator US Cloud EU Cloud APJC Cloud	SecureX Orchestration Tutorial	Documentation
	Pondering Automations - Cisco Community	Configuration Troubleshooting
	ActionOrchestratorContent - Github	Documentation

Integrations related articles

Product Portals	Related Articles	Tags
Cisco Secure Endpoint US Cloud EU Cloud APJC Cloud	Integrating Secure Endpoint with FMC	Configuration
	Installation and Configuration of AMP Module Through AnyConnect 4.x and AMP Enabler	Configuration
	ESA/CES - Procedure to register clustered appliances to Secure Endpoint	Configuration
	Integrate Secure Endpoint and Secure Malware Analytics with WSA	Configuration
Cisco Secure Malware Analytics US Cloud EU Cloud	Umbrella and Secure Malware Analytics Integration	Configuration
	File Analysis Client ID on Content Security Appliances (ESA, SMA, WSA) and DC/FMC	Troubleshooting

Cognitive Threat Analytics / **Global Threat Alerts** (CTA)	CTA Demo with Secure Endpoint	Configuration
	Secure Endpoint Global Threat Alerts (GTA) End of Service FAQ	Documentation