Guida di riferimento per la risoluzione dei problemi delle soluzioni di minacce avanzate

Sommario

Introduzione

Questo documento descrive i collegamenti della documentazione delle soluzioni ATS (Advanced Threat Solutions) per prodotti come Cisco Secure Endpoint, Cisco Secure Malware Analytics, Cisco Threat Response (CTR) e Cisco SecureX.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

L'articolo seguente è una guida di riferimento per la configurazione e la risoluzione dei problemi dei prodotti Advanced Threat Solutions. È possibile fare riferimento a questo articolo prima di attivare Cisco TAC.

Collegamenti alla documentazione di Cisco Secure Endpoint

Portali dei prodotti	Articoli correlati	Tag
Cloud pubblico Cloud USA EU Cloud APJC Cloud	Documentazione generale	Documentation
	Indirizzi server richiesti per operazioni di analisi sicure di endpoint e malware	Configuration
	Criteri di supporto Secure Endpoint Connector	Documentation
	Guida dell'utente di Cisco Security Account	Documentation
	Configurazione dell'autenticazione a due fattori in un endpoint sicuro	Configuration
	Metodologia e best practice per l'implementazione di endpoint sicuri	Configuration

	Diritti per Secure Endpoint		Configuration
	Abilita Secure Sign-On per gli account di sicurezza Cisco		Configuration
	Messaggi di notifica endpoint sicuri		Configuration
	Configurare e gestire le esclusioni in Secure Endpoint	Video	Configuration
	Modifiche all'elenco di esclusione gestite da Cisco per Secure Endpoint Console		Configuration
	Procedure ottimali per le esclusioni di endpoint sicuri		Configuration
	Configurare un elenco di rilevamento personalizzato semplice sul portale degli endpoint sicuri		Configuration
	Secure Endpoint Console e il filtro Ultimo visto		Troubleshooting
	Esporta elenchi di blocco applicazioni dal portale degli endpoint sicuri con API		Configuration
	Come creare un flusso di eventi con API Secure Endpoint		Configuration
	Come inviare un file in Secure Malware Analytics dal portale degli endpoint sicuri?		Troubleshooting
	Consenso esplicito e abilitazione della ricerca avanzata orbitale nella distribuzione di endpoint sicuri		Documentation
	Risoluzione dei problemi relativi agli errori di aggiornamento delle definizioni TETRA		Troubleshooting
	Integrazione sicura degli endpoint con Splunk		Configuration
	Configura notifica popup in endpoint sicuro		Configuration
	Risoluzione dei problemi relativi agli eventi di analisi dei file falsi positivi in un endpoint protetto		Troubleshooting
	Endpoint sicuro - Registri orbitali che completano gli errori - CSCwh73163		Documentation
	Secure Endpoint su AWS Workspaces - Script di avvio e configurazione per Golden Images		Configuration
	Informazioni sulle snapshot forensi degli		Configuration

	endpoint sicuri		
	Verifica analisi Windows Secure Endpoint (CSE)		Documentation
	Identificazione delle condizioni per l'attivazione di azioni automatizzate in un endpoint sicuro		Documentation
Android Connector	Ottenere informazioni sulla risoluzione dei problemi relativi ai dati in un dispositivo Android per Secure Endpoint		Troubleshooting
	Compatibilità del sistema operativo con il connettore Android per endpoint sicuro		Documentation
Chiarezza iOS	Cisco Security Connector Compatibilità Apple iOS		Documentation
	Creazione di rapporti su problemi/dati di diagnostica da Secure Endpoint Cisco Security Connector		Troubleshooting
	Come controllare un dispositivo iOS per l'utilizzo con Cisco Security Connector (CSC)?		Troubleshooting
Windows Connector	Raccolta di dati diagnostici da un connettore di endpoint protetto in esecuzione su Windows		Troubleshooting
	Compatibilità sistema operativo Windows Connector Secure Endpoint		Documentation
	Requisiti per il riavvio dell'aggiornamento di Windows Connector per l'endpoint sicuro		Documentation
	Annuncio di termine del supporto per le versioni di Secure Endpoint Connector		Documentation
	Annuncio di fine supporto per Windows XP, Windows Vista e Windows 2003 per Secure Endpoint Connector		Documentation
	Domande frequenti per clienti esistenti dall'8 gennaio 2020 relative ai nuovi pacchetti di endpoint sicuri		Documentation
	Configurare i criteri di Windows in Secure Endpoint	Video	Configuration

	[External] - Switch della riga di comando per il programma di installazione di Secure Endpoint Connector		Configuration
	Switch della riga di comando per Secure Endpoint		Configuration
	Forza manualmente l'aggiornamento delle definizioni TETRA - Endpoint protetto	Video	Troubleshooting
	Passaggi di configurazione del server di aggiornamento degli endpoint sicuri		Configuration
	Come raccogliere i log di ProcMon per risolvere i problemi relativi a Secure Endpoint all'avvio		Troubleshooting
	Creazione di un elenco avanzato di rilevamento personalizzato in Cisco Secure Endpoint		Troubleshooting
	Analizza bundle di diagnostica degli endpoint sicuri per CPU elevata		Troubleshooting
	Come disinstallare Secure Endpoint Windows Connector con la modalità provvisoria		Troubleshooting
	Procedura per disinstallare il connettore Secure Endpoint se la password viene dimenticata		Troubleshooting
	Windows Process viene avviato prima della soluzione Secure Endpoint Connector - Endpoint sicuro		Configuration
	Compatibilità del motore Secure Endpoint Exploit Prevention Engine con EMET		Configuration
	Prevenzione degli utilizzi		Documentation
	Cisco Secure Endpoint Guide to Identity Persistence		Configuration
	Elenco dei certificati radice necessari per l'installazione di endpoint sicuri in Windows		Troubleshooting
	Codici di uscita del programma di installazione di Windows Connector per endpoint sicuro		Documentation
	Risoluzione dei problemi di protezione degli script in Secure Endpoint		Troubleshooting
	Limitazioni del controllo dei dispositivi negli		Troubleshooting

	ambienti VMWare		
	Risoluzione dei problemi relativi all'aggiornamento delle definizioni TETRA con errore 3000		Troubleshooting
	Configurare i rilevamenti personalizzati - Avanzate con ClamAV SIGTOOL.EXE su Windows		Configuration
	Risolvere i problemi relativi all'installazione di Secure Client Full|Installazione guidata rete		Troubleshooting
	Configurare un'ora personalizzata per i download TETRA		Configuration
Connettore Linux	Raccolta di dati diagnostici dal connettore Secure Endpoint Linux		Troubleshooting
	Compatibilità del sistema operativo del connettore Linux dell'endpoint sicuro		Documentation
	Requisiti per il riavvio dell'aggiornamento del connettore Linux dell'endpoint sicuro		Documentation
	Installazione del connettore Secure Endpoint Linux	Video	Configuration
	Opzioni di definizione dei virus Secure Endpoint ClamAV in Linux		Configuration
	CLI di Cisco Secure Endpoint Mac/Linux		Configuration
	Errori del connettore Linux dell'endpoint sicuro		Troubleshooting
	Guida alla risoluzione dei problemi di base per il connettore Secure Endpoint Linux		Troubleshooting
	Primer Linux Secure Endpoint		Documentation
	Secure Endpoint Linux Connector su Ubuntu		Configuration
	Consulenza per Secure Endpoint Linux Connector 1.15.0 su Ubuntu 20.04.0 LTS e Ubuntu 20.04.1 LTS		Documentation
	Errore di sviluppo del kernel Linux		Troubleshooting
	Supporto a lungo termine Secure Endpoint Linux Connector		Documentation
	Risoluzione dei problemi relativi all'errore		Troubleshooting

	del connettore Linux dell'endpoint sicuro 18	
	Risoluzione dei problemi relativi all'ID errore 11 sull'endpoint sicuro SUSE Linux	Troubleshooting
Connettore Mac	Secure Endpoint Connector per raccolta dati di diagnostica Mac	Troubleshooting
	Compatibilità con il sistema operativo del connettore Mac dell'endpoint protetto	Documentation
	Analizza il pacchetto di diagnostica degli endpoint sicuri macOS per CPU elevata	Troubleshooting
	Esclusioni di processi endpoint sicuri in macOS e Linux	Configuration
	Guida all'ottimizzazione delle prestazioni del connettore Mac Secure Endpoint	Troubleshooting
	Kernel MAC e accesso completo al disco nella console - Endpoint protetto	Troubleshooting
	Procedura di disinstallazione manuale per il connettore Mac Secure Endpoint	Configuration
	Consulenza per Secure Endpoint Mac Connector 1.14 su macOS 11 (Big Sur), macOS 10.15 (Catalina) e macOS 10.14 (Mojave)	Configuration
	Errori del connettore Mac dell'endpoint sicuro	Troubleshooting
	Configurazione delle autorizzazioni per il connettore Mac dell'endpoint protetto e orbitale con MDM: Accesso completo al disco, Estensioni di sistema	Configuration
Cloud privato	Documentazione generale	Documentation
	Criteri di supporto cloud privato per endpoint sicuri	Documentation
	Installazione e configurazione di Secure Endpoint Virtual Private Cloud	Documentation
	Nuova immagine di Secure Endpoint Private Cloud PC3000 e ripristino del backup	Configuration
	Genera e aggiungi i certificati necessari per	Configuration

	l'installazione di Secure Endpoint Private Cloud 3.x e versioni successive	
	Procedura di aggiornamento per AirGapped Secure Endpoint Private Cloud (virtuale e appliance)	Configuration
	Genera snapshot del supporto cloud privato per endpoint sicuro e abilita sessione di supporto in tempo reale	Troubleshooting
	Accesso alla CLI di Secure Endpoint Private Cloud tramite SSH e trasferimento di file tramite SCP	Configuration
	Procedura di aggiornamento Secure Endpoint Private Cloud 3.0.1	Documentation
	Aggiornamento a Secure Endpoint Private Cloud 3.1.1 - aggiunta di spazio su disco e memoria	Documentation
	Annuncio EOS per versioni Secure Endpoint Private Cloud	Documentation
Efficacia/Correzione/Conformità	Epidemia/Infezione (Risposta All'Incidente)	Documentation

Cisco Secure Malware Analytics Appliance

Portali dei prodotti	Articoli correlati	Tag
Cisco Secure Malware Analytics Appliance	Guide alla configurazione	Documentation
	Guide all'installazione e all'aggiornamento	Documentation
	Versione del sistema Secure Malware Analytics	Documentation
	Annuncio di fine ciclo di vita utile e di vendita	Documentation
	Configurazione di Secure Malware Analytics Appliance per le operazioni cluster	Configuration
	Genera snapshot del supporto di analisi malware sicura e abilita sessione di supporto in tempo reale	Troubleshooting
	Configurazione del client SSH per Cisco	

	Secure Malware Analytics Appliance	Configuration
	Aggiorna modalità Air-Gap di Secure Malware Analytics Appliance	Configuration
	Genera snapshot del supporto di analisi malware sicura e abilita sessione di supporto in tempo reale	Configuration
	Configurazione di Secure Malware Analytics Appliance con il software di monitoraggio Prometheus	Configuration
	Come avviare Secure Malware Analytics Appliance in modalità di ripristino con la shell EFI e aggiungere la modalità di ripristino alle opzioni di avvio	Configuration
	Aggiorna modalità Air-Gap di Secure Malware Analytics Appliance	Configuration
	Configurare l'autenticazione RADIUS di analisi sicura dei malware su DTLS per la console e il portale OPadmin	Configuration
	Configurazione delle integrazioni di terze parti per Secure Malware Analytics Appliance	Configuration
	Risoluzione dei problemi relativi a esempi e dispositivi non presenti nel dashboard di Secure Malware Analytics	Configuration
	Risoluzione dei problemi relativi all'integrazione di Secure Malware Analytics Appliance con FMC	Configuration
	Playlist video di Secure Malware Analytics	Video

Cisco SecureX

Portali dei prodotti	Articoli correlati	Tag
Cisco SecureX Cloud USA	Guide alla configurazione	Documentation
	Guida di riferimento a SecureX	Configuration
	Blog SecureX	Documentation

EU Cloud APJC Cloud	Domande frequenti su SecureX	Documentation
	Libreria on-demand Cisco Live	Video
	Playlist video Cisco SecureX	Video
SecureX Threat Response [in precedenza Cisco Threat Response(CTR)] Cloud USA EU Cloud APJC Cloud	Integrazione di CTR e analisi sicure dei malware	Configuration
	Integrazione di Cisco Threat Response e Firepower	Configuration
	Risoluzione dei problemi relativi all'integrazione di CCP e CTR	Configuration
	Integrazione Cisco Threat Response (CTR) ed ESA — Video	Configuration
	ESA: Reputazione dei file e analisi dei file	Configuration
	Integrazione di WSA con CTR	Configuration
	Domande frequenti sul CTR	Configuration
	Esercitazioni sulla configurazione di Cisco Threat Response	Configuration
	Playlist video di Cisco Threat Response	Video
SecureX Orchestrator Cloud USA EU Cloud APJC Cloud	Esercitazione sull'orchestrazione SecureX	Documentation
	Pondering Automations - Cisco Community	Configuration Troubleshooting
	ActionOrchestratorContent - Github	Documentation

Articoli correlati integrazioni

Portali dei prodotti	Articoli correlati	Tag
Cisco Secure Endpoint Cloud USA EU Cloud APJC Cloud	Integrazione di Secure Endpoint con FMC	Configuration
	Installazione e configurazione del modulo AMP con AnyConnect 4.x e AMP Enabler	Configuration
	ESA/CES - Procedura per registrare gli accessori del cluster su Secure Endpoint	Configuration
	Integrazione di Secure Endpoint e Secure Malware Analytics con WSA	Configuration
Cisco Secure Malware Analytics Cloud USA EU Cloud	Integrazione con Umbrella e Secure Malware Analytics	Configuration
	ID client di analisi dei file su appliance di sicurezza dei contenuti (ESA, SMA, WSA) e DC/FMC	Troubleshooting
Analisi cognitiva delle minacce / Avvisi globali sulle minacce (CTA)	Demo CTA con endpoint sicuro	Configuration
	Domande frequenti sulla fine del servizio GTA (Secure Endpoint Global Threat Alerts)	Documentation

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).