Guia de referência de solução de problemas do Advanced Threat Solutions

Contents

Introdução

Este documento descreve os links da documentação do Advanced Threat Solutions (ATS) para produtos como Cisco Secure Endpoint, Cisco Secure Malware Analytics, Cisco Threat Response (CTR) e Cisco SecureX.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O artigo a seguir é um guia de referência para a configuração/solução de problemas dos produtos Advanced Threat Solutions. Este artigo pode ser consultado antes de contratar o Cisco TAC.

Links da documentação do Cisco Secure Endpoint

Portais de produtos	Artigos relacionados	Tags
Nuvem pública Nuvem nos EUA Nuvem da UE Nuvem da APJC	Documentação geral	Documentation
	Endereços de servidor necessários para operações seguras apropriadas de análise de malware e endpoint	Configuration
	Política de Suporte do Conector de Ponto Final Seguro	Documentation
	Guia do usuário da Cisco Security Account	Documentation
	Configurar Autenticação de Dois Fatores em Ponto de Extremidade Seguro	Configuration
	Metodologia de implantação segura de endpoint e práticas recomendadas	Configuration

	Qualificação para endpoint seguro		Configuration
	Ativar login seguro para contas de segurança da Cisco		Configuration
	E-mails de notificação de endpoints seguros		Configuration
	Configurar e Gerenciar Exclusões no Ponto de Extremidade Seguro	Vídeo	Configuration
	Alterações da lista de exclusão mantidas pela Cisco para o console de endpoint seguro		Configuration
	Práticas recomendadas para exclusões de endpoints seguros		Configuration
	Configurar uma lista de detecção personalizada simples no Secure Endpoint Portal		Configuration
	Console de endpoint seguro e o filtro visto por último		Troubleshooting
	Exportar listas de bloqueio de aplicativos do Secure Endpoint Portal com APIs		Configuration
	Como criar um fluxo de eventos com APIs de endpoint seguras		Configuration
	Como enviar um arquivo no Secure Malware Analytics a partir do Secure Endpoint Portal?		Troubleshooting
	Aceite e ative a pesquisa avançada orbital na implantação de endpoints seguros		Documentation
	Troubleshooting de falhas de atualização de definições TETRA		Troubleshooting
	Integração segura de endpoint com o Splunk		Configuration
	Configurar Notificação Pop-Up em Ponto de Extremidade Seguro		Configuration
	Solucionar problemas de eventos de análise de arquivo com falsos positivos em um endpoint seguro		Troubleshooting
	Endpoint seguro - Registros orbitais preenchendo com erros - CSCwh73163		Documentation
	Endpoint seguro no AWS Workspaces - Scripts de inicialização e configuração		Configuration

	para Golden Images		
	Informações de snapshot forense de endpoint seguro		Configuration
	Revisar verificações do Windows do Secure Endpoint (CSE)		Documentation
Conector Android	Obtenha dados de solução de problemas em um dispositivo Android para endpoint seguro		Troubleshooting
	Compatibilidade de SO do Conector Android de Ponto de Extremidade Seguro		Documentation
Clareza do iOS	Compatibilidade com o Cisco Security Connector Apple iOS		Documentation
	Criar relatório de problemas/dados de diagnóstico a partir do conector de segurança seguro da Cisco para endpoints		Troubleshooting
	Como supervisionar um dispositivo iOS para uso com o Cisco Security Connector (CSC)?		Troubleshooting
Conector do Windows	Coleta de Dados de Diagnóstico de um Conector de Ponto de Extremidade Seguro em Execução no Windows		Troubleshooting
	Compatibilidade de SO do Conector do Windows de Ponto de Extremidade Seguro		Documentation
	Requisitos de reinicialização de atualização do Conector do Windows de Ponto de Extremidade Seguro		Documentation
	Anúncio de fim do suporte para versões do conector de endpoint seguro		Documentation
	Anúncio de fim de suporte para Windows XP, Windows Vista e Windows 2003 para o conector de endpoint seguro		Documentation
	Perguntas frequentes para clientes atuais a partir de 8 de janeiro de 2020 sobre novos pacotes de endpoint seguros		Documentation
	Configurar a Política do Windows no Ponto de	Vídeo	Configuration

	Extremidade Seguro		
	[Externo] - Switches de Linha de Comando para Instalador do Conector de Ponto de Extremidade Seguro		Configuration
	Switches de linha de comando Secure Endpoint		Configuration
	Force manualmente a atualização de definições TETRA - endpoint seguro	Vídeo	Troubleshooting
	Etapas de Configuração do Servidor de Atualização de Ponto de Extremidade Seguro		Configuration
	Como coletar logs do ProcMon para solucionar problemas do Secure Endpoint na inicialização		Troubleshooting
	Crie uma lista de detecção personalizada avançada no Cisco Secure Endpoint		Troubleshooting
	Analisar o pacote Secure Endpoint Diagnostic para CPU alta		Troubleshooting
	Como desinstalar o conector do Windows do ponto de extremidade seguro com o modo de segurança		Troubleshooting
	Procedimento para desinstalar o conector de ponto de extremidade seguro se a senha for esquecida		Troubleshooting
	Processo do Windows inicia antes da solução alternativa do conector de endpoint seguro - endpoint seguro		Configuration
	Compatibilidade do mecanismo de prevenção de exploração de endpoint seguro com EMET		Configuration
	Prevenção de exploração		Documentation
	Guia do Cisco Secure Endpoint para persistência de identidade		Configuration
	Lista de Certificados Raiz Necessários para a Instalação Segura de Ponto de Extremidade no Windows		Troubleshooting
	Códigos de Saída do Instalador do Conector do Windows de Ponto de Extremidade Seguro		Documentation
	Solucione problemas de proteção de		Troubleshooting

	script em endpoints seguros		
	Limitações de controle de dispositivos em ambientes VMWare		Troubleshooting
	Troubleshooting de Falha de Atualização de Definições TETRA com Erro 3000		Troubleshooting
	Configurar detecções personalizadas - Avançado com ClamAV SIGTOOL.EXE no Windows		Configuration
	Solucionar Problemas Completos do Cliente Seguro|Problemas de Instalação do Assistente de Instalação de Rede		Troubleshooting
Conector Linux	Coleta de dados de diagnóstico do conector Linux de endpoint seguro		Troubleshooting
	Compatibilidade de SO do conector Linux de endpoint seguro		Documentation
	Requisitos de reinicialização de atualização do conector Linux de endpoint seguro		Documentation
	Instalação do conector Linux de endpoint seguro	Vídeo	Configuration
	Opções de definição de vírus Secure Endpoint ClamAV no Linux		Configuration
	Cisco Secure Endpoint Mac/Linux CLI		Configuration
	Falhas do conector Linux de endpoint seguro		Troubleshooting
	Guia Básico de Solução de Problemas para Conector Linux de Ponto de Extremidade Seguro		Troubleshooting
	Secure Endpoint Linux Primer		Documentation
	Conector Linux de endpoint seguro no Ubuntu		Configuration
	Recomendação para Secure Endpoint Linux Connector 1.15.0 no Ubuntu 20.04.0 LTS e no Ubuntu 20.04.1 LTS		Documentation
	Falha no nível de kernel do Linux		Troubleshooting
	Suporte a longo prazo do conector Secure Endpoint Linux		Documentation

	Solucionar problemas de falha do conector do Secure Endpoint Linux 18	Troubleshooting
Conector Mac	Conector de Ponto de Extremidade Seguro para Coleta de Dados de Diagnóstico Mac	Troubleshooting
	Compatibilidade de SO do Conector Mac de Ponto de Extremidade Seguro	Documentation
	Analisar o pacote Secure Endpoint Diagnostic do MacOS para CPU alta	Troubleshooting
	Exclusões de processos de endpoints seguros no MacOS e no Linux	Configuration
	Guia de Ajuste de Desempenho do Conector Mac para Secure Endpoint	Troubleshooting
	Kernel MAC e acesso total ao disco no	Troubleshooting

	console - endpoint seguro	
	Procedimento de desinstalação manual do conector Mac do ponto de extremidade seguro	Configuration
	Recomendação para Secure Endpoint Mac Connector 1.14 no macOS 11 (Big Sur), macOS 10.15 (Catalina) e macOS 10.14 (Mojave)	Configuration
	Falhas do Conector Mac do Ponto de Extremidade Seguro	Troubleshooting
Nuvem privada	Documentação geral	Documentation
	Política de suporte à nuvem privada de endpoints seguros	Documentation
	Instalação e configuração de nuvem privada virtual de endpoint segura	Documentation
	Recrie o PC3000 de nuvem privada de endpoint seguro e restaure o backup	Configuration
	Gerar e adicionar certificados necessários para a instalação da Secure Endpoint Private Cloud 3.x em diante	Configuration
	Procedimento de atualização para a nuvem privada de endpoint seguro AirGapped (virtual e dispositivo)	Configuration
	Gerar instantâneo de suporte à nuvem privada de endpoint seguro e habilitar sessão de suporte ao vivo	Troubleshooting
	Acesso à CLI da nuvem privada de endpoint seguro via SSH e transferência de arquivos via SCP	Configuration
	Procedimento de atualização do Secure Endpoint Private Cloud 3.0.1	Documentation
	Atualizando para Secure Endpoint Private Cloud 3.1.1 - adicionando espaço em disco e memória	Documentation
	Anúncio de EOS para versões de nuvem privada de endpoint segura	Documentation

Eficácia/Correção/Conformidade	Epidemia/Infecção (Resposta a Incidente)	Documentation

Cisco Secure Malware Analytics Appliance

Portais de produtos	Artigos relacionados	Tags
Cisco Secure Malware Analytics Appliance	Guias de configuração	Documentation
	Guias de instalação e atualização	Documentation
	Versão do sistema do Secure Malware Analytics Appliance	Documentation
	Anúncio de fim das vendas e fim da vida útil	Documentation
	Configurar o Secure Malware Analytics Appliance para operações de cluster	Configuration
	Gerar instantâneo de suporte analítico de malware seguro e habilitar sessão de suporte ao vivo	Troubleshooting
	Configurando o cliente SSH para o Cisco Secure Malware Analytics Appliance	Configuration
	Atualizar modo Air-Gap do Secure Malware Analytics Appliance	Configuration
	Gerar instantâneo de suporte analítico de malware seguro e habilitar sessão de suporte ao vivo	Configuration
	Configure o Secure Malware Analytics Appliance com o software de monitoramento Prometheus	Configuration
	Como inicializar o Secure Malware Analytics Appliance no modo de recuperação com o EFI Shell e adicionar o modo de recuperação às opções de inicialização	Configuration
	Atualizar modo Air-Gap do Secure Malware Analytics Appliance	Configuration
	Configurar Secure Malware Analytics RADIUS sobre autenticação DTLS para Console e Portal OPadmin	Configuration
	Configurar Integrações de Terceiros do Secure Malware Analytics Appliance	Configuration

	Amostras de solução de problemas e dispositivos não presentes no painel do Secure Malware Analytics Appliance	Configuration
	Solução de problemas de integração do Secure Malware Analytics Appliance com o FMC	Configuration
	Lista de reprodução de vídeo Secure Malware Analytics	Video

Cisco SecureX

Portais de produtos	Artigos relacionados		Tags
Cisco SecureX Nuvem nos EUA Nuvem da UE Nuvem da APJC	Guias de configuração		Documentation
	Guia de referência do SecureX		Configuration
	Blogs do SecureX		Documentation
	Perguntas frequentes do SecureX		Documentation
	Biblioteca Cisco Live sob demanda		Video
	Lista de reprodução de vídeo do Cisco SecureX		Video
Resposta a ameaças SecureX [antigo Cisco Threat Response(CTR)] Nuvem nos EUA Nuvem da UE Nuvem da APJC	Integre o CTR e Secure Malware Analytics		Configuration
	Integre o Cisco Threat Response e o Firepower		Configuration
	Solução de problemas na integração FMC e CTR		Configuration
	Cisco Threat Response (CTR) e integração ESA	Vídeo	Configuration
	ESA: Reputação de arquivos e análise de arquivos		Configuration
	Integrar o WSA com o CTR		Configuration
	Perguntas frequentes do CTR		Configuration

	Tutoriais de configuração da Cisco Threat Response	Configuration
	Playlist do vídeo de resposta às ameaças da Cisco	Video
SecureX Orchestrator Nuvem nos EUA Nuvem da UE Nuvem da APJC	Tutorial de orquestração SecureX	Documentation
	Pondering Automations - Comunidade Cisco	Configuration Troubleshooting
	ActionOrchestratorContent - Github	Documentation

Artigos relacionados a integrações

Portais de produtos	Artigos relacionados	Tags
Endpoint seguro da Cisco Nuvem nos EUA Nuvem da UE Nuvem da APJC	Integração do Secure Endpoint com o FMC	Configuration
	Instalação e configuração do módulo AMP por meio do AnyConnect 4.x e do AMP Enabler	Configuration
	ESA/CES - Procedimento para registrar dispositivos em cluster para endpoint seguro	Configuration
	Integre endpoints seguros e análises de malware seguras com o WSA	Configuration

Integração de análise de malware segura e

Cisco Secure Malware Analytics Nuvem nos EUA Nuvem da UE	abrangente	Configuration
	ID do cliente de análise de arquivo em dispositivos de segurança de conteúdo (ESA, SMA, WSA) e DC/FMC	Troubleshooting
Análise cognitiva de ameaças / Alertas globais de ameaças (CTA)	Demonstração do CTA com endpoint seguro	Configuration
	Perguntas frequentes de fim de serviço sobre alertas de ameaças globais (GTA) para endpoints seguros	Documentation

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.