# ESA/CES - Procedimento para registrar dispositivos em cluster na AMP para endpoints

# Contents

Introduction Problema Solução Etapa 1 - Fazer login e navegar até a página AMP no ESA/CES. Etapa 2 - Alterar o modo de configuração. Etapa 3 - Alternar para o modo de substituição da máquina. Etapa 4 - Registrar o AMP para endpoints na configuração da máquina. Etapa 5 - Alternar para o modo cluster. Informações Relacionadas

# Introduction

Este documento descreve o procedimento para registrar os dispositivos Cisco Email Security Appliances (ESA) / Cloud Email Security (CES) em um ambiente de configuração em cluster para Advanced Malware Protection (AMP) for Endpoints.

# Problema

**Note**: Este documento foi escrito a partir do ESA/CES AsyncOS 11.1. Para obter mais informações sobre a documentação do ESA/CES, consulte os <u>Guias do Usuário e a</u> <u>Documentação</u>.

Tentando registrar um cluster ESA/CES com AMP para endpoints na GUI na página **Serviços de segurança > Reputação e análise de arquivo**, o botão *Registrar dispositivo com AMP para endpoints* está acinzentado e não consegue concluir o registro.

#### Mostrado na imagem:

$\triangledown$ Advanced Settings for File Reputation	File Reputation Server:	AMERICAS (cloud-sa.amp.cisco.com)
	AMP for Endpoints Console Integration $\textcircled{O}$	Register Appliance with AMP for Endpoints
	SSL Communication for File Reputation:	Use SSL (Port 443)
		Tunnel Proxy (Optional):
		Server:

# Solução

Para registrar um dispositivo ESA/CES em uma configuração em cluster para o AMP for Endpoints, isso deve ser feito com **substituições no nível da máquina**. Isso significa que para cada máquina no cluster, ela terá uma configuração de substituição individual que terá precedência. As etapas a serem concluídas são as seguintes:

### Etapa 1 - Fazer login e navegar até a página AMP no ESA/CES.

Navegue até **Serviços de segurança > Reputação e análise de arquivo** e verifique o modo atual de configuração. Isso é indicado pelo **Mode - Cluster** na saída fornecida.

#### **File Reputation and Analysis**

Mode — Cluster: AMPTEST enge Mode · · ·					
Advanced Malware Protection					
File Reputation:	Enabled				
File Analysis:	Enabled				
	Edit Global Settings				

Click here to group or view appliances for File Analysis reporting.

### Etapa 2 - Alterar o modo de configuração.

Clique em Opções de gerenciamento centralizado > Gerenciar configurações.

Mode - Cluster: AMPTEST Change Mode.					
Settings are defined: Delete Settings for this feature at this mode. You can also Manage Settings.					
Advanced Malware Protection					
File Reputation:	Enabled				
File Analysis:	Enabled				

Em Gerenciar configurações, **copie a configuração do cluster** para a respectiva máquina conectada. Depois de selecionada, **Submeta e confirme** as alterações.



### Etapa 3 - Alternar para o modo de substituição da máquina.

Clique em Alterar modo... e selecione a respectiva máquina com a substituição a ser configurada.

#### **File Reputation and Analysis**

Mode - Cluster: AMPTEST	Change Mode 🔻		
Centralized Management Options	Change Mode		
v centralized Hanagement options	* Cluster: AMPTEST (current mode)		
	Group: Main_Group		
dvanced Malware Protection	Machine: ESA.cisco.com		
	Machine: esa4.aricent.com		
Fi	le Reputation: Enabled		
	File Analysis: Enabled		
		Edit Global Settings.	
Click here to group or view appliances for File Analysis reporting.			

### Etapa 4 - Registrar o AMP para endpoints na configuração da máquina.

Depois que o modo de configuração for comutado para Máquina: <Nome da máquina>.

Clique em Editar configurações globais... em seguida, expanda as configurações avançadas do componente Análise de arquivo.

Clique no botão Register Appliance with AMP for Endpoints" para concluir o registro.

Mode — Machine: esa4.aricent.com Change Mode T						
Advanced Malware Protection						
Advanced Malware Protection services require network communication to the cloud servers on ports 32137 or 443 (for File Reputation) and 443 (for File Analysis). Please see the Online Help for additional details.						
File Reputation Filtering:	C Enable File Reputation					
File Analysis: (?)	Enable File Analysis   Select All Expand All C  Archived and compressed  Configuration  Configuration  Database  Document  Email  Email  Encoded and Encrypted  Executables  Microsoft Documents  Miscellaneous	ollapse All Reset				
	File Reputation Server:	AMERICAS (cloud-sa.amp.cisco.com)				
	AMP for Endpoints Console Integration 🕐	Register Appliance with AMP for Endpoints				
	SSL Communication for File Reputation:	Use SSL (Port 443) Tunnel Proxy (Optional):				

**Repita as etapas 1 a 4** nas máquinas restantes no cluster para registrar-se na AMP para endpoints.

**aviso:** Versões do software ESA/CES afetadas pela id do defeito: <u>CSCvp23281</u> deve ignorar a Etapa 5 conforme fornecido na solução do defeito.

### Etapa 5 - Alternar para o modo cluster.

Depois que cada máquina tiver registrado o AMP para endpoints, altere o modo de volta para cluster removendo as substituições de nível de máquina para Reputação e Análise de Arquivo em **Opções de Gerenciamento Centralizado > Gerenciar Configurações**. Todas as configurações do dispositivo devem corresponder para que o cluster funcione com êxito. O botão **Register Appliance with AMP for Endpoints** ainda estará acinzentado e indisponível no modo de cluster.

## Informações Relacionadas

- Suporte Técnico e Documentação Cisco Systems
- <u>Cisco AMP para endpoints Portal de documentação</u>
- <u>Cisco Cloud Email Security Guias do usuário final</u>
- Cisco Email Security Appliance Guias do usuário final