# ESA/CES:クラスタ化アプライアンスをエンド ポイント用AMPに登録する手順

# 内容

#### 概要

#### 問題

#### 解決方法

ステップ1:ログインし、ESA/CESの[AMP]ページに移動します。

ステップ2:設定モードを変更します。

<u>ステップ3:マシンオーバーライドモードに切り替えます。</u> 手順4:マシン設定のエンドポイント用AMPを登録します。

ステップ5:クラスタモードに切り替えます。

<u>関連情報</u>

### 概要

このドキュメントでは、クラスタ化設定環境のCisco Eメールセキュリティアプライアンス (ESA)/クラウドEメールセキュリティ(CES)アプライアンスをエンドポイント用Advanced Malware Protection(AMP)に登録する手順について説明します。

# 問題

注:このドキュメントは、ESA/CES AsyncOS 11.1で作成されました。ESA/CESのドキュメントの詳細については、ユーザガイドおよびドキュメントを参照してください。

[Security Services] > [File Reputation and Analysis]ページのGUIからESA/CESクラスタをエンドポイント用AMPに登録しようとすると、[Register Appliance with AMP for Endpoints]ボタンがグレー表示され、登録を完了できません。

次の図に示します。



# 解決方法

ESA/CESアプライアンスをクラスタ構成でエンドポイント用AMPに登録するには、マシンレベルの上書きでこの処理を行う**必要があります**。これは、クラスタ内の各マシンに対して、個別の上書き設定が優先されることを意味します。

次の手順を実行します。

# ステップ1:ログインし、ESA/CESの[AMP]ページに移動します。

[セキュリ**ティサービス] > [ファイルレピュテーションと分析]に移動**し、現在の設定モードを確認 します。これは、指定された出力のMode - Clusterによって示されます。

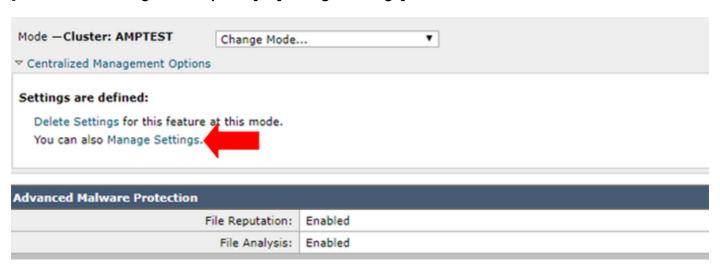
#### File Reputation and Analysis

Mode —Cluster: AMPTEST → mge Mode ▼  ▷ Centralized Management Options			
Advanced Malware Protection			
File Reputation:	Enabled		
File Analysis:	Enabled		
	Edit Global Settings		

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

#### ステップ2:設定モードを変更します。

[Centralized Management Options] > [Manage Settings]をクリックします。



[Manage Settings]で、クラスタ**からログインしたそれぞれの**マシンに構成をコピーします。選択したら、変更を**送信して確定**します。

ode -Cluster: AMPTEST	Change Mode ▼	
Centralized Management Option		
Copy ▼ settings to:      Cluster: AMPTEST (currer Group: Main_Group Machine: ESA.cisco.ci Machine: esa4.aricen      Delete settings from:  Cluster: AMPTEST ♣	mode) 🛦	
Cancel		Submit

#### ステップ3:マシンオーバーライドモードに切り替えます。

[Change Mode...]**ドロップダウンをクリック**し、設定するオーバーライド付きのマシンを選択します。

# Mode — Cluster: AMPTEST Change Mode... Change Mode.

## 手順4:マシン設定のエンドポイント用AMPを登録します。

設定モードをマシンに切り替えた後: <マシン名>。

[グローバル**設定の編集…]をクリックします。** 次に、[ファイル解析**]コンポーネントの[詳細設定]を**展開します。

[Register Appliance with AMP for Endpoints]ボタンをクリックして、登録を完了します。

Mode — Machine: esa4.aricent.com  Change Mode  Change Mode  Change Mode  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:	☑ Enable File Reputation				
File Analysis:	Enable File Analysis  Select All Expand All C  Archived and compressed  Configuration  Database  Document  Email  Encoded and Encrypted  Executables  Microsoft Documents  Miscellaneous	ollapse All Reset			
♥ Advanced Settings for File Reputation	File Reputation Server:  AMP for Endpoints Console Integration ②  SSL Communication for File Reputation:	AMERICAS (cloud-sa.amp.cisco.com)  Register Appliance with AMP for Endpoints  Use SSL (Port 443)  Tunnel Proxy (Optional):			

クラスタ内の残りのマシンで手順1~4を繰り返し、エンドポイント用AMPに登録します。

**警告:**不具合IDの影響を受けるESA/CESソフトウェアのバージョン:<u>CSCvp23281</u>は、不 具合の回避策に記載されているように、ステップ5をスキップする必要があります。

#### ステップ5: クラスタモードに切り替えます。

各マシンがエンドポイント用AMPに登録された後、[Centralized Management Options] > [Manage Settings]でファイルレピュテーションと分析のマシンレベルの上書きを削除し、モードをクラスタに戻します。 クラスタリングが正常に動作するには、すべてのデバイス設定が一致している必要があります。 [Register Appliance with **AMP for Endpoints]ボタンは引き続きグレー表**示され、クラスタモードでは使用できません。

# 関連情報

- テクニカル サポートとドキュメント Cisco Systems
- エンドポイント向けCisco AMP ドキュメントポータル
- CiscoクラウドEメールセキュリティ エンドユーザガイド
- Cisco E メール セキュリティ アプライアンス: エンドユーザ ガイド