ESA/CES - Procedure to register clustered appliances to AMP for Endpoints

Contents

Introduction

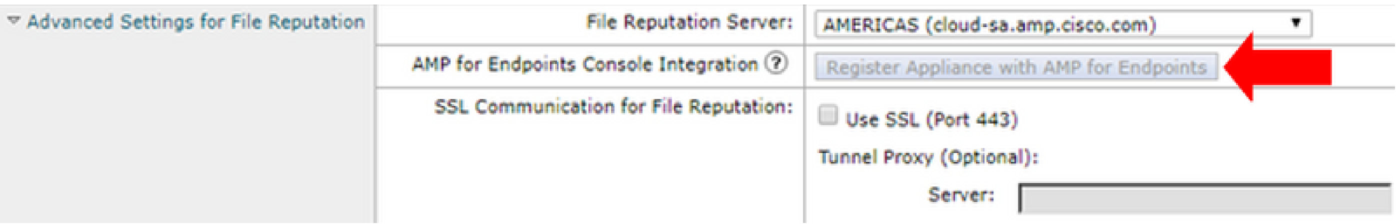
This document describes the procedure to register Cisco Email Security Appliances (ESA) / Cloud Email Security (CES) Appliances in a clustered configuration environment to Advanced Malware Protection (AMP) for Endpoints.

Problem

> **Note**: This document was written as of ESA/CES AsyncOS 11.1. For more information on ESA/CES documentation, please refer to the User Guides and Documentation.

Attempting to register an ESA/CES cluster with AMP for Endpoints from the GUI within the **Security Services > File Reputation and Analysis** page, the button ***Register Appliance with AMP for Endpoints*** is greyed out and unable to complete the registration.

Shown in the image:



▿ Advanced Settings for File Reputation

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):

Server:

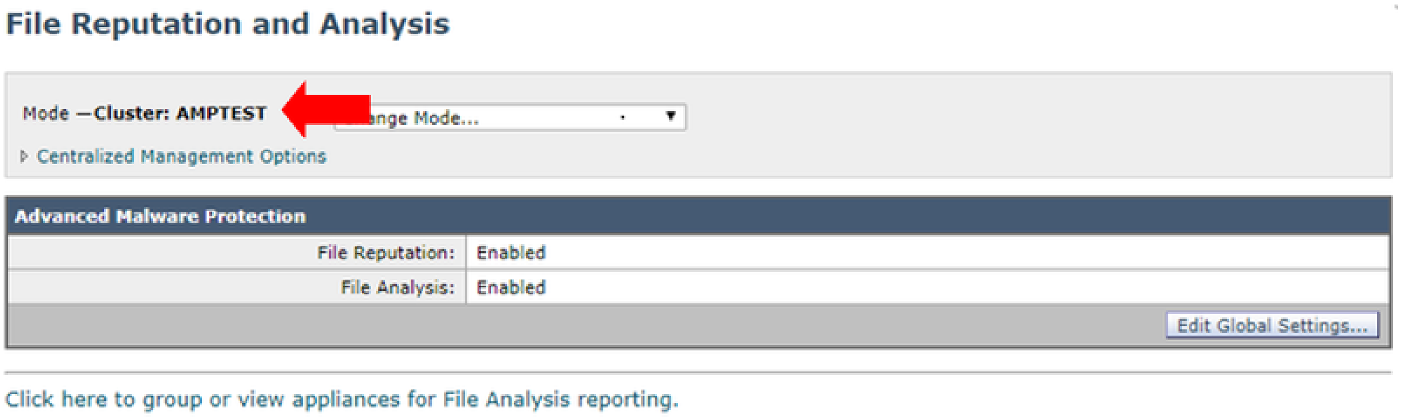
Solution

To register an ESA/CES appliance in a clustered configuration to AMP for Endpoints, this must be done with **machine level overrides**. This means that for each machine in the cluster, it will have an individual override setting that will take precedence.

The steps to complete are as follows:

Step 1 - Log in and Navigate to the AMP Page on the ESA/CES.

Navigate to **Security Services > File Reputation and Analysis** and verify the current mode of configuration. This is indicated by the **Mode - Cluster** in the provided output.



File Reputation and Analysis

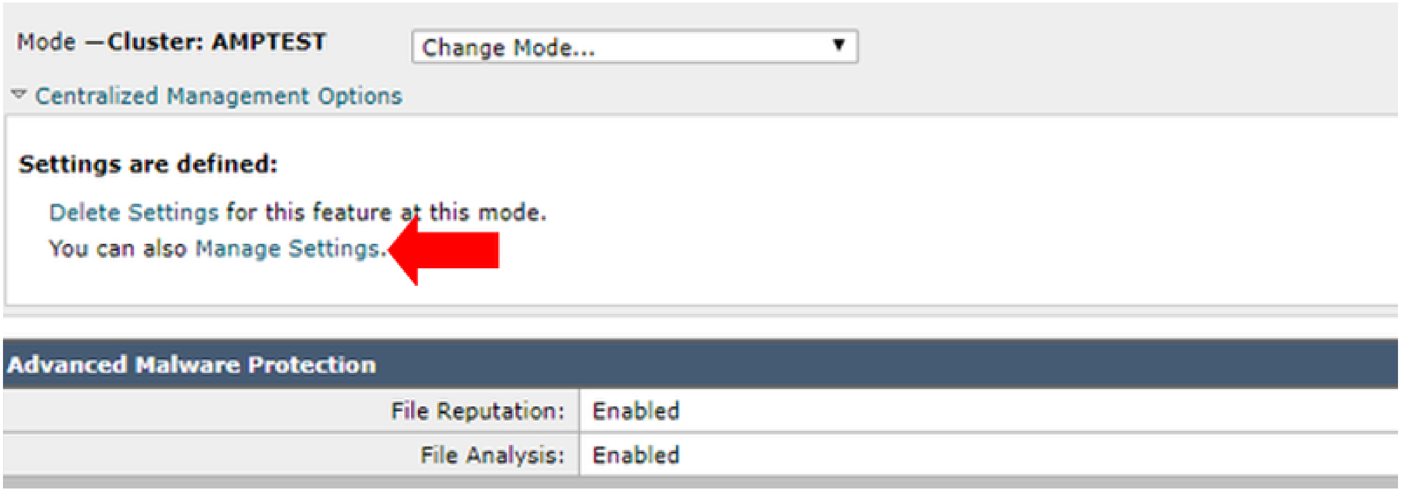
Mode —**Cluster: AMPTEST**

Advanced Malware Protection	
File Reputation:	Enabled
File Analysis:	Enabled

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

Step 2 - Change the mode of configuration.

Click **Centralized Management Options > Manage Settings.**



Mode —**Cluster: AMPTEST**

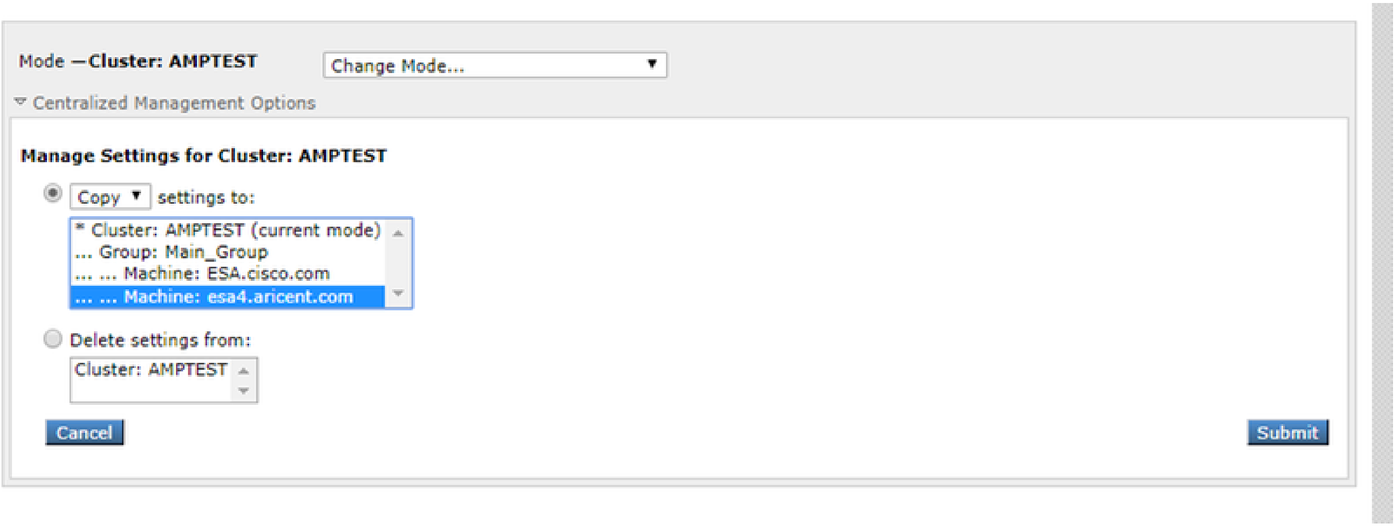
Settings are defined:

Delete Settings for this feature at this mode.

You can also Manage Settings.

Advanced Malware Protection	
File Reputation:	Enabled
File Analysis:	Enabled

Under Manage Settings, **copy the configuration from cluster** to the respective machine logged in. Once selected, **Submit and Commit** the changes.


Mode —Cluster: AMPTEST

Manage Settings for Cluster: AMPTEST

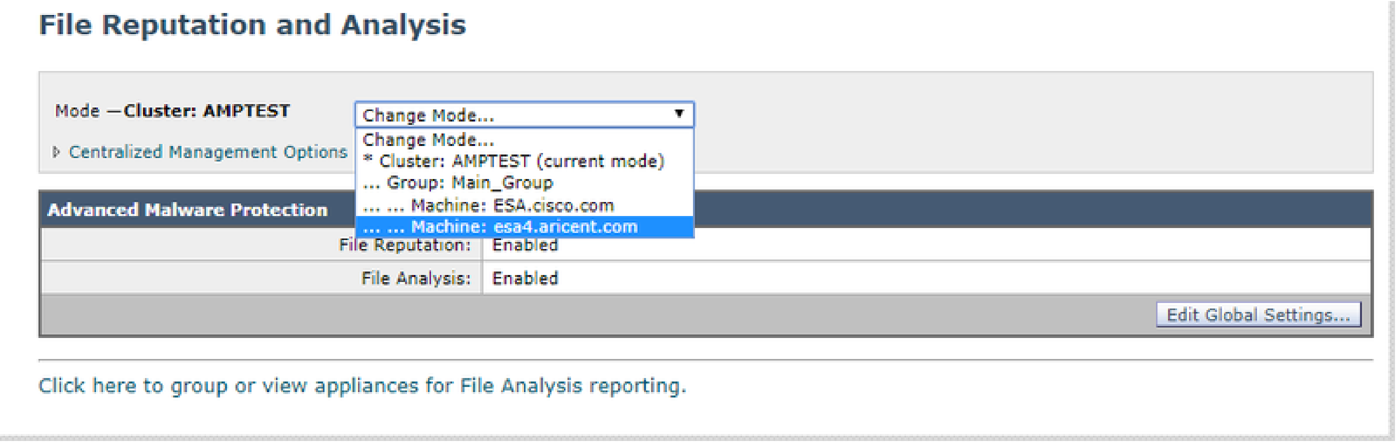
● Copy settings to: ... ... Machine: esa4.aricent.com

○ Delete settings from: Cluster: AMPTEST

Change Mode...
Centralized Management Options
Copy
* Cluster: AMPTEST (current mode)
... Group: Main_Group
... ... Machine: ESA.cisco.com
... ... Machine: esa4.aricent.com
Cluster: AMPTEST
Cancel
Submit

Step 3 - Switch to the Machine Override Mode.

Click on the **Change Mode...** drop down and select the respective machine with the override to configure.


File Reputation and Analysis

Mode —Cluster: AMPTEST

Advanced Malware Protection

File Reputation: Enabled

File Analysis: Enabled

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

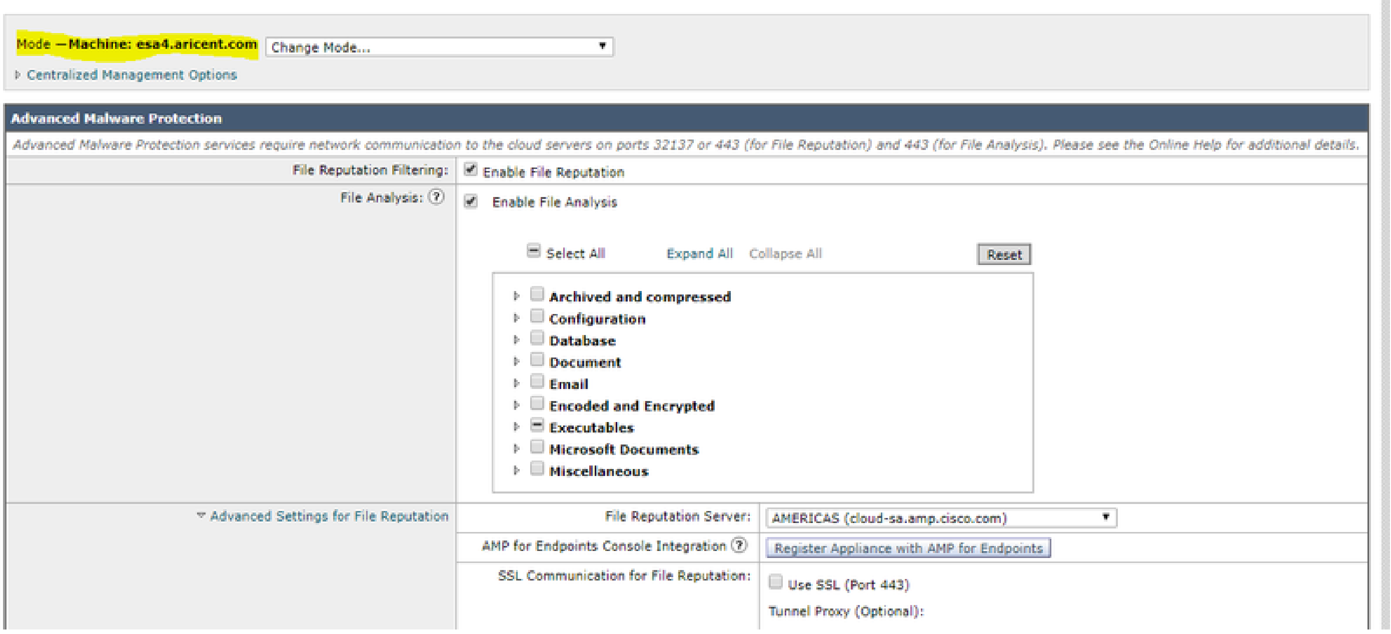
Change Mode...
Centralized Management Options
Change Mode...
* Cluster: AMPTEST (current mode)
... Group: Main_Group
... ... Machine: ESA.cisco.com
... ... Machine: esa4.aricent.com
Edit Global Settings...

Step 4 - Register AMP for Endpoints for the Machine setting.

After the configuration mode is switched to **Machine: <Machine Name>.**

Click **Edit Global Settings...** then expand the **Advanced settings for File Analysis** component.

Click the button for **Register Appliance with AMP for Endpoints**" to complete registration.



Mode —Machine: esa4.aricent.com Change Mode...

▸ Centralized Management Options

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 Collapse All Reset ▸ □ Archived and compressed ▸ □ Configuration ▸ □ Database ▸ □ Document ▸ □ Email ▸ □ Encoded and Encrypted ▸ ⊟ Executables ▸ □ Microsoft Documents ▸ □ Miscellaneous
▾ Advanced Settings for File Reputation	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):

Repeat Steps 1 - 4 on the remaining machines in the cluster to register for AMP for Endpoints.

> **Warning**: ESA/CES software versions affected by defect id:CSCvp23281 should skip Step 5 as provided on the defect workaround.

Step 5 - Switch to Cluster Mode.

After each machine has registered with AMP for Endpoints, change the mode back to cluster by removing the machine level overrides for File Reputation and Analysis under **Centralized Management Options > Manage Settings**. All of the device settings must match for the clustering to work successfully. The **Register Appliance with AMP for Endpoints** button will still be greyed out and unavailable in cluster mode.

Related Information

- **Technical Support & Documentation - Cisco Systems**
- **Cisco AMP for Endpoints - Documentation Portal**
- **Cisco Cloud Email Security - End-User Guides**
- **Cisco Email Security Appliance - End-User Guides**