

Mitigate “Not Available” Security Feature Status

Contents

[Introduction](#)

[Requirements](#)

[Prerequisites](#)

[Solution](#)

[Remove Machine Override to Fall Back to Cluster Level](#)

[Related Information](#)

Introduction

This document describes how to troubleshoot and resolve ESA and CES security features showing “Not Available” on mail policies.

Contributed by Alan Macorra and Mathew Huynh Cisco CX Engineers.

Requirements

Prerequisites

- Any ESA (Email Security Appliance)/CES (Cloud Email Security) on any version of AsyncOS.
- Device licensed with available feature keys for security services.
- Understanding of the different levels of cluster configuration and overrides.

Background

The ESA (Email Security Appliance)/CES (Cloud Email Security) device is failing to execute any security scanning from services such as:

- Anti-Spam
- Anti-Virus
- Advanced Malware Protection
- Graymail
- Outbreak filters
- DLP (Outbound only)

Feature keys are available and can be verified on the GUI or CLI.

GUI: System Administration > Feature Keys

CLI: featurekeys

Security features on Incoming and Outgoing Mail Policies display "Not Available" even though the service is enabled.

Problem

- Feature keys are available on the device, however, services display "Not Available" when executing scans.
- When clicking the "Not Available" link on the mail policies, it redirects to the global settings for that specific security service. This displays the service is enabled and imposing any modifications does not change the "Not Available" status on the mail policies.

Incoming Mail Policies

Mode -- Cluster: Gear 1 Change Mode...

Centralized Management Options

Find Policies

Email Address: Recipient Sender Find Policies

Any LDAP lookups will be made from the Login Host.

Policies

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
	Default Policy	Not Available	Not Available	Not Available	Not Available	Disabled	Not Available	

Outgoing Mail Policies

Mode -- Cluster: Gear 1 Change Mode...

Centralized Management Options

Find Policies

Email Address: Recipient Sender Find Policies

Any LDAP lookups will be made from the Login Host.

Policies

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	DLP	Delete
	Default Policy	Not Available	Not Available	Not Available	Not Available	Disabled	Not Available	Not Available	

Sophos

Mode -- Machine: ESA_1.cisco.com Change Mode...

Centralized Management Options

Inheriting settings from Cluster: Gear 1

Override Settings

Settings for this feature are currently defined at:

- Cluster: Gear 1

Sophos Anti-Virus Overview

Anti-Virus Scanning by Sophos Anti-Virus:	Enabled
Virus Scanning Timeout (seconds):	60
Automatic Updates:	Enabled

Edit Global Settings

Current Sophos Anti-Virus files

File Type	Last Update	Current Version	New Update
Sophos Anti-Virus Engine	Never Updated	3.2.67.368.1_5-39	Available
Sophos IDE Rules	Never Updated	0	Available


Attention - Updates completed with error. Update Now


Applies to Login Host only.

Solution

This issue occurs when feature keys expire before renewal and license re-installation. When this arises, the End User License Agreement (EULA) must be re-accepted. Since the devices were enabled prior to expiration, the initial feature keys were reinstalled/renewed, the EULA was not presented again and the device(s) were set to the cluster level.

To resolve this, you must override the settings on the ESA/CES to **machine level** to allow the EULA to present for acceptance. In doing so, the device registers the keys for renewal and re-activate the features again.

 **Note:** The configuration mode you are currently logged in with displays on the upper-left where it displays **Mode -- Cluster/Group/Machine**. Depending on the mode, what is displayed can be different from the initial output provided, which is already in **Machine Mode**.


 **Warning:** When creating overrides for this solution, ensure you **DO NOT** select **Move Configuration**, as this forces the cluster level configuration into an unconfigured mode for the specific service. If this is selected when removing the override, the feature falls back into an unconfigured (not enabled) state.

On each security service that displays "**Not Available**":

1. Click the **Not Available** link from the Incoming or Outgoing Mail Policies Page.
2. This redirects to the global settings per engine.
3. Select **Change Mode...** and from the drop-down menu select the machine that is currently logged in.
4. Click on **Override Settings**.
5. Select **Copy from: Cluster** (this copies your current enabled settings from the cluster level down to your machine).
6. Click **Submit**.
7. The configuration displays it is enabled. Proceed by clicking on the **Edit Global Settings...**
8. The EULA displays, you can read through and accept the EULA.
9. **Commit Changes** by saving this setting.
10. Repeat the steps on your other features, which require you to re-enable.

Sample output:

Using the drop-down on the right, change it to the machine you're logged into:



The screenshot shows a configuration interface. At the top, it displays "Mode -- Cluster: Gear 1" on the left and a dropdown menu labeled "Change Mode..." on the right. Below this, there is a section titled "Centralized Management Options" with a downward arrow. Underneath, it says "Settings are defined:" followed by two lines of text: "Delete Settings for this feature at this mode." and "You can also Manage Settings."

Copying the settings from the cluster to the machine override:

Mode —Machine: ESA_1.cisco.com Change Mode...

Centralized Management Options

Creating New Settings for Machine: ESA_1.cisco.com

Note: Creating new settings for this machine will override the settings currently inherited from Cluster: Gear 1.

Start with default settings

Copy from: Cluster: Gear 1

Cluster: Gear 1

Cancel Submit

Override setting output:

Mode —Machine: ESA_2.cisco.com Change Mode...

Centralized Management Options

Sophos Anti-Virus Overview

Anti-Virus Scanning by Sophos Anti-Virus:	Enabled
Virus Scanning Timeout (seconds):	60
Automatic Updates:	Enabled

Edit Global Settings...

After clicking on the **Edit Global Settings...** the EULA displays:

Mode —Machine: ESA_2.cisco.com Change Mode...

Centralized Management Options

(Sophos Anti-Virus) License Agreement

To enable Sophos Anti-Virus scanning, please review and accept the license agreement below.

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTERED AS THE END USER YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT OR AVAILABLE AT THE TIME OF YOUR ORDER (COLLECTIVELY THE "AGREEMENT"). TO THE EXTENT OF ANY CONFLICT BETWEEN THE TERMS OF THIS END USER LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE AGREEMENT, THE SUPPLEMENTAL LICENSE AGREEMENT SHALL APPLY. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU ARE REPRESENTING THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND BINDING YOURSELF TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY

Decline Accept

Accept the EULA and your commit changes.

The settings for Sophos is reflected on the mail policy and no longer shows "Not Available".

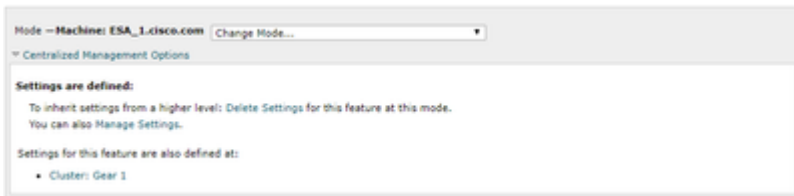
Remove Machine Override to Fall Back to Cluster Level

To remove the machine override settings:

1. Go to **Machine Mode** from the drop-down menu.
2. Click to expand the **Centralized Management Options**.

3. Click on the **Delete Settings**.
4. Click the **Delete** button and the settings fall back to the higher level (Group or Cluster, whichever is configured).
5. Verify the settings are properly configured on the higher level selected.
6. **Commit Changes** to save this setting.

Sample Output:



Related Information

- [Cisco Email Security Appliance - End-User Guides](#)
- [Technical Support & Documentation - Cisco Systems](#)