

# Configure Packet Capture in Email Security Appliance GUI

## Contents

[Introduction](#)

[Background Information](#)

[Procedure](#)

[Conclusion](#)

## Introduction

This document describes how enable a packet capture in Cisco Email Security Appliance.

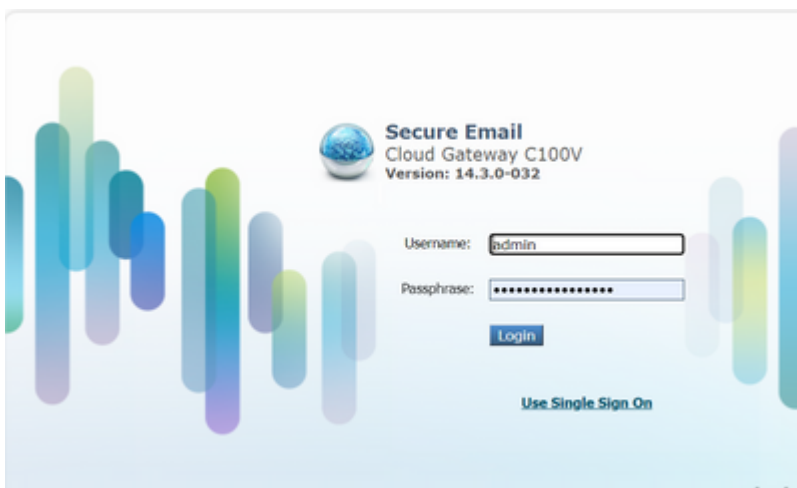
## Background Information

Packet capture intercepts and analyzes the network traffic that passes through the Cisco Email Security Appliance. It enables administrators to monitor network traffic, detect potential security threats, and troubleshoot network issues. Packet capture can be enabled on Cisco Email Security Appliance through GUI or CLI.

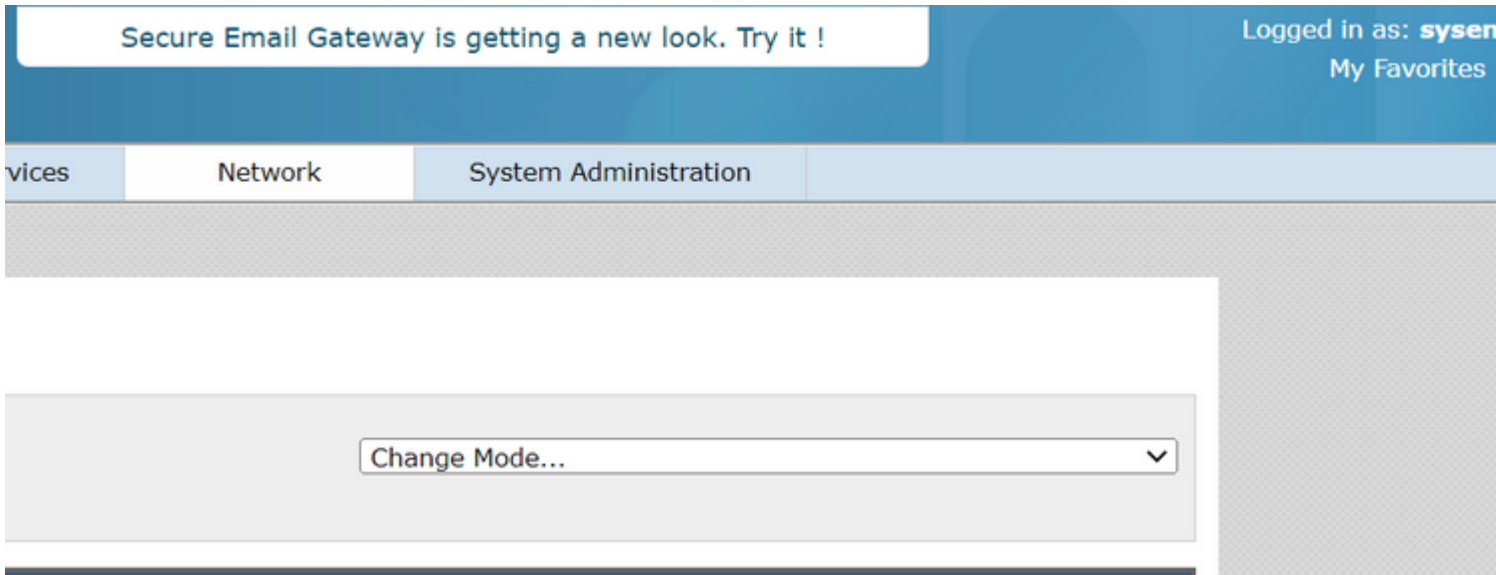
## Procedure

In order to configure a packet capture, complete this procedure:

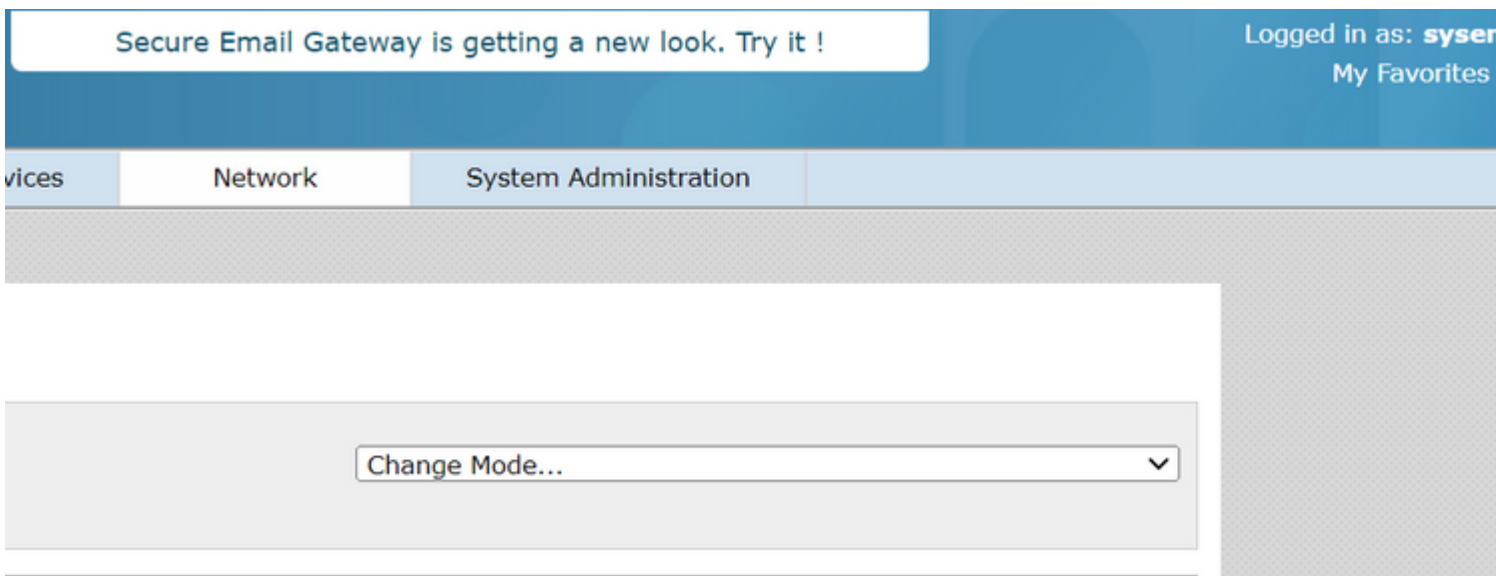
1. Log in to the Cisco Email Security Appliance with administrator credentials.



2. Hover the mouse in the Help And Support settings on the top right corner.



3. Click **Packet Capture**.



4. Scroll down to Packet Capture Settings and click **Edit Settings**.

Packet Capture Settings	
Capture File Size Limit:	10 MB
Capture Duration:	Run Capture Until File Size Limit Reached
Interfaces Selected:	Data 1
Filters Selected:	(tcp port 25)

5. Enter the Packet Capture Settings:

- Capture File Size Limit
- Capture Duration
- Interfaces

Packet Capture Settings	
Capture File Size Limit: <span>?</span>	<input type="text" value="10"/> MB <i>Maximum file size is 200MB</i>
Capture Duration:	<input checked="" type="radio"/> Run Capture Until File Size Limit Reached <input type="radio"/> Run Capture Until Time Elapsed Reaches <input type="text"/> <input type="radio"/> Run Capture Indefinitely <p><i>The capture can be ended manually at any time; use the settings should end automatically.</i></p>
Interfaces:	<input checked="" type="radio"/> Use selected interfaces <input checked="" type="checkbox"/> Data 1 <input type="checkbox"/> Data 2 <input type="radio"/> Use all interfaces

6. Configure the Packet Capture Filters.

Packet Capture Filters	
Filters:	<p><i>All filters are optional. Fields are not mandatory.</i></p> <input type="radio"/> No Filters <input type="radio"/> Predefined Filters <span>?</span> Ports: <input type="text" value="25"/> Client IP: <input type="text"/> Server IP: <input type="text"/> <input checked="" type="radio"/> Custom Filter <span>?</span> <input type="text" value="host 10.10.10.1"/>

**Note:** It is recommended to use a Custom Filter, and add the destination ip address with the format of **host x.x.x.x**.

In case of multiple destination ip addresses, the correct format is **host x.x.x.x or host x.x.x.x**.

In the case where a specific port is to be captured, use the format **host x.x.x.x && port x**.

7. Click **Submit** and **Start Capture**.

8. Click **Stop Capture** when needed to stop the capture.

**Current Packet Capture**

Status: Capture in progress (Duration: 6s)  
File Name: C100V-420D675A2129EFC06C8B-23C34D457581-20230330-155622.cap (Size: 0B)

Current Settings:  
Max File Size: 10MB  
Capture Limit: File Size  
Capture Interfaces: Data 1  
Capture Filter: (tcp port 25)

9. Choose the capture from Manage Packet Capture Files menu and click **Download File** to save it to the local computer.

**Manage Packet Capture Files**

C100V-420D675A2129EFC06C8B-23C34D457581-20230330-155622.cap (808B)

Delete Selected Files Download File

10. The file is now ready to be checked with a packet analyzer tool.

## Conclusion

Packet capture is an essential feature that enables administrators to monitor network traffic and detect potential security threats. This article has provided a step-by-step procedure on how to enable packet capture on the Cisco Email Security Appliance GUI.