Cisco Email Security Appliance 11 Lab v1.1

Last Updated: 28-AUGUST-2018

About This Demonstration

This guide for this preconfigured demonstration includes:

Requirements

The table below outlines the requirements for this preconfigured demonstration.

Table 1. Requirements

Required	Optional
• Laptop	• Cisco AnyConnect®

About This Solution

Cisco Email Security formerly Cisco IronPort Email Security, delivers industry-leading inbound and outbound email cleansing and control, offering high availability email protection against the constant, dynamic, rapidly changing threats affecting email today in a variety of form factors to fit customer needs.

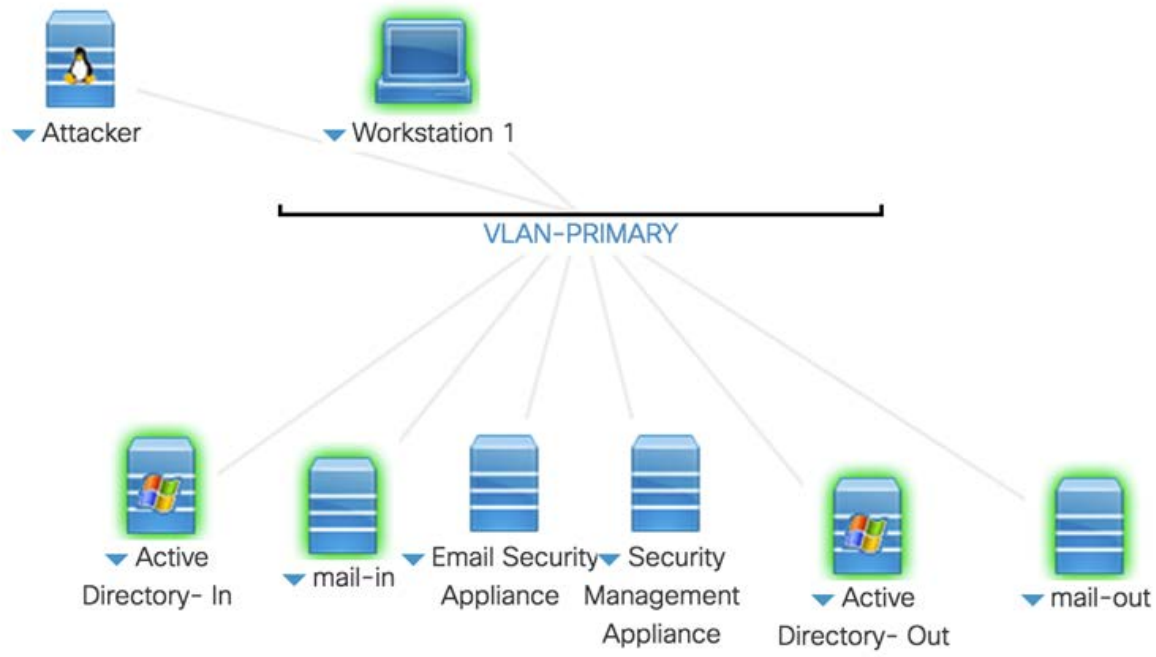
Read the Email Security Overview for detailed information on Cisco Email Security features and benefits, available form factors, Cisco differentiators, and more.

For additional information about Cisco Cloud Email Security, visit http://www.cisco.com/go/cloudemail.

Topology

This content includes preconfigured users and components to illustrate the scripted scenarios and features of the solution. Most components are fully configurable with predefined administrative user accounts. You can see the IP address and user account credentials to use to access a component by clicking the component icon in the **Topology** menu of your active session and in the scenario steps that require their use.

Figure 1. dCloud Topology

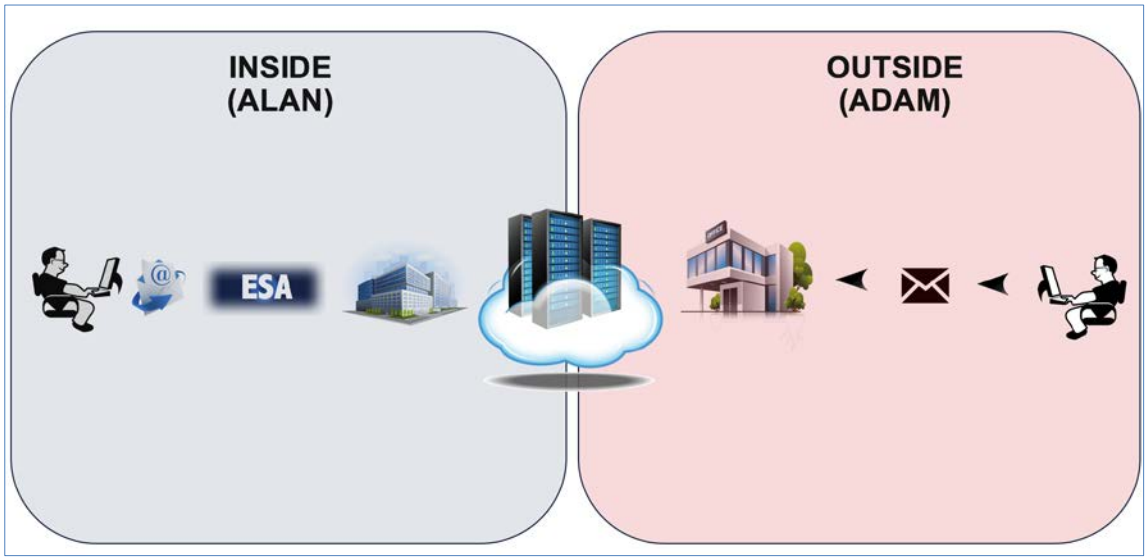


The logical topology for all lab scenarios are based on the following: -

Alan represents an internal user and uses Microsoft Outlook as his mail client. The corporate mail servers are Microsoft Exchange which in turn forwards to the Cisco Email Security solution for policy control and email hygiene before routing messages.

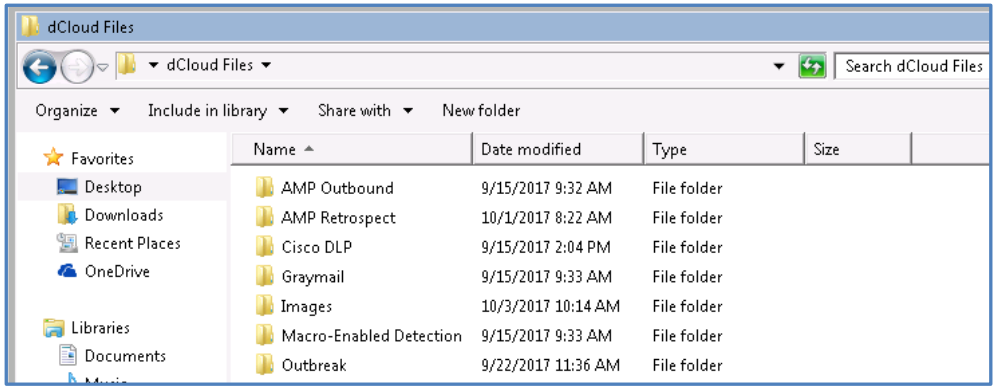
Adam represents an external user located anywhere on the internet, Adam also uses the Microsoft Outlook client for managing his mailbox, however the mail server platform used here is arbitrary.

Alan - alan@dcloud.cisco.com Adam - adam@dcloud-out.cisco.com



Supporting Files

This lab uses supporting files within various scenarios; these are all located in the dCloud Files folder on the desktop of the Workstation.



NOTE: In some scenarios Security warnings may be presented warning the user to exercise caution when executing certain supporting files, these are perfectly safe. All files that are classified as malicious are in fact benign and present no harm to any environment.

Get Started

BEFORE PRESENTING

Cisco dCloud strongly recommends that you perform the tasks in this document with an active session before presenting in front of a live audience. This will allow you to become familiar with the structure of the document and content.

It may be necessary to schedule a new session after following this guide in order to reset the environment to its original configuration.

PREPARATION IS KEY TO A SUCCESSFUL PRESENTATION.

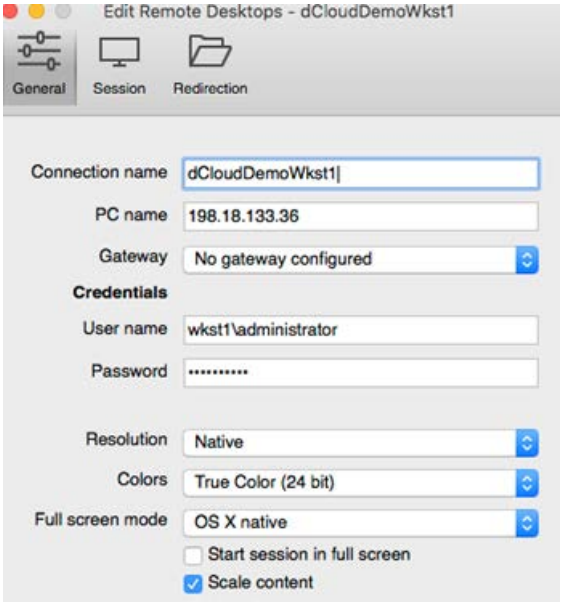
1. Follow the steps to schedule a session of the content and configure your presentation environment.
2. Initiate your dCloud session. [Show Me How]

NOTE: It may take up to 10 minutes for your session to become active.

3. For best performance, connect to the workstation with **Cisco AnyConnect VPN** [Show Me How] and the **local RDP client on your laptop** [Show Me How]

Workstation 1: **198.18.133.36**, Username: **administrator**, Password: **C1sco12345**

NOTE: You can also connect to the workstation using the Cisco dCloud Remote Desktop client [Show Me How]. The dCloud Remote Desktop client works best for accessing an active session with minimal interaction. However, many users experience connection and performance issues with this method.



Case Study

Voyage Corp

Voyage Corp are a US based company and major supplier of IT equipment and services to the retail and financial sector across the United States and Europe. With significant investment in key area of the business has resulted in the company slowly expanding its global reach to Asia.

Its business model relies on electronic transactions with key customers and suppliers. All communications between internal and external parties is done primarily by electronic mail.

Email use has increased by over 20% over the past two years and Voyage Corp is seeing a huge spike in the number of ransomware and malware attacks coming into their mail systems. Recently appointed Chief Technology Officer (CTO) Mark Valentino ordered a review of all strategic communications systems starting with what he labelled the most critical of them all, email.

Following a lengthy review of the leading players in the Secure Email Gateway business as reported by the Gartner Magic Quadrant, Voyage Corp opted for the Cisco Email Security solution as its email security platform of choice for its ability to defend against todays sophisticated attacks. In the words of the CTO, Cisco is a leader in the Email Security business with leading edge, state of the art features and is backed with years of unrivalled product innovation.

Voyage Corp uses Microsoft Exchange to manage email transactions and communications between internal and external environments, however has investigated retiring on premise for Microsoft Exchange Online; no decision to migrate has yet been made.

Potential Threats and Security Concerns

Voyage Corp wants to make sure that it receives and processes only messages from authenticated sources where possible and has been forced to tighten their security posture after pressure from external parties who are governed by third party legislation, namely HIPAA and PCI-DSS.

Voyage Corp also wants to make sure that it can receive and retrieve documents from outside its corporate network as safely as possible following an increase in documents coming into several business functions as attachments to email the InfoSec team are concerned the organization may be vulnerable.

Security Solution

Voyage Corp opted for the **Cisco Email Security Solution** to run on their existing virtual platform, in order to remain as secure Voyage Corp invested in the following Cisco Email Security features: -

- Advanced Malware Protection
- Sophos Anti-Virus
- McAfee Anti-Virus
- Outbreak Filters
- Data Loss Prevention
- Image Analyzer

Objective

This lab will run the through a series of exercises to implement the necessary security controls to defend against todays sophisticated attacks. Email remains a primary attack vector and given its importance to Voyage Corp, it is vital that all avenues are sufficiently defended.

Though not strictly required, it is however advisable that all scenarios are run in sequence.

Scenario 1. Data Loss Prevention Policy (DLP)

Use Case

Voyage Corp has been working within an eco-system of business partners and subsequently the volume of email exchanged between them has steadily increased. One case in point being the Human Resources (HR) department who now are inundated with requests for personal employee information by the local authority as part of a county wide initiate to ensure that all staff are working in compliance with local laws. The type of information that is frequently requested is employment history, tax codes and Social Security Numbers.

Previously, this information was sent by local courier. However, this is now becoming an issue as the time to print and then prepare these as packages is becoming a little too onerous on the HR department, who are already down on headcount. Furthermore, the cost of sending these secure packages has increased by 10% and the Chief Accountant has been tasked with implementing cost control measures.

The HR lead instructed his team to send this information using email, citing the many benefits of using existing technology such as speed and cost. For over 12 months this helped reduce the administrative burden on the department, however, following a policy review, the information security (InfoSec) group within the company has instructed that this must not continue as it represents a serious violation to the company's security policy.

InfoSec have instructed the Cisco Email Security administrators to implement the necessary controls immediately to prevent this from happening.

Security Control

The Cisco Email Security solution can inspect the message and attachments and make a decision on whether Alan has indeed sent information that is prohibited; this is achieved by using the Cisco DLP feature, which is part of the Premium license which was purchased by the Voyage.

Objective

This scenario will walk through the configuration of an end to end Data Loss Prevention (DLP) policy to address this use case where an internal user Alan wishes to send an email to an external user Adam. Under normal working conditions the exchange of email traffic from an internal user to an external party would be conventional and normal task, however this scenario will ensure that Alan does not send anything outside of the company that represents a risk to his organization.

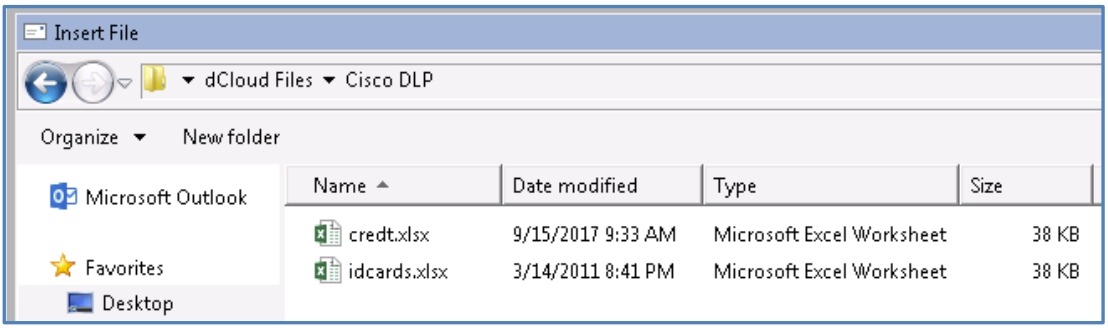
Steps

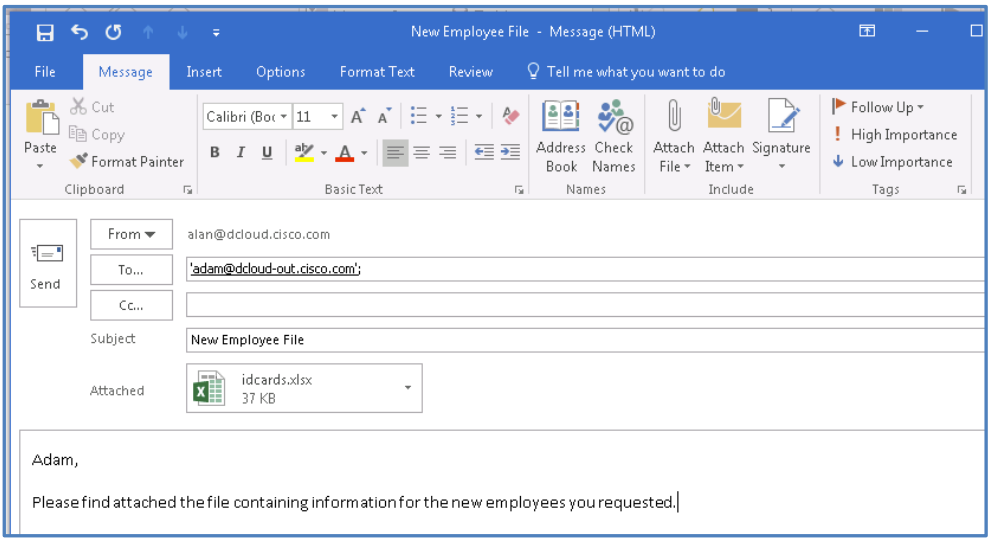
Task - Sending an email with an attachment without Cisco DLP (Estimated time to complete: 5 min)

DLP policies are relatively easy to create once the criteria that will trigger a DLP Policy have been identified and then what action should be taken on it thereafter.

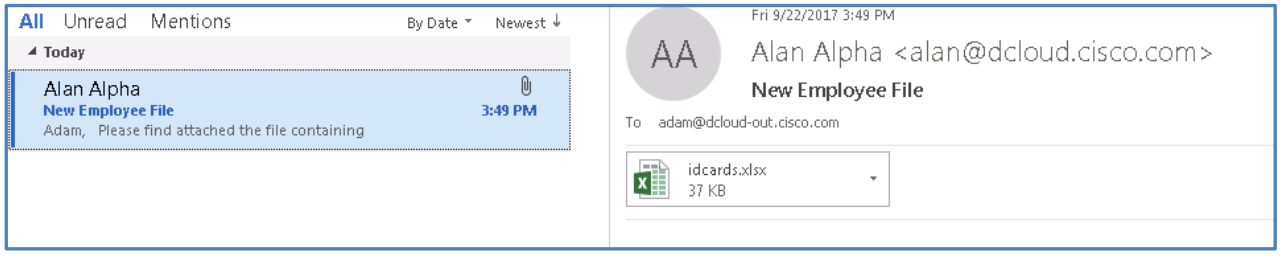
For this scenario, internal user Alan will send a Microsoft Excel file that contains Social Security numbers to an external interest; Adam, with and without Cisco DLP policies configured to see the effect on the end results.

1. Launch Microsoft Outlook from the taskbar of Workstation 1 (known henceforth as workstation) and prepare an email with the following parameters: -
    - **From**: alan@dcloud.cisco.com
    - **To**: adam@dcloud-out.cisco.com
    - **Subject**: New Employee File
    - **Body**: Adam, Please find attached the file containing information for the new employees you requested.
    - **Attachment**: IdCards.xlsx - located on the desktop under the Cisco DLP sub-folder.





2. Send the email - Force the synchronization process by clicking **Send/Receive Folder** or by pressing the **F9** key.
3. Navigate back to Adams inbox and synchronize the mail client by clicking the **Send/Receive Folder** button or pressing the **F9** key 2-3 times.
4. As there is no DLP policy present, the email with attachment will be delivered to Adams mailbox, this is expected behaviour. Open the attachment to view the content of the Microsoft Excel file, the content should be clearly visible and the email message unaltered.



5. Though the message has been delivered to its intended recipient it still has been processed by the multiple Cisco Email Security solution engines, and if at point any one of these engines deemed the message or attachment to contain something that may be untoward, such as a viral attachment then the configured action would have been applied.
6. The next task configures the Cisco Email Security solution with the DLP feature to implement the necessary controls to prohibit sensitive data from leaving the organization.

Task - Configuring Cisco DLP Text Resources (Estimated time to complete: 5 min)

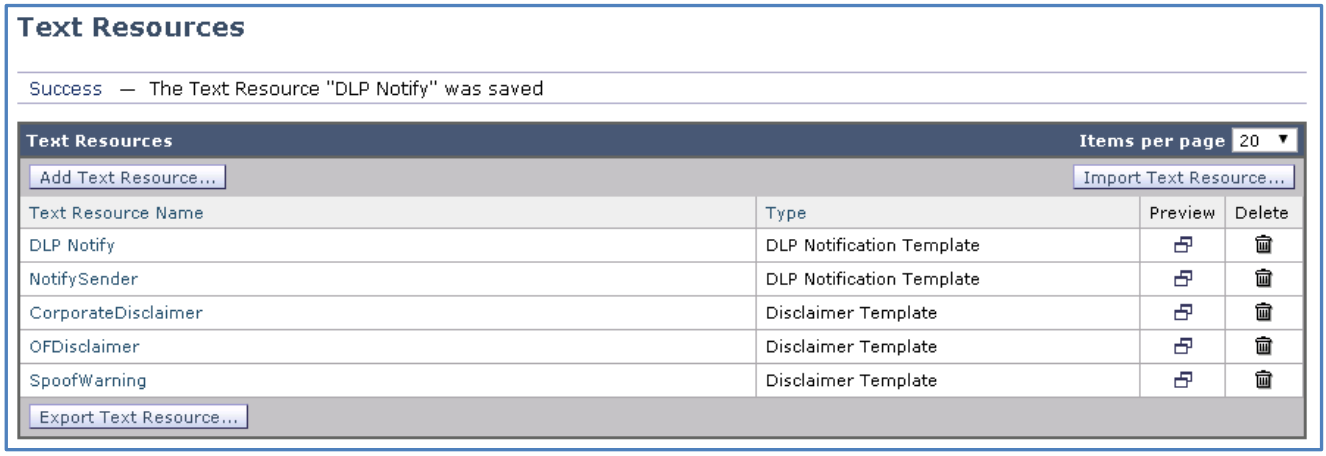
The first step in configuring a DLP policy is to create (custom) text resources. Text resources are text templates that can be attached to messages or sent as messages. For example, a text resource can be created to advise a user that an action has been taken on an email that is in violation of the configured policy. This provides valuable feedback to a user as to why an action has been taken and even what needs to be done next, such as internal training or leveraging encryption.

This scenario will create a *DLP Notification* template and a *DLP Disclaimer* template that will later be used within the Cisco DLP policy.

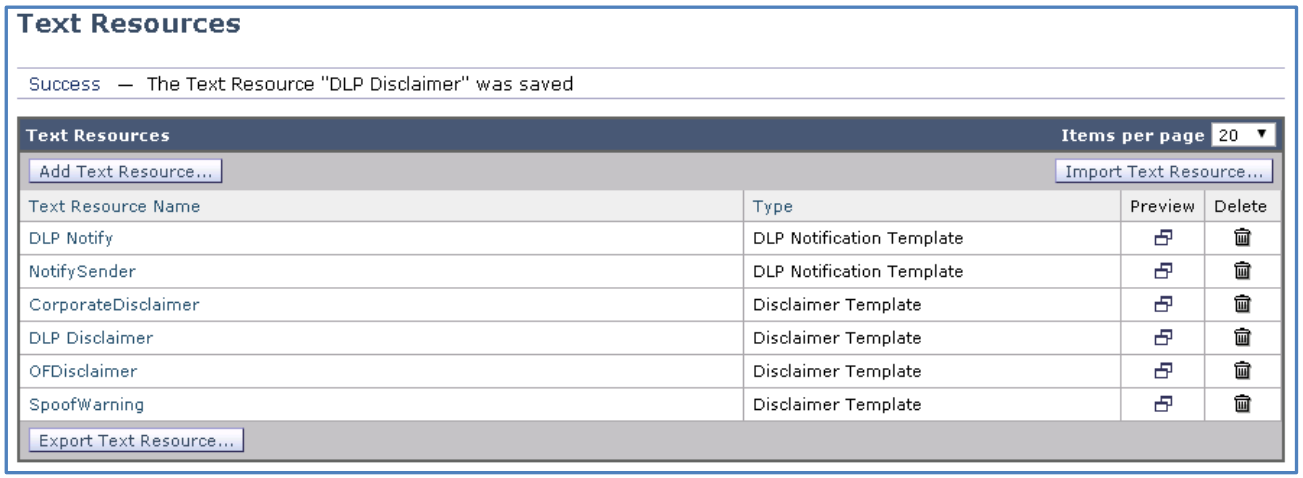
1. From the workstation launch Google Chrome, acknowledge the warning that connection is unsafe by clicking **Advanced** and then **Proceed to esa.dcloud.cisco.com (unsafe)** and the default page will automatically load, this will be the Cisco Email Security GUI page. Log in with the following credentials: -
    - **Username**: admin
    - **Passphrase**: C1sco12345
2. Upon successful authentication, the Cisco Email security landing page, My Dashboard will be presented.
3. Navigate to **Mail Policies > Text Resources** to be presented with the default and pre-configured text resources. Click the **Add Text Resource** button to create a custom notification template, using the following information:
    - **Name**: DLP Notify

- **Type**: DLP Notification Template
- **HTML**: You have sent an email that is inconsistent with corporate policies on acceptable use

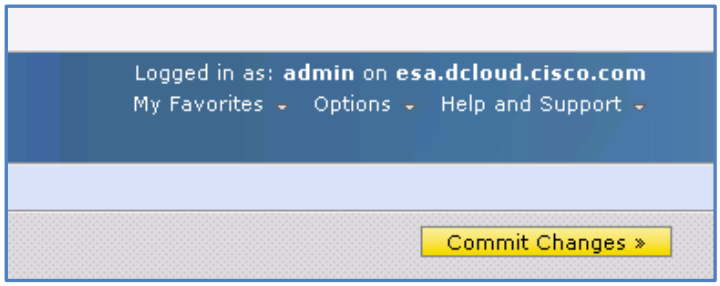
4. Click **Submit** to create the text resource and confirm that is has been added to the list of previously configured text resources.

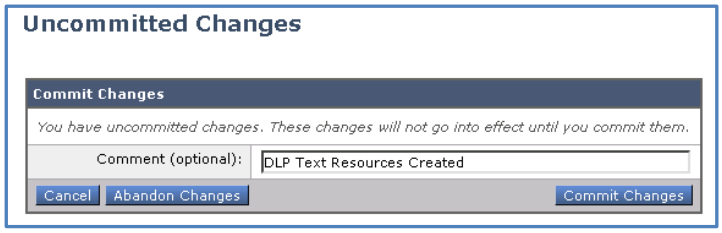


5. Repeat this step for the other text resource, this time changing the *Type* to Disclaimer Template.
   - **Name**: DLP Disclaimer
   - **Type**: Disclaimer Template
   - **HTML**: This email may contain confidential and privileged material for the sole use of the intended recipient only.
6. Click **Submit** to create the text resource.



7. Once complete, ensure the changes are applied by clicking the **Commit Changes** button - top right of screen, adding optional comments if desired.

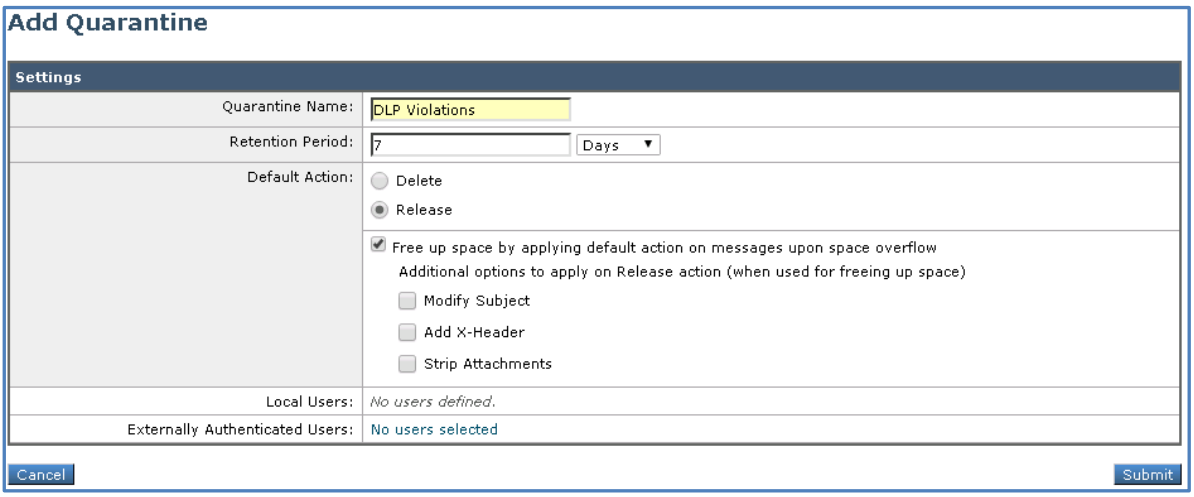




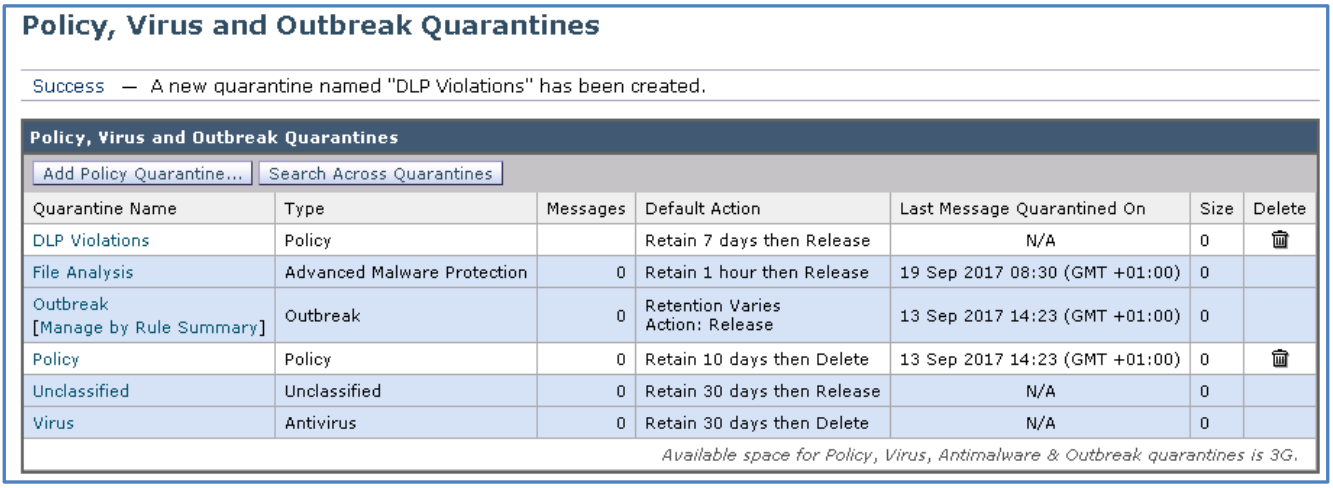
Task - Configuring a DLP Quarantine (Estimated time to complete: 5 min)

When the Cisco Email Security solution detects possible malware or content that is not allowed as instructed within in incoming or outgoing messages, it can send those messages to quarantine instead of deleting them immediately. A quarantine holds these messages safely for a period, allowing an administrator to review them, or to await an update that will better evaluate the safety of the message if additional security engines are being queried.
This task will create a separate quarantine for messages that violate the Cisco DLP policy to be placed into before they are reviewed and either released to their intended recipient or permanently deleted.

1. Navigate to **Monitor > Policy, Virus and Outbreak Quarantines** and select the **Add Policy Quarantine** button. Create a new quarantine using the following information:
    - **Quarantine Name**: DLP Violations
    - **Retention Period**: 7 Days
    - **Default Action**: Release



2. Click **Submit** to create the quarantine.



3. Once complete, ensure the changes are applied by clicking the **Commit Changes** button - top right of screen, adding optional comments if desired.

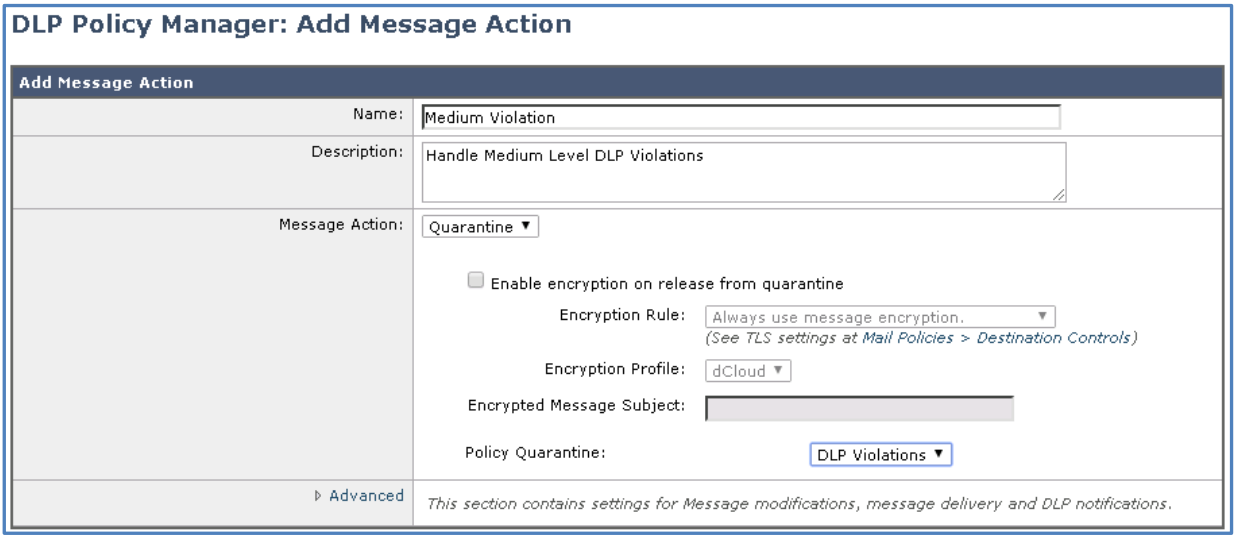
Task - Configuring a DLP Policy Customizations (Estimated time to complete: 5 min)

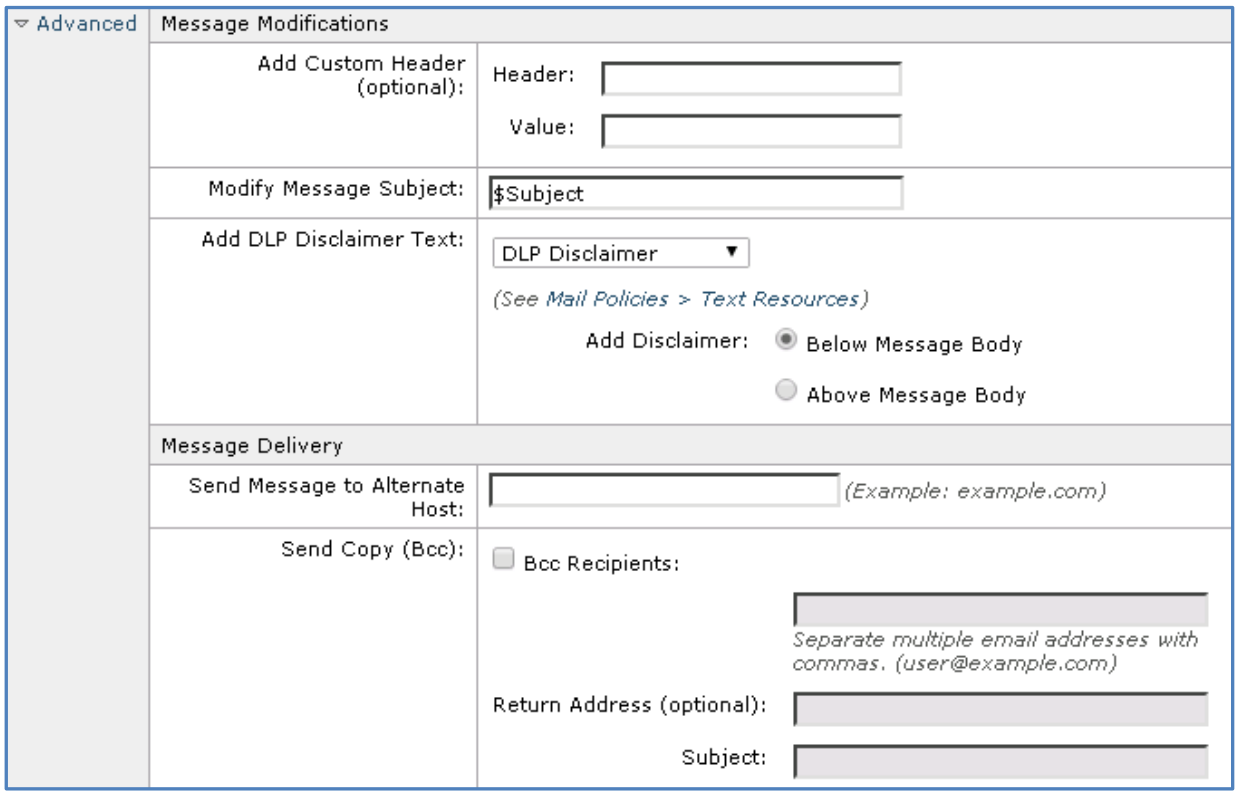
Primary and Secondary actions can be applied when the Cisco Email Security Solution detects a possible DLP violation in an outgoing message. Different actions can be assigned for different violation types and severities.

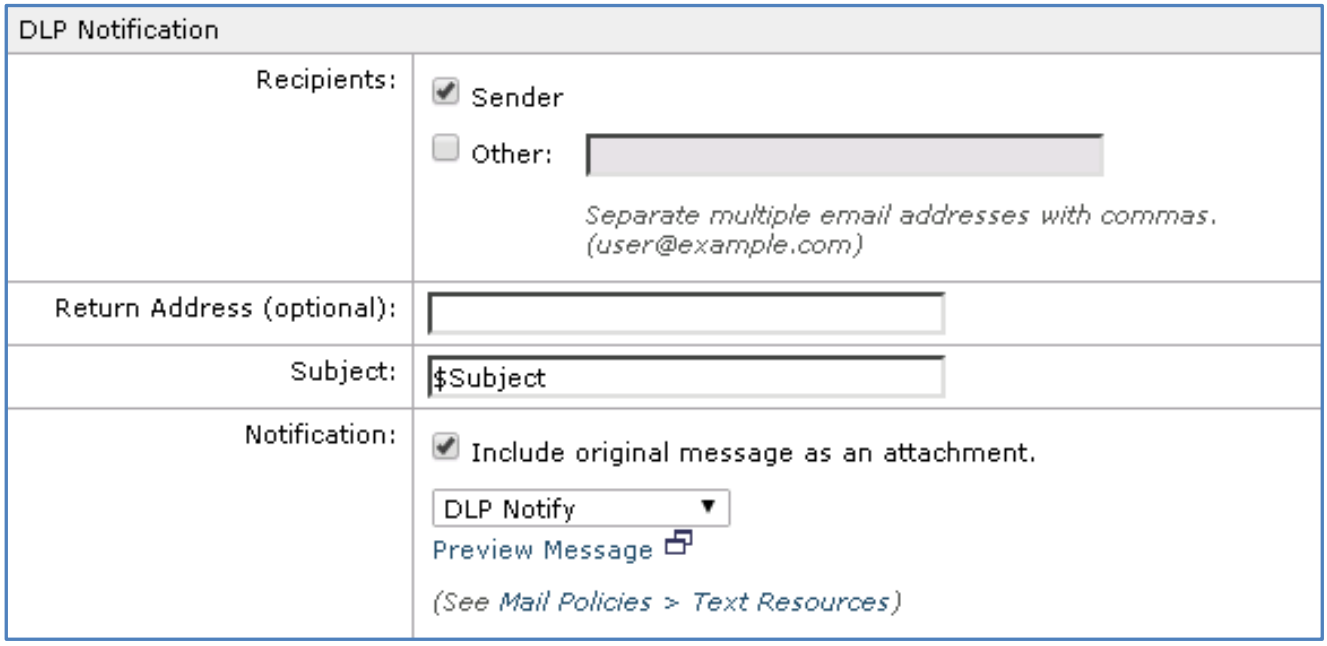
- **Primary actions include**: Deliver, Drop or Quarantine
- **Secondary actions include**: Encrypting, modifying subject header or adding disclaimers.

This task will create a message action that will be applied when a violation for a policy has been triggered.

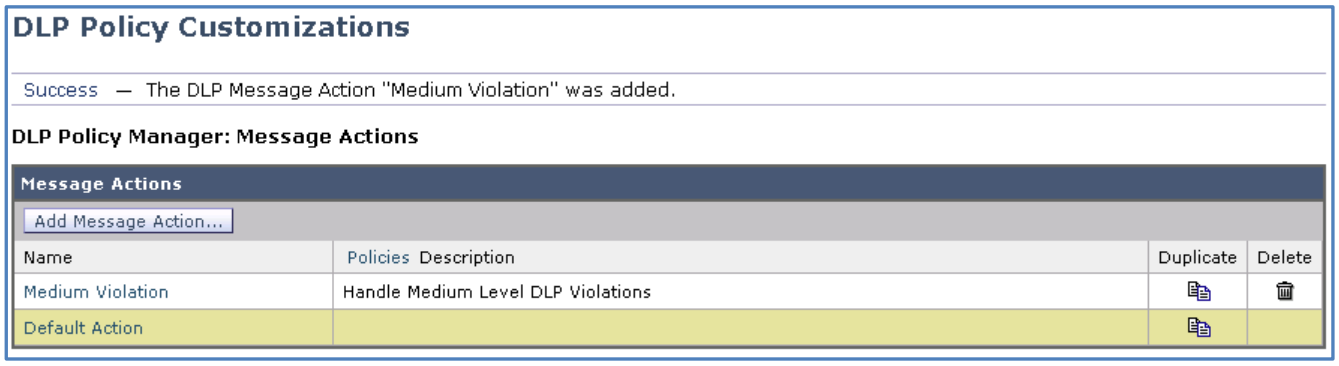
1. Navigate to **Mail Policies > DLP Policy Customizations** and select the **Add Message Action** button. Create the message action using the following information: -
    - **Name**: Medium Violation
    - **Description**: Handle Medium Level DLP Violations
    - **Message Action**: Quarantine
    - **Policy Quarantine**: DLP Violations (created in previous task - Under Advanced)
    - **Modify Message Subject**: $Subject
    - **Add DLP Disclaimer Text**: DLP Disclaimer
    - **Add Disclaimer**: Tick Below Message Body
    - **DLP Notification**: Tick Sender
    - **Subject**: $Subject
    - **Notification**: Tick Include original message as an attachment and select DLP Notify







2. Click **Submit** to create the action.



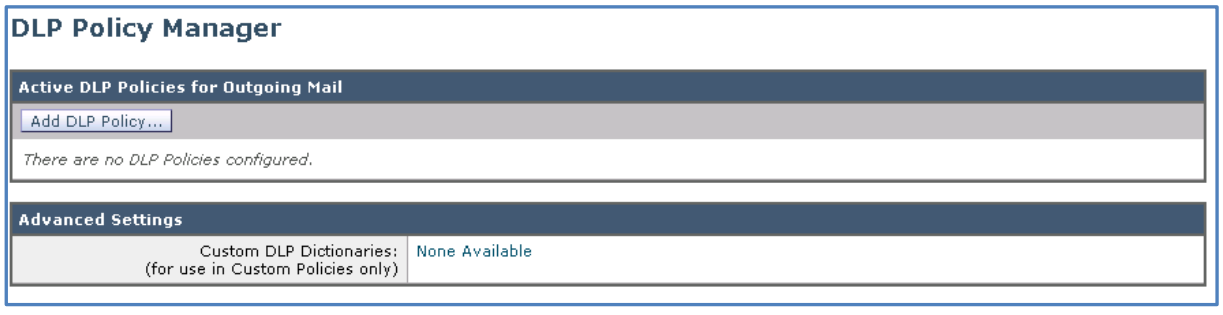
3. Once complete, ensure the changes are applied by clicking the **Commit Changes** button - top right of screen, adding optional comments if desired.

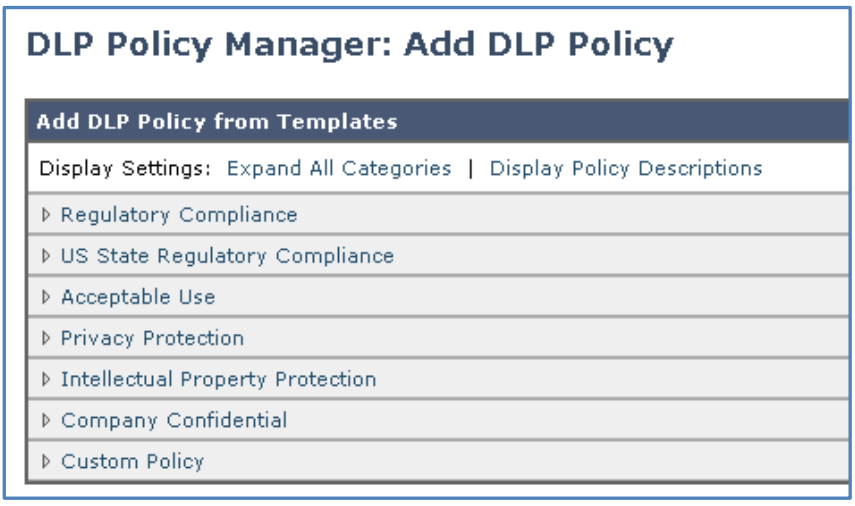
Task - Configuring a DLP Policy to Detect SSNs (Estimated time to complete: 5 min)

A DLP policy is required to determine what to look for inside an email message that may be inconsistent with corporate policy. The Cisco DLP engine comes installed with over 100 pre-configured commonly used policies, further granular control can be achieved by customising a policy to tailor it to most requirements.

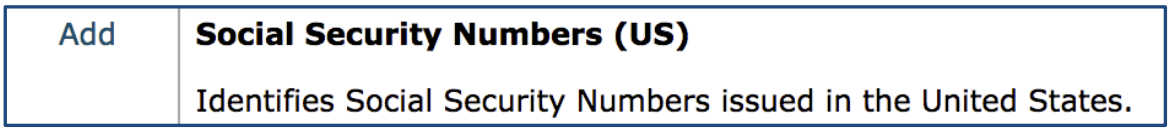
This task will make us of one of the pre-configured templates, to identify Social Security Numbers (SSN), and use the customisation configured in the previous task, Medium Violation, to determine what action will be taken - send the message to the quarantine and notify the sender of this violation.

1. Navigate to **Mail Policies > DLP Policy Manager** and select the **Add DLP Policy** button.



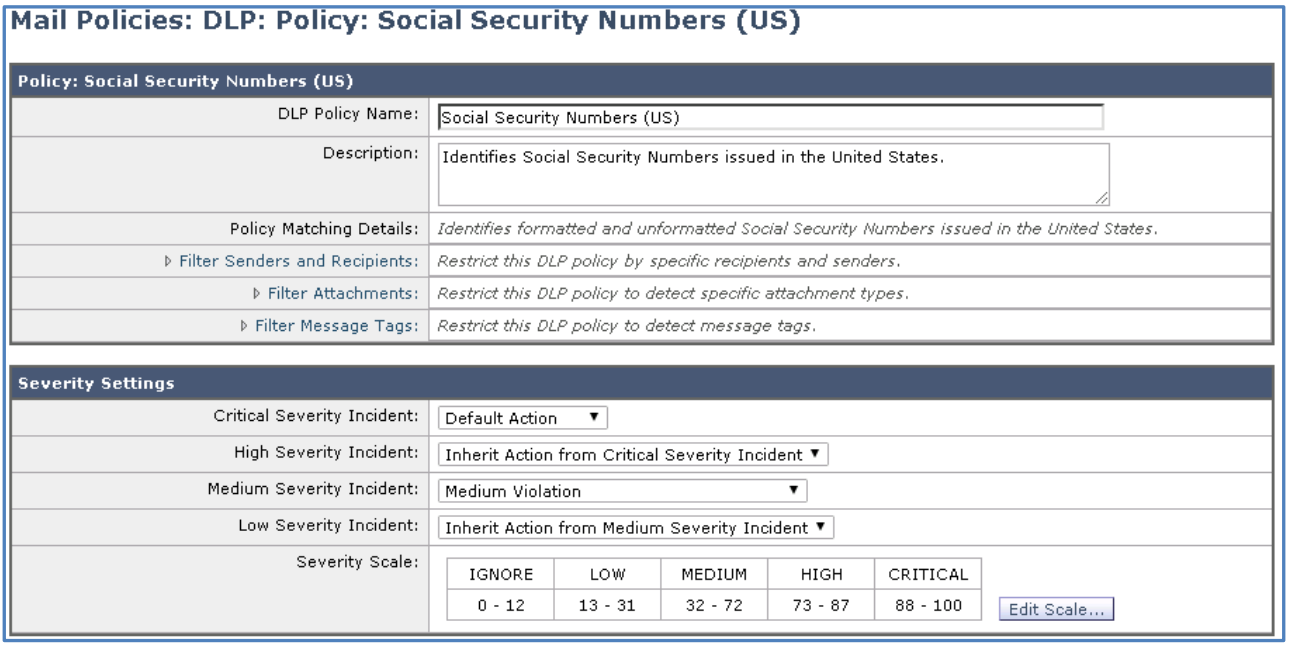


2. Select the template Privacy Protection and scroll down to Social Security Numbers (US) and click Add.

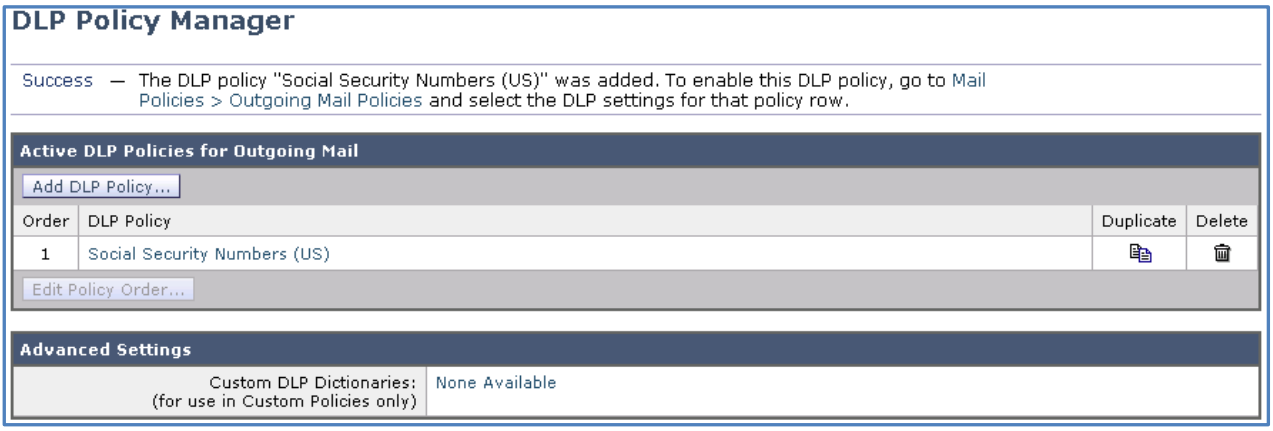


3. Edit the policy, by changing the **Severity Settings** to **Medium Violation**. This instructs the policy to use the customized violation settings configured earlier, such as directing a message that violates this policy to the quarantine.

    - **Medium Severity Incident**: Medium Violation



4. Click **Submit** to create the policy.

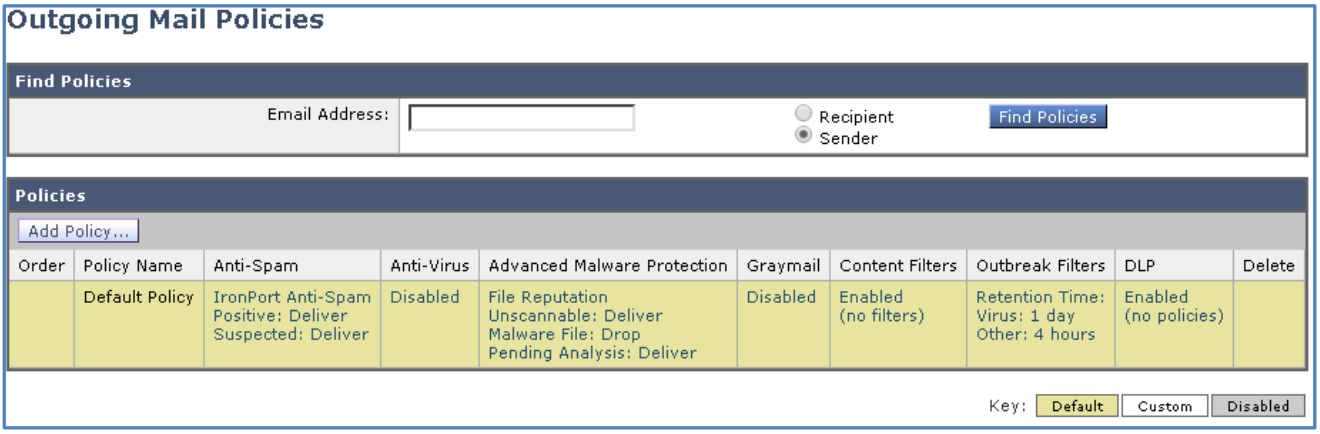


5. Once complete, ensure the changes are applied by clicking the **Commit Changes** button - top right of screen, adding optional comments if desired.

Task - Configuring an outgoing Mail Policy (Estimated time to complete: 2 min)

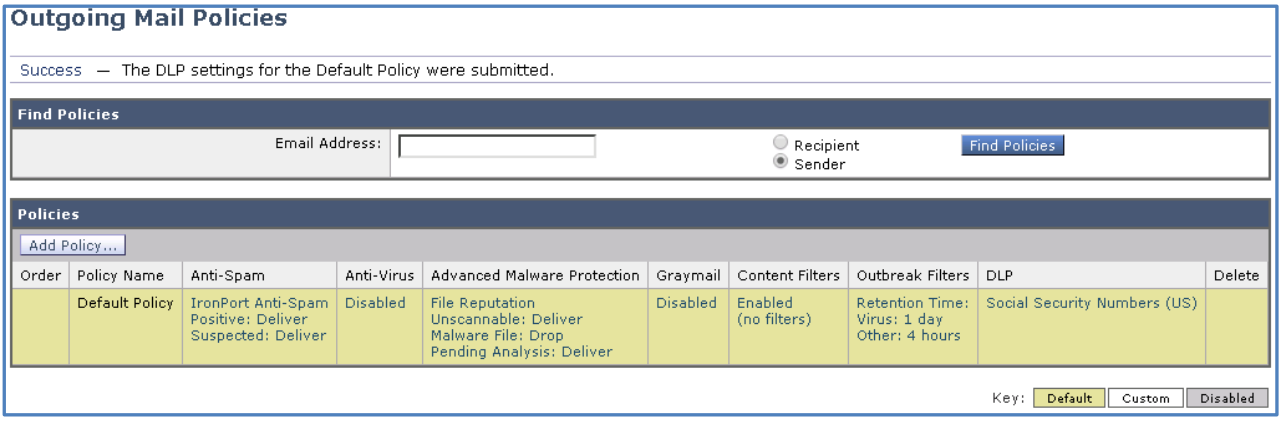
The final step is to configure an outgoing mail policy to tie all the components configured previously together. Mail policies can be either incoming or outgoing, however some features, such as data loss prevention can only be performed on outgoing messages.

1. Navigate to **Mail Policies > Outgoing Mail Policies** and click on the hyperlink **Enabled (no policies)** under the *DLP* column; it is here the policy that was previously defined is applied to the Default Policy.



2. Place a checkmark against the only policy in the list and then click **Submit**

3. Verify the DLP Policy has been added to the *DLP* section of the outgoing mail policy.

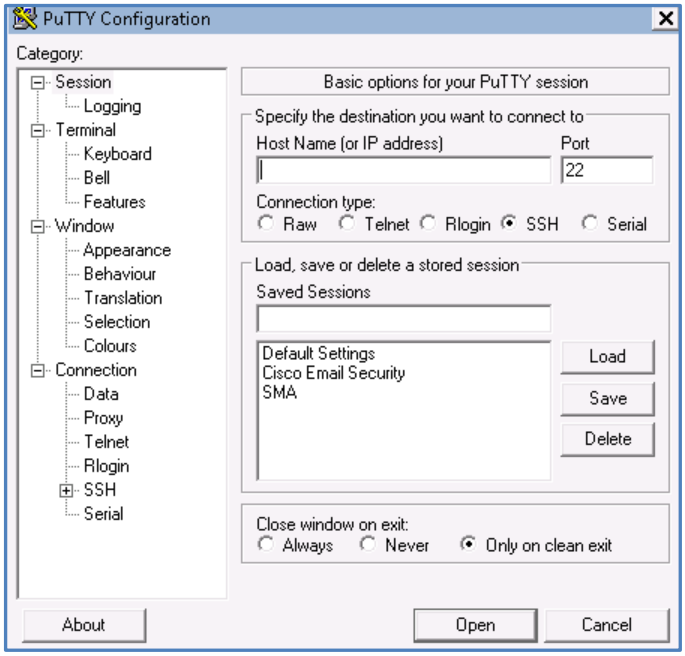


4. Finally, apply the change by clicking the **Commit Changes** button, adding optional comments if desired.

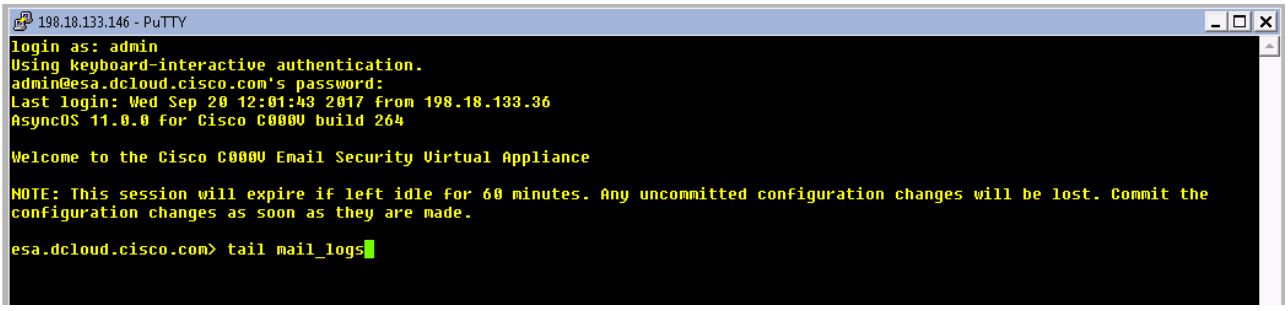
Task - Test the DLP Policy (Estimated time to complete: 10 min)

With all of the necessary components created and configured, the policy can be tested by sending an email with an attachment that should trigger a Medium violation in the policy. To assist in understanding how the Cisco Email Security solution processes messages and the various actions that are taken the CLI can be monitored to view real time information on each message.

1. From the workstation launch *Putty* located on the taskbar. Select Cisco Email Security from the Saved Sessions and click Open. Acknowledge any security warning presented.

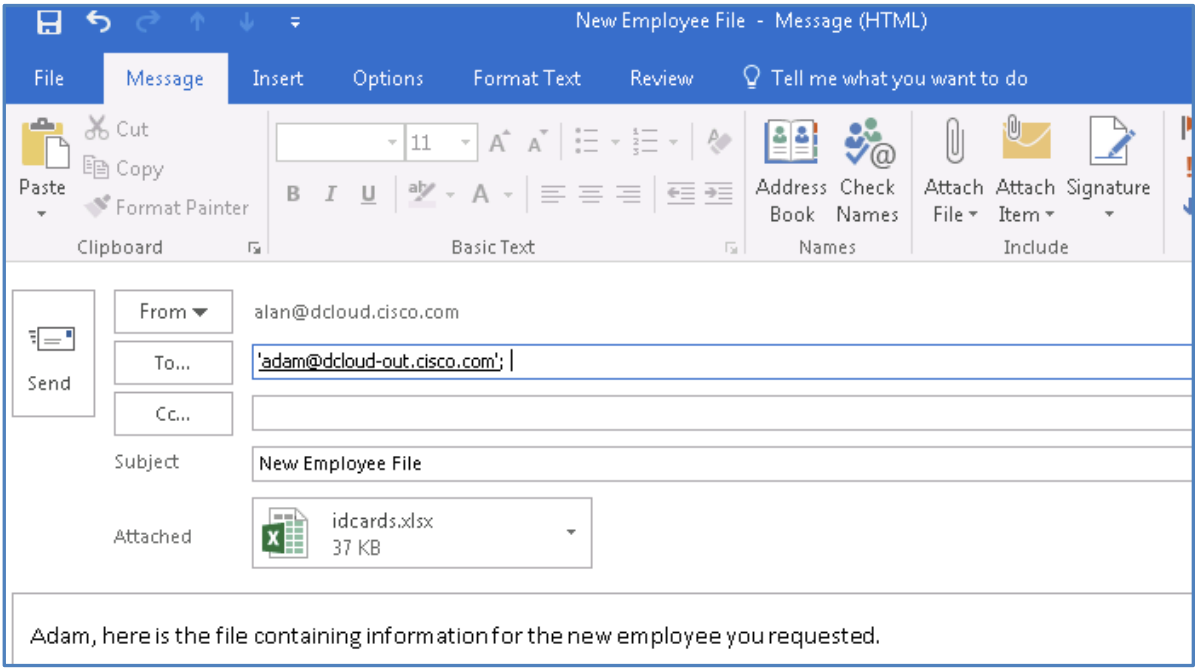


2. Log in using the credentials listed earlier in this document. Once logged in, issue the command **tail mail_logs** and press enter. Leave this running in the background and proceed to the next step.



NOTE: The tail command is used to print the last few lines from the logs mail logs on the terminal, this especially useful to read the last few lines to know about the error messages or events as they happen. This can be used against any of the 30+ log files available on the Cisco Email Security solution, type **tail** on its own and press enter to view the list of logs.

3. Launch Microsoft Outlook from the taskbar of Workstation and prepare an email with the following parameters:
    - **From**: alan@dcloud.cisco.com
    - **To**: adam@dcloud-out.cisco.com
    - **Subject**: New Employee File
    - **Body**: Adam, Please find attached the file containing information for the new employees you requested.
    - **Attachment**: IdCards.xlsx - located on the desktop under the Cisco DLP sub-folder.



4. Send the email - Force the synchronization process by clicking **Send/Receive Folder** or by pressing the **F9** key.
5. Switch back to the CLI window opened in the first step, it may take a few moments for the logging to appear.
6. The first point of interest is the fact the message contains a violation, the risk factor of 35 falls within the range of a Medium violation for Social Security Numbers

```
Fri Sep 29 16:43:43 2017 Info: MID 279740 ready 55144 bytes from <alan@dcloud.cisco.com>
Fri Sep 29 16:43:43 2017 Info: MID 279740 matched all recipients for per-recipient policy DEFAULT in the outbound table
Fri Sep 29 16:43:43 2017 Info: MID 279740 AMP file reputation verdict : UNKNOWN
Fri Sep 29 16:43:45 2017 Info: MID 279740 Outbreak Filters: verdict negative
Fri Sep 29 16:43:45 2017 Info: MID 279740 attachment 'idcards.xlsx'
Fri Sep 29 16:43:45 2017 Info: MID 279740 DLP violation. Severity: MEDIUM (Risk Factor: 35). DLP policy match: 'Social Security
 Numbers (US)'.
Fri Sep 29 16:43:45 2017 Info: Start MID 279741 ICID 0
Fri Sep 29 16:43:45 2017 Info: MID 279741 was generated based on MID 279740 by notify-copy filter 'Medium Violation'
Fri Sep 29 16:43:45 2017 Info: MID 279741 ICID 0 From: <MAILER-DAEMON@esa.dcloud.cisco.com>
Fri Sep 29 16:43:45 2017 Info: MID 279741 ICID 0 RID 0 To: <alan@dcloud.cisco.com>
Fri Sep 29 16:43:45 2017 Info: MID 279741 DomainKeys: cannot sign - no profile matches MAILER-DAEMON@esa.dcloud.cisco.com
Fri Sep 29 16:43:45 2017 Info: MID 279741 DKIM: cannot sign - no profile matches MAILER-DAEMON@esa.dcloud.cisco.com
Fri Sep 29 16:43:45 2017 Info: MID 279741 ready 57623 bytes from <MAILER-DAEMON@esa.dcloud.cisco.com>
Fri Sep 29 16:43:45 2017 Info: MID 279741 queued for delivery
Fri Sep 29 16:43:45 2017 Info: MID 279740 rewritten to MID 279742 by add-footer filter 'Footer Stamping'
Fri Sep 29 16:43:45 2017 Info: Message finished MID 279740 done
Fri Sep 29 16:43:45 2017 Info: New SMTP DCID 2538 interface 198.18.133.146 address 198.18.133.2 port 25
Fri Sep 29 16:43:45 2017 Info: MID 279742 quarantined to "DLP Violations" (DLP violation)
Fri Sep 29 16:43:45 2017 Info: Message finished MID 279742 done
```

7. Next, note the message was redirected to the custom DLP quarantine.

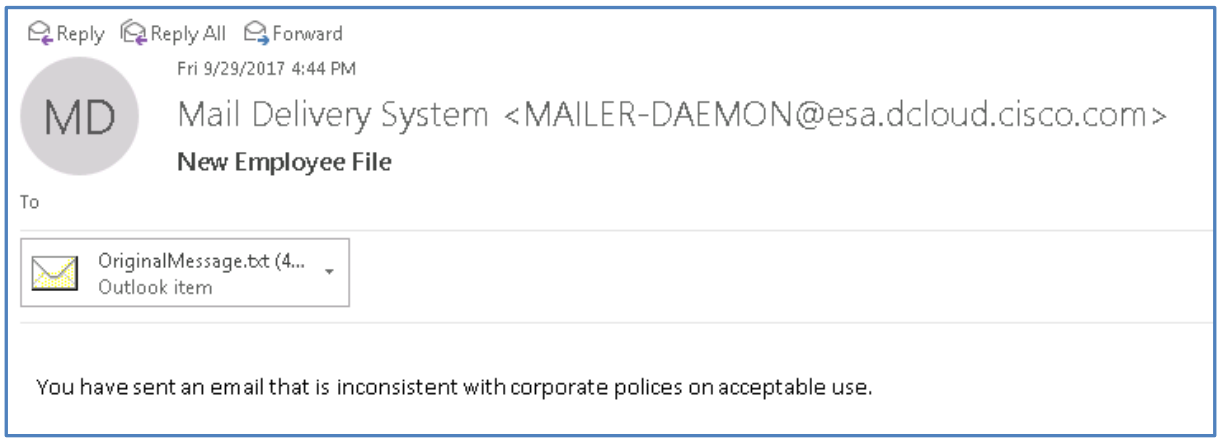
```
Fri Sep 29 16:43:43 2017 Info: MID 279740 Subject 'New Employee File'
Fri Sep 29 16:43:43 2017 Info: MID 279740 ready 55144 bytes from <alan@dcloud.cisco.com>
Fri Sep 29 16:43:43 2017 Info: MID 279740 matched all recipients for per-recipient policy DEFAULT in the outbound table
Fri Sep 29 16:43:43 2017 Info: MID 279740 AMP file reputation verdict : UNKNOWN
Fri Sep 29 16:43:45 2017 Info: MID 279740 Outbreak Filters: verdict negative
Fri Sep 29 16:43:45 2017 Info: MID 279740 attachment 'idcards.xlsx'
Fri Sep 29 16:43:45 2017 Info: MID 279740 DLP violation. Severity: MEDIUM (Risk Factor: 35). DLP policy match: 'Social Security
 Numbers (US)'.
Fri Sep 29 16:43:45 2017 Info: Start MID 279741 ICID 0
Fri Sep 29 16:43:45 2017 Info: MID 279741 was generated based on MID 279740 by notify-copy filter 'Medium Violation'
Fri Sep 29 16:43:45 2017 Info: MID 279741 ICID 0 From: <MAILER-DAEMON@esa.dcloud.cisco.com>
Fri Sep 29 16:43:45 2017 Info: MID 279741 ICID 0 RID 0 To: <alan@dcloud.cisco.com>
Fri Sep 29 16:43:45 2017 Info: MID 279741 DomainKeys: cannot sign - no profile matches MAILER-DAEMON@esa.dcloud.cisco.com
Fri Sep 29 16:43:45 2017 Info: MID 279741 DKIM: cannot sign - no profile matches MAILER-DAEMON@esa.dcloud.cisco.com
Fri Sep 29 16:43:45 2017 Info: MID 279741 ready 57623 bytes from <MAILER-DAEMON@esa.dcloud.cisco.com>
Fri Sep 29 16:43:45 2017 Info: MID 279741 queued for delivery
Fri Sep 29 16:43:45 2017 Info: MID 279740 rewritten to MID 279742 by add-footer filter 'Footer Stamping'
Fri Sep 29 16:43:45 2017 Info: Message finished MID 279740 done
Fri Sep 29 16:43:45 2017 Info: New SMTP DCID 2538 interface 198.18.133.146 address 198.18.133.2 port 25
Fri Sep 29 16:43:45 2017 Info: MID 279742 quarantined to "DLP Violations" (DLP violation)
```

8. Make note of the Message ID (MID) this will be correlated later.

NOTE: A Message ID (MID) is a unique identifier assigned to a particular message by the ESA. A MID is associated with every message received by the Cisco appliance and can be tracked in mail logs.

NOTE : Learn more about the different type of IDs here: - What is a Message ID (MID), Injection Connection ID (ICID), or Delivery Connection ID (DCID)?

9. Navigate back to the Outlook client, the mailboxes should have synchronized at this point, if they are not, force the synchronization process by clicking **Send/Receive Folder** or by pressing the **F9** key.
10. Here the action taken on the message can be seen; notice the custom message created earlier has been applied and delivered to Alan advising him of the violation. Most importantly the message did not make it to the recipient as it was re-directed the quarantine as per our instruction.



Task - Monitor the DLP Policy (Estimated time to complete: 5min)

The DLP Incidents page shows information on the incidents of data loss prevention (DLP) policy violations occurring in outgoing mail. The solution uses the DLP email policies enabled in the Outgoing Mail Policies table to detect sensitive data sent by users.

Every occurrence of an outgoing message violating a DLP policy is reported as an incident. Using the DLP Incidents report, it is possible to answer questions like:

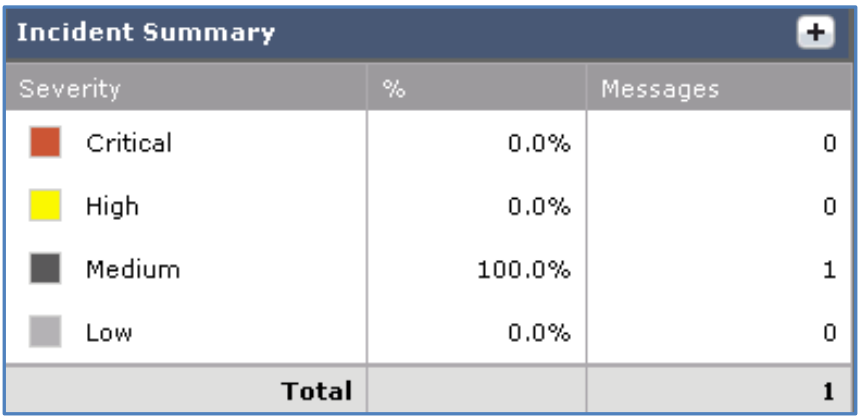
- What type of sensitive data are users sending?
- How severe are these DLP incidents?
- How many of these messages are being delivered?
- How many of these messages are being dropped?
- Who is sending these messages?

The DLP Incidents page is comprised of two main sections:

- The DLP incident trend graphs summarizing the top DLP incidents by severity (Low, Medium, High, Critical) and policy matches.
- The DLP Incidents Details listing.

This task will perform some analysis on the pervious DLP incident to get more information on what happened and why it happened.

1. From GUI session on the workstation and navigate to **Monitor > DLP Incidents** report and from the incident summary a Medium level violation will be recorded.

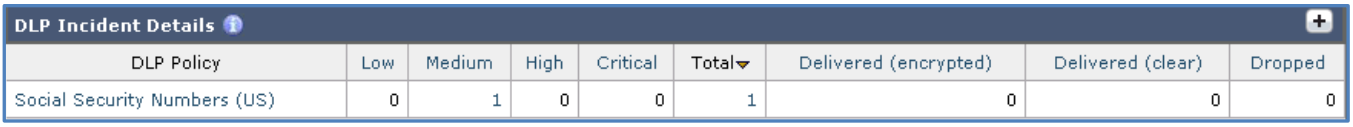


Incident Summary

Severity	%	Messages
Critical	0.0%	0
High	0.0%	0
Medium	100.0%	1
Low	0.0%	0
Total		**1**

: It may be necessary to refresh the window to see the violation in the report.

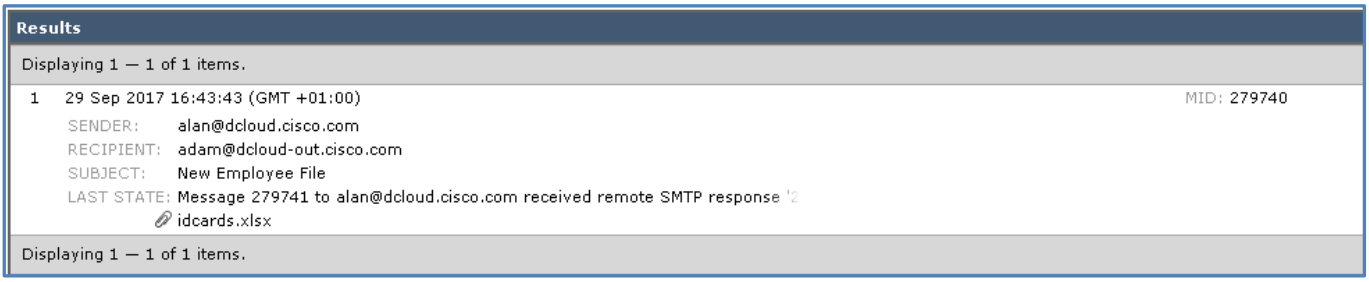
2. Scroll towards the bottom of the screen to view further details of this incident. The Medium column shows the violation.



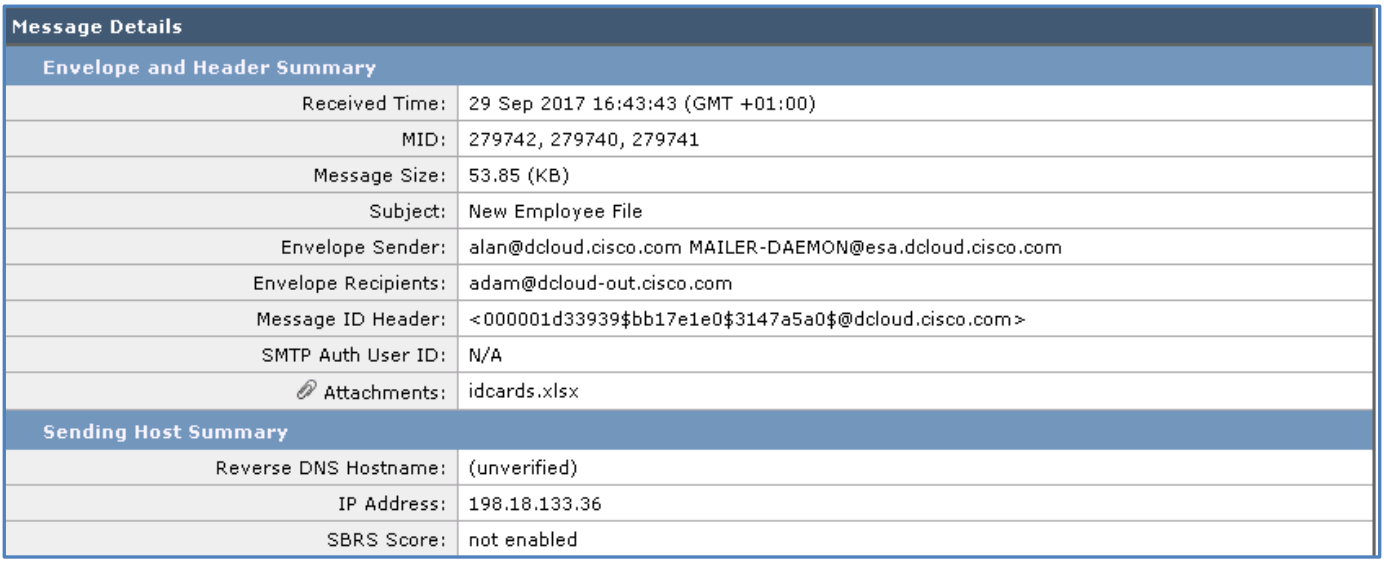
DLP Incident Details

DLP Policy	Low	Medium	High	Critical	Total	Delivered (encrypted)	Delivered (clear)	Dropped
Social Security Numbers (US)	0	1	0	0	1	0	0	0

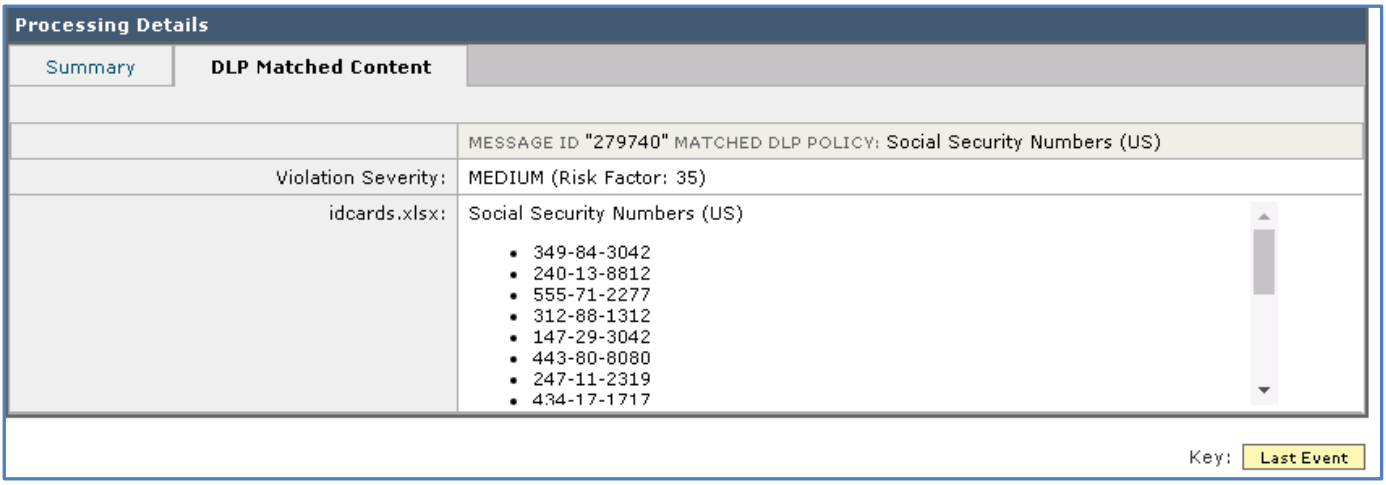
3. Click on the incident under Medium this will launch Message Tracking where more information of the message flow and the various actions applied to it can be viewed.
4. From the message tracking window, scroll towards the *Results* section and compare the message identification (MID) from earlier on, this will be the same value.



5. Click **Show Details** to view this specific message in detail.

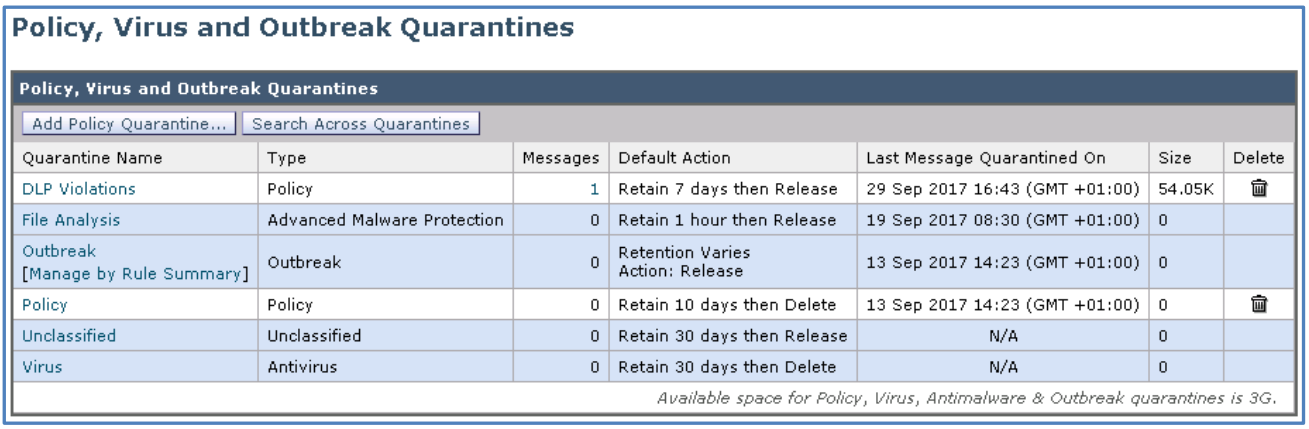


6. Under the *Processing Details* section, click on the **DLP Matched Content** tab, to see exactly the content that caused the violation.

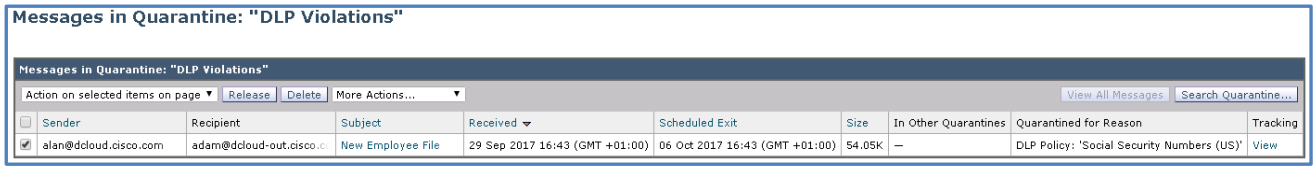


7. Close the Message Tracking window.

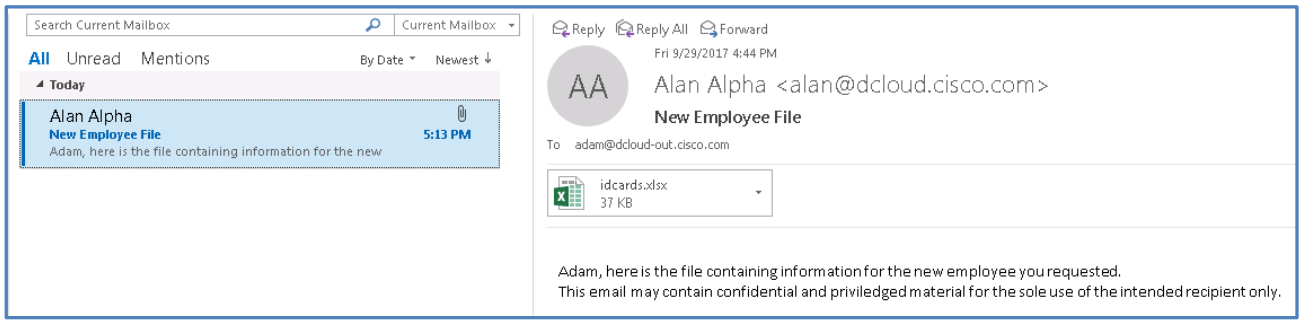
8. Navigate to **Monitor > Policy, Virus and Outbreak Quarantines > DLP Violations** the message that never made it to the recipient Adam will be in the quarantine created earlier.



9. Click on the number under the *Messages* column to see the message details. Select the message and click the **Release** button and confirm the action when prompted**.**



10. Return to the workstation, synchronize the messages once more and the message will now appear in Adams mailbox, note the additional text has been added as configured in the disclaimer earlier.



11. Open the attachment to confirm the content is once again visible.

NOTE: Typically in a use like this it would be advisable either encrypt the message prior to sending it or leave it in the quarantine rather than releasing it.

Scenario 2. Protecting Against Malicious or Undesirable URLs

Use Case

The advertising department of Voyage Corp decided to work on a new campaign to make better use of how the company products are advertised. Previously all advertising was limited to the popular computing journals. The director of advertising operations has asked his team to make use of additional resources to really drive the message home on Voyage Corps products and services following a small dip in services revenue.

Several advertising agencies were approached to better understand how Voyage Corp could advertise using on-line computing websites and blogs. Sample adverts were placed on several sites and the results of the trial with weekly statistics were sent to the advertising manager via email for review. One late afternoon the advertising manager clicked on a link within an innocent looking message, which resulted in his browser redirecting him to a website that downloaded, unknown to him at the time, some malicious code that shut down key services on his computer. Once this was reported to the in-house support team, the infected machine as immediately removed from the network for cleansing and posture assessment; the whole process took a few days prompting the introduction of Outbreak Filtering technology.

Security Control

Control and protection against malicious or undesirable links is incorporated into the anti-spam, outbreak, content, and message filtering processes in the work queue. These controls increase the effectiveness of protection from malicious URLs in messages.

URL filtering is incorporated into Outbreak Filtering. This strengthened protection is useful even if an organization already has a Cisco Web Security Appliance or similar protection from web-based threats, because it blocks threats at the point of entry.

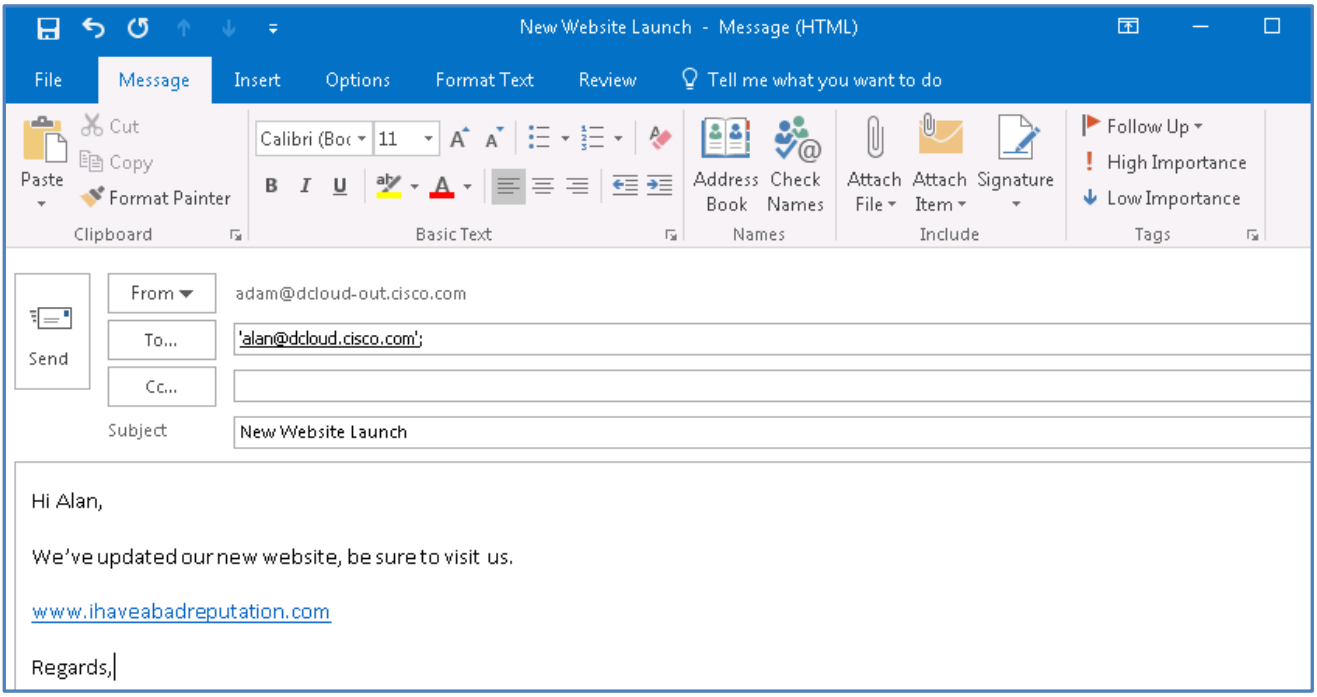
Objective

This scenario will demonstrate how to protect against malicious URLs within emails by leveraging the Cisco Security Proxy service to ensure end users are not accessing websites that may be a source of malware of viruses.

Steps

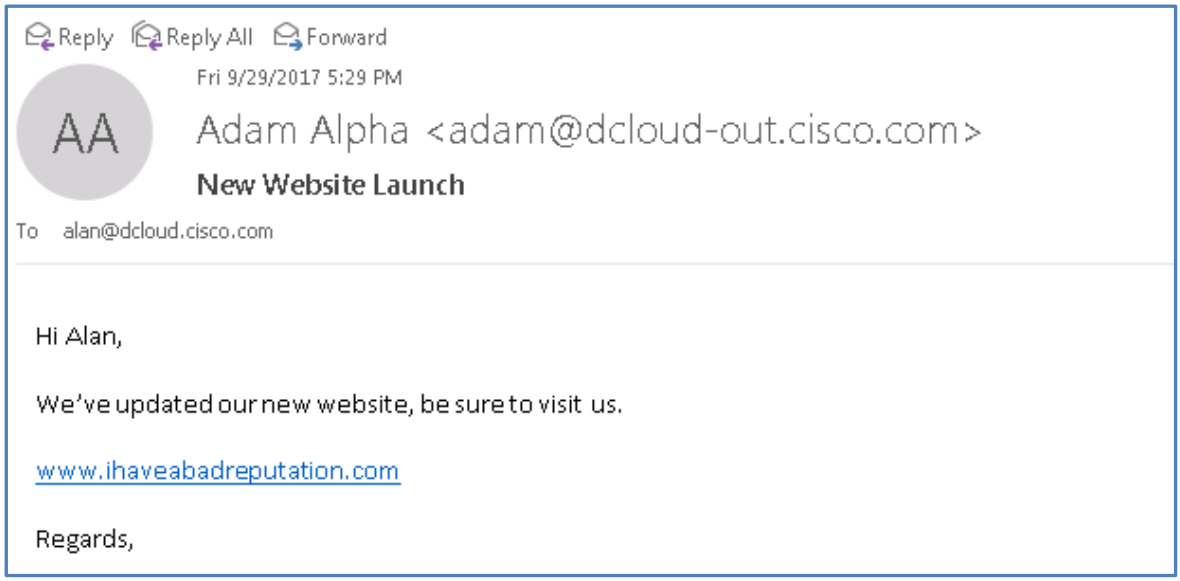
Task - Accessing URLs within Messages (Estimated time to complete: 5 min)

1. The first task will demonstrate how potentially dangerous links within email could be if mechanisms are not in place to advise users of the dangers of URL within messages.
2. From the workstation launch Microsoft Outlook and from Adams inbox, prepare a new message with the following parameters.
   - To: alan@dcloud.cisco.com
   - Subject: New Website Launch
   - Body: Hi Alan,
     We've updated our website, be sure to visit us.
     www.ihaveabadreputation.com
     Regards,

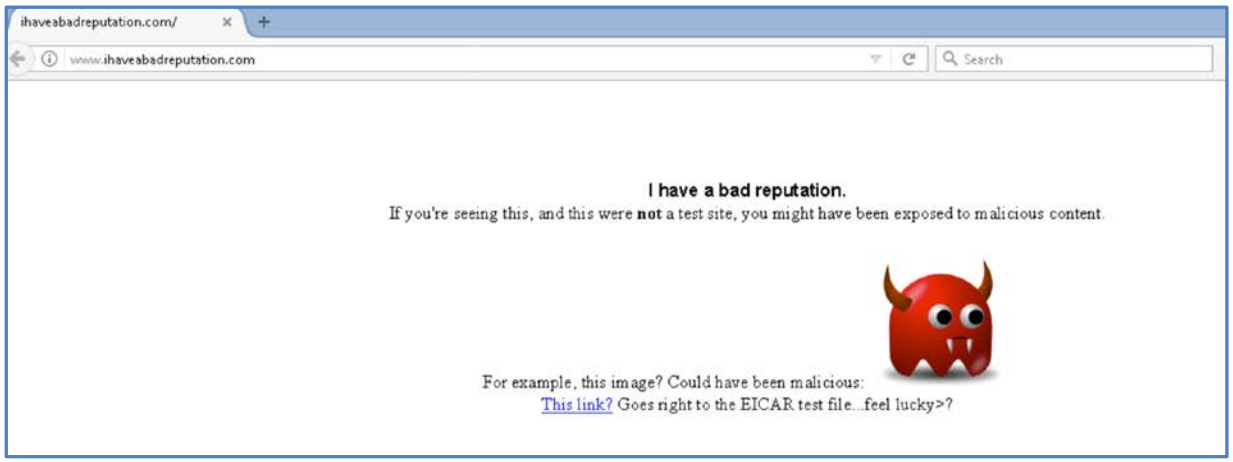


3. Send the email - Force the synchronization process by clicking **Send/Receive Folder** or by pressing the **F9** key.

4. Examine Alan's inbox to verify receipt of the message. It should appear arrive exactly as sent with the potentially malicious hyperlink present.



5. Click the hyperlink within the message once, it will then launch a browser with the site accessible, if this was a site that contained malicious content the end user that clicked the link would be exposed and the damage could spread quickly between across interconnected devices.



6. Close the browser window.

Task - Configuring a Content Filter (Estimated time to complete: 3 min)

Content Filters are used to customize handling of messages beyond the standard routine handling by the other content security features such as anti-virus scanning or DLP.

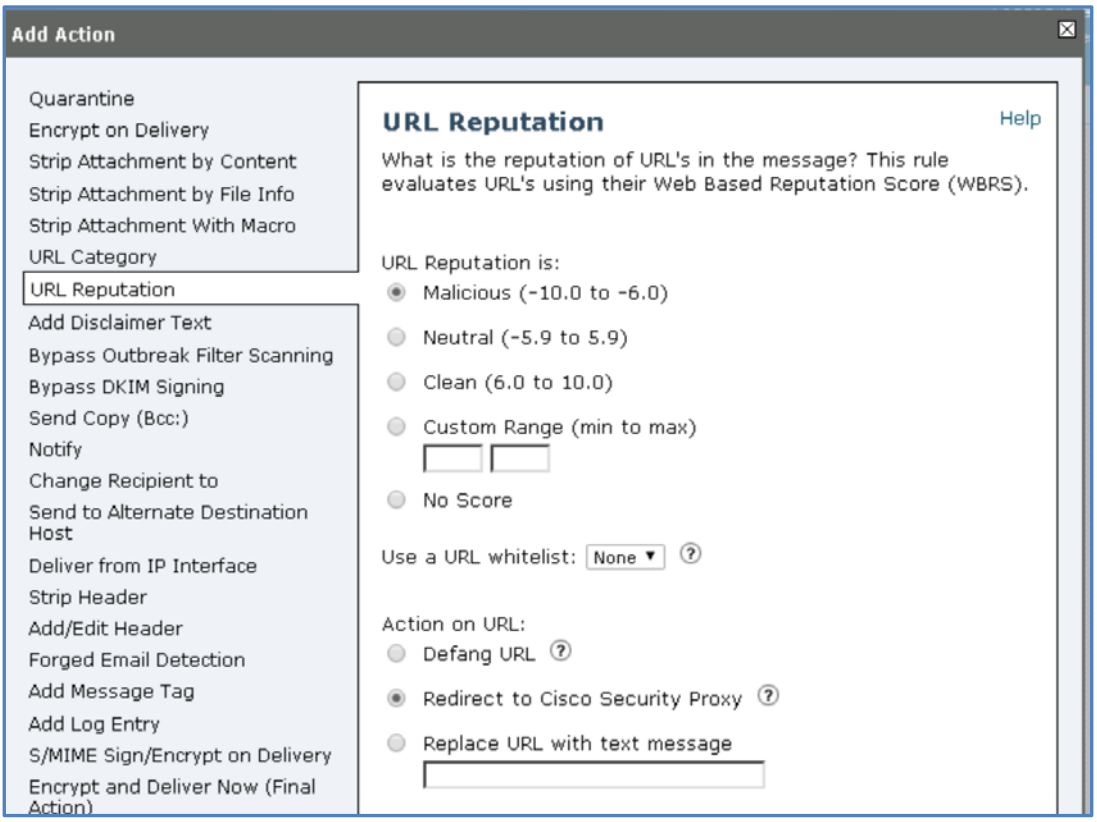
For example, a content filter can be used to, if the content warrants quarantining for later examination, or because corporate policy requires certain messages to be encrypted before delivery

Content filters have the following components:

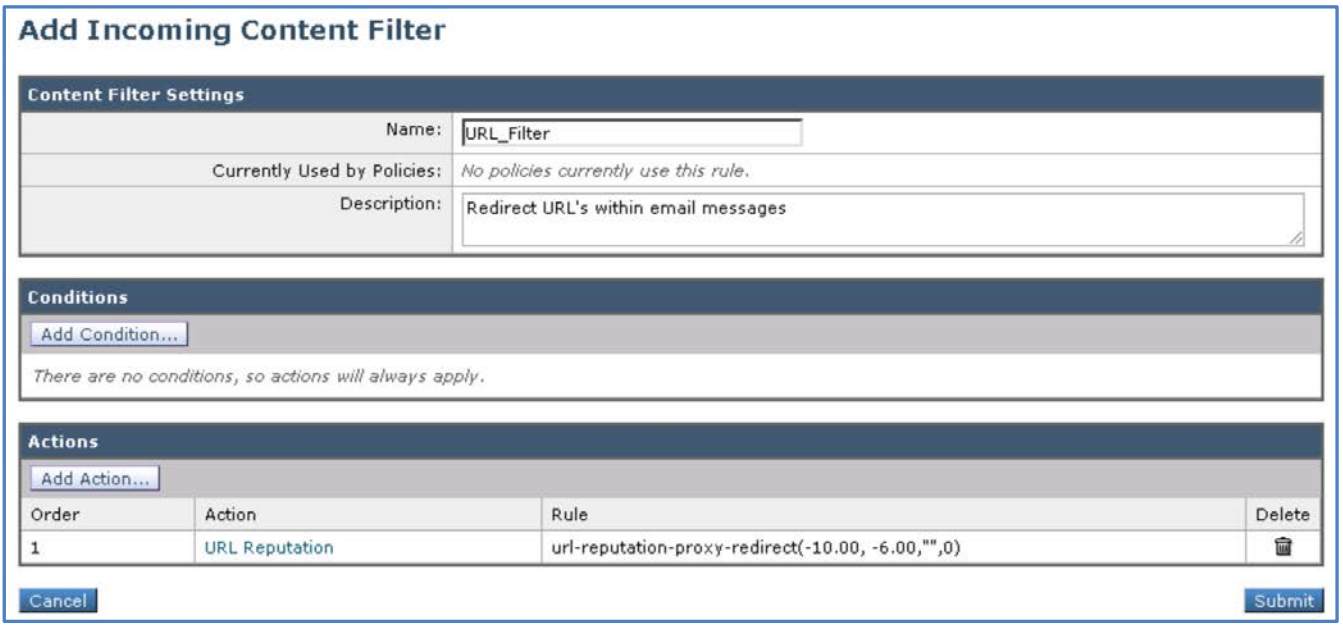
- ***conditions*** - that determine when the solution uses a content filter to scan a message (optional)
- ***actions*** - that the solution takes on a message (required)

This task will create a new content filter to identify potentially malicious URLs within email messages and take an appropriate action on that message – direct it through the Cisco Security Proxy, which in turn will determine if the URL is in fact potentially dangerous.

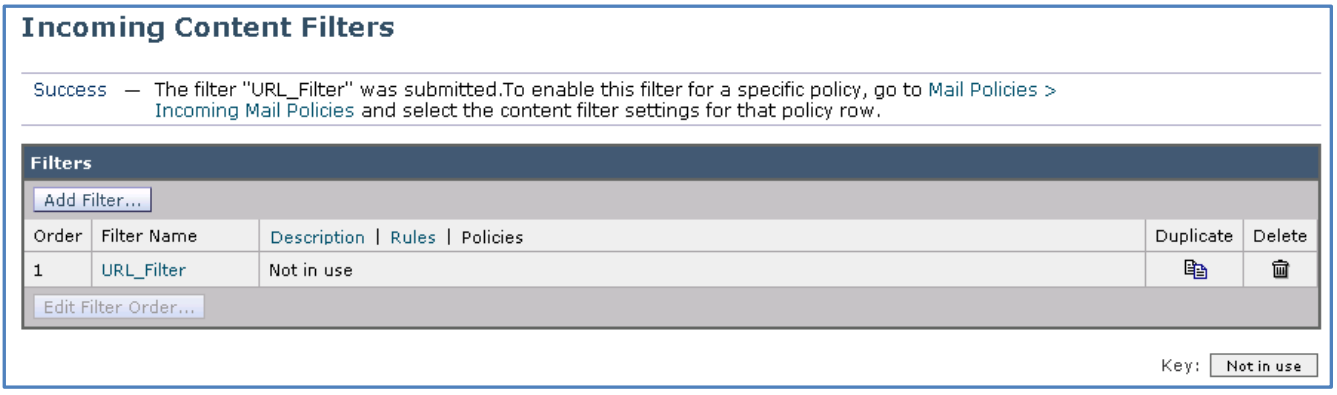
1. From the workstation access the GUI and navigate to **Mail Policy > Incoming Content Filters** and click **Add Filter**.
2. Using the following settings configure the *Conditions* and *Actions*.
   - Name: URL_Filter
   - Description: Redirect URLs within email messages
   - Action 1: URL Reputation > Redirect to Cisco Security Proxy



3. Click **OK.**



4. Click **Submit** to apply the actions

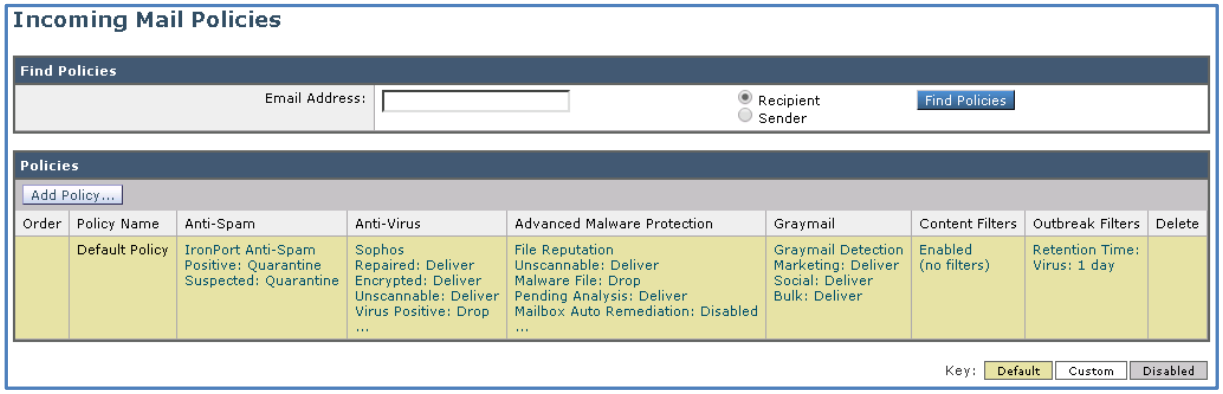


5. Once complete, ensure the changes are applied by clicking the **Commit Changes** button, adding optional comments if desired.

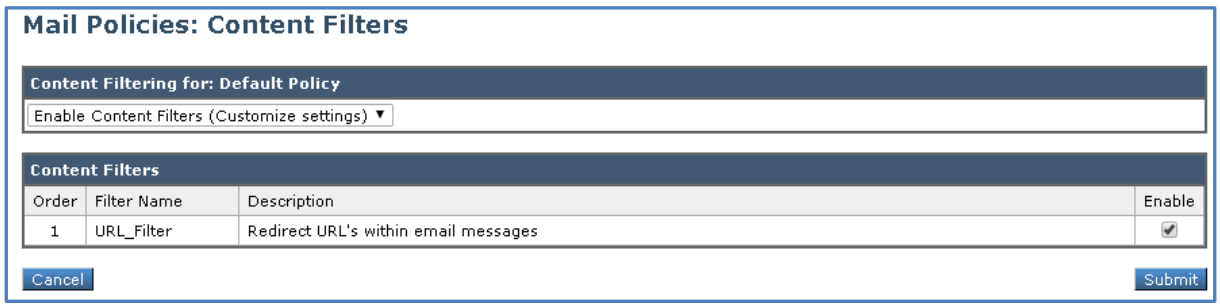
Task - Edit Incoming Mail Policy (Estimated time to complete: 1 min)

Once the necessary content filter has been configured it must be enabled to a Mail Policy to be effective.

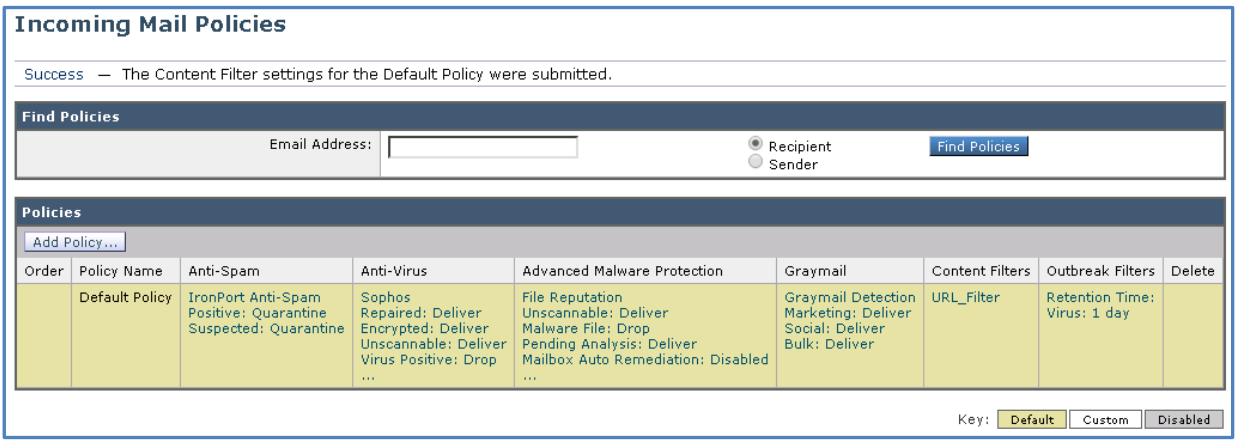
1. From the workstation access the GUI and navigate to **Mail Policy > Incoming Mail Policies** and click within the *Content Filters* box of the Default Policy.



2. Place a checkmark against the content filter **URL_Filter** created in the previous step to enable it.



3. Click **Submit** to create the content Filter and verify the policy.



4. Once complete, ensure the changes are applied by clicking the **Commit Changes** button - top right of screen, adding optional comments if desired.

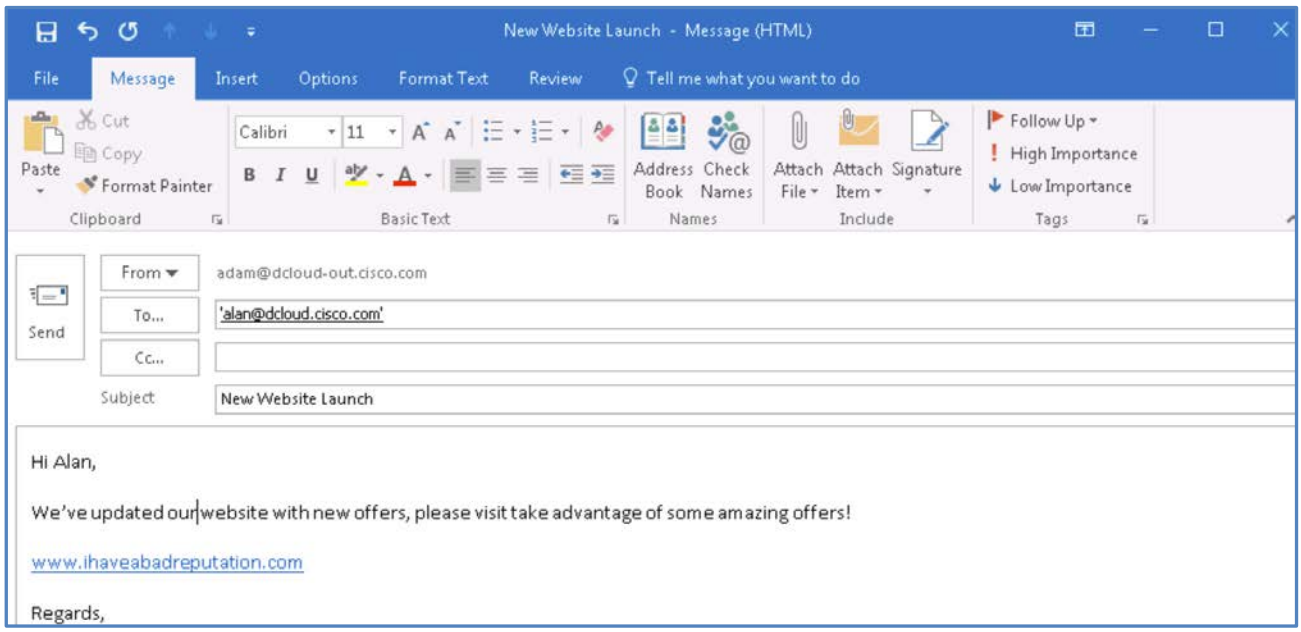
Task - Testing URL Filtering (Estimated time to complete: 5 min)

With the pre-requisite configuration in place, the URL Filtering feature can be tested by sending an email to Alan from external user Adam with a potentially malicious URL within the body of the message.

Initiate a CLI session

Prior to preparing the message, initiate a connection to the Cisco Email Security solution from the CLI in order to view, using the tail command, the mail logs to see the message being processed and the actions being applied as it works its way through the pipeline, repeat the same steps to initiate this from the previous scenario.

1. From the workstation launch Microsoft Outlook and from Adams inbox, prepare a new message with the following parameters.
   - To: alan@dcloud.cisco.com
   - Subject: New Website Site
   - Body: Hi Alan,
     We've updated our website with new offers, please visit to take advantage of some amazing offers!
     www.ihaveabadreputation.com
     Regards,

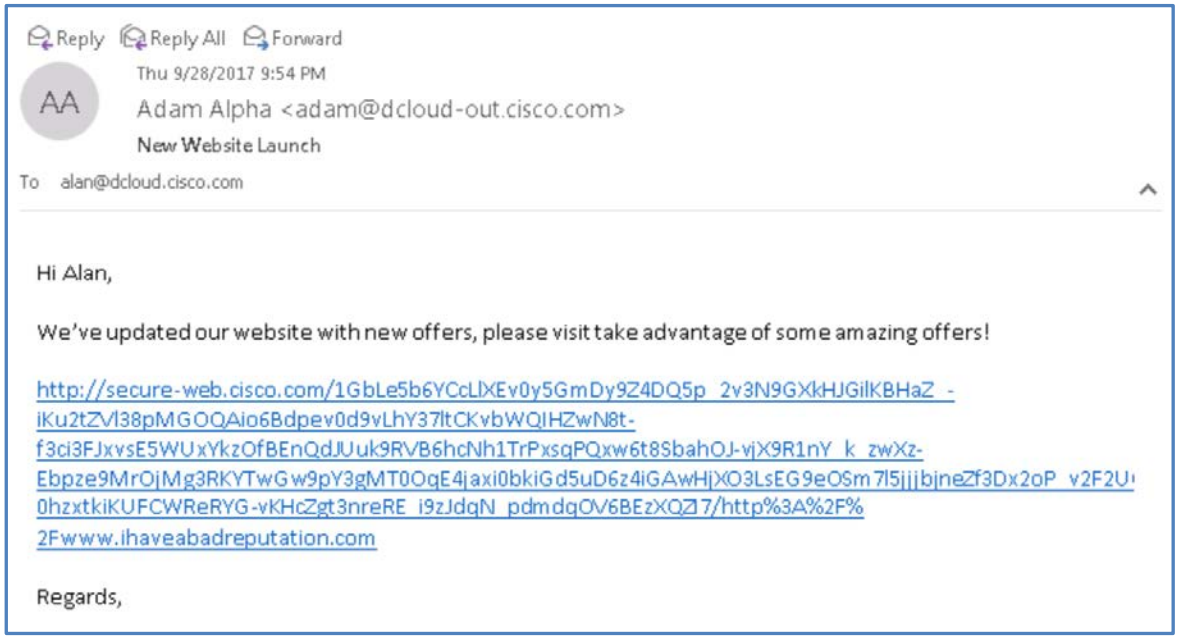


2. Send the email - Force the synchronization process by clicking **Send/Receive Folder** or by pressing the **F9** key.

3. Switch back to the CLI and notice how the content filter handled the message, it was redirect to the Cisco Security Proxy which will determine based on web reputation if the URL within the message is potentially dangerous.

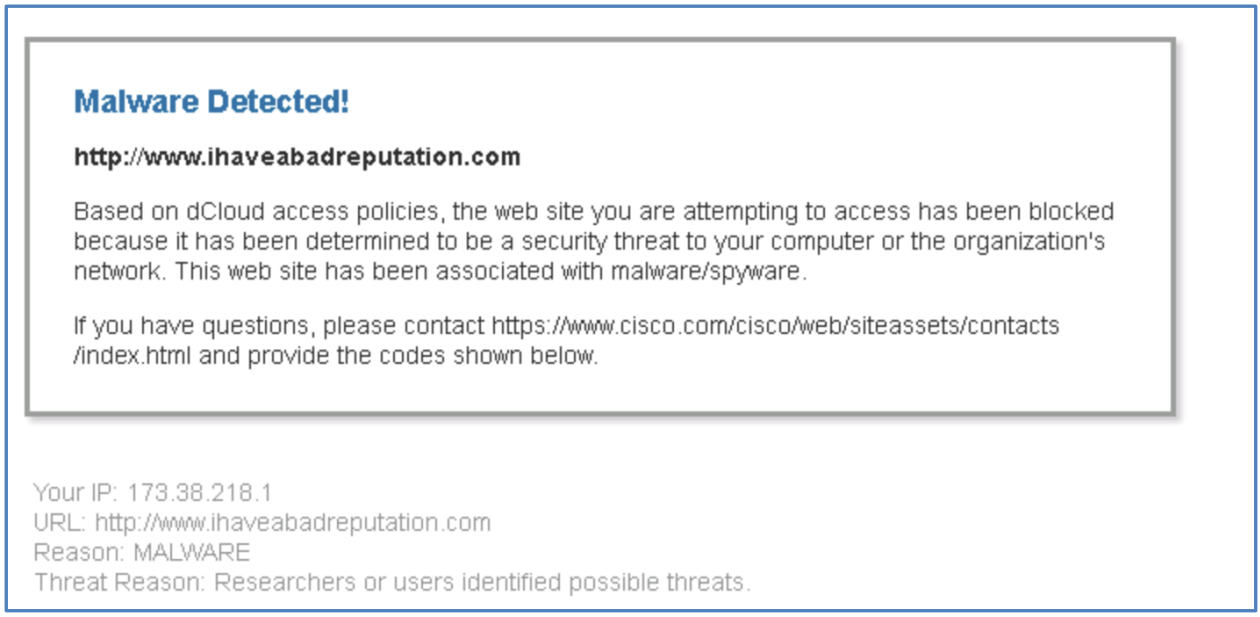
```
Fri Sep 29 17:38:05 2017 Info: Start MID 279747 ICID 6431
Fri Sep 29 17:38:05 2017 Info: MID 279747 ICID 6431 From: <adam@dcloud-out.cisco.com>
Fri Sep 29 17:38:05 2017 Info: MID 279747 ICID 6431 RID 0 To: <alan@dcloud.cisco.com>
Fri Sep 29 17:38:05 2017 Info: MID 279747 Message-ID '<002101d33941$5356c7d0$fa045770$@dcloud-out.cisco.com>'
Fri Sep 29 17:38:05 2017 Info: MID 279747 Subject 'New Website Launch'
Fri Sep 29 17:38:05 2017 Info: MID 279747 ready 3385 bytes from <adam@dcloud-out.cisco.com>
Fri Sep 29 17:38:05 2017 Info: MID 279747 matched all recipients for per-recipient policy DEFAULT in the inbound table
Fri Sep 29 17:38:05 2017 Info: MID 279747 interim verdict using engine: CASE spam negative
Fri Sep 29 17:38:05 2017 Info: MID 279747 using engine: CASE spam negative
Fri Sep 29 17:38:05 2017 Info: MID 279747 interim AV verdict using Sophos CLEAN
Fri Sep 29 17:38:05 2017 Info: MID 279747 antivirus negative
Fri Sep 29 17:38:05 2017 Info: MID 279747 AMP file reputation verdict : SKIPPED (no attachment in message)
Fri Sep 29 17:38:05 2017 Info: MID 279747 using engine: GRAYMAIL negative
Fri Sep 29 17:38:05 2017 Info: MID 279747 rewritten to MID 279748 by url-reputation-proxy-redirect-action filter 'URL_Filter'
Fri Sep 29 17:38:05 2017 Info: Message finished MID 279747 done
Fri Sep 29 17:38:05 2017 Info: MID 279748 Outbreak Filters: verdict negative
Fri Sep 29 17:38:05 2017 Info: MID 279748 queued for delivery
Fri Sep 29 17:38:05 2017 Info: New SMTP DCID 2543 interface 198.18.133.146 address 198.18.133.2 port 25
Fri Sep 29 17:38:05 2017 Info: Delivery start DCID 2543 MID 279748 to RID [0]
Fri Sep 29 17:38:06 2017 Info: Message done DCID 2543 MID 279748 to RID [0]
Fri Sep 29 17:38:06 2017 Info: MID 279748 RID [0] Response '2.6.0 <002101d33941$5356c7d0$fa045770$@dcloud-out.cisco.com> [Inter
nalId=4] Queued mail for delivery'
Fri Sep 29 17:38:06 2017 Info: Message finished MID 279748 done
Fri Sep 29 17:38:07 2017 Info: ICID 6431 close
Fri Sep 29 17:38:11 2017 Info: DCID 2543 close
```

4. Navigate back to Alan's inbox, notice how the URL has now changed, with the hyperlink much longer as it contains a redirection to the Cisco Security Proxy.

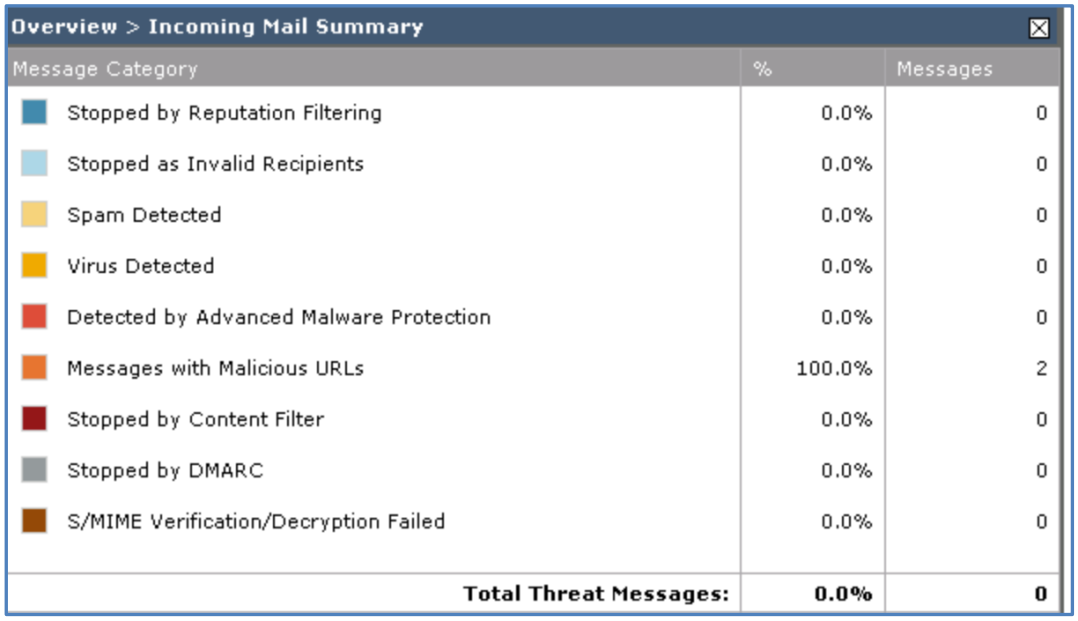


NOTE: URL reputation and category are provided by cloud-based Cisco Web Security Services. The Email Security Solution connects to the Cisco Web Security Services either directly or through a web proxy, using the port specified for URL filtering services in Firewall Information Communication is over HTTPS with mutual certificate authentication.

5. Click the URL once to access it within a browser and note that based on reputation access to the URL is strictly prohibited as per the policy configured earlier.



6. Navigate to **Monitor > My Dashboard** and note the *Messages with Malicious URLs* chart reflects what actions have taken place.



Overview > Incoming Mail Summary

Message Category	%	Messages
Stopped by Reputation Filtering	0.0%	0
Stopped as Invalid Recipients	0.0%	0
Spam Detected	0.0%	0
Virus Detected	0.0%	0
Detected by Advanced Malware Protection	0.0%	0
Messages with Malicious URLs	100.0%	2
Stopped by Content Filter	0.0%	0
Stopped by DMARC	0.0%	0
S/MIME Verification/Decryption Failed	0.0%	0
Total Threat Messages:	**0.0%**	**0**

Scenario 3. Outbreak Filters

Use Case

Recently the services arm of Voyage Corp launched a new catalogue of customised services for the retail sector to help them procure, utilise and support the various IT products that they offer; this was launched on the back of a successful marketing campaign where email was the primary method of communication for this launch.

A mailing list was used to send out the marketing emails, however all replies were sent to a marketing co-ordinator who was responsible for gathering metrics of the campaign, unfortunately the marketing co-ordinator received an email containing attachments and URL that at first glance appeared to be non-suspicious, however after clicking the link within the email an infected payload was delivered to her personal computer that was not detected by the multiple anti-virus engines installed across the company infrastructure.

Security Control

This scenario demonstrates how Outbreak Filters protect users from targeted, URL-based threats.

Low volume, targeted threats can be difficult to detect. If anti-spam settings are too high, false positives will increase, leaving users searching quarantines for legitimate messages. However, if anti-spam settings are too low, more spam will get through.

Outbreak Filters gives suspicious emails additional checks. If a message fails those checks, the ESA will rewrite URLs, quarantine, and then rescan the message after release before delivering it. This quarantine gives the ESA time to hold the message to see if new anti-spam rules that arrive identify the message as spam/malicious before the message release time occurs.

Objective

This scenario will demonstrate how to protect Outbreak Filters protects an organization from large-scale virus outbreaks and smaller, non-viral attacks, such as phishing scams and malware distribution, as they occur. Unlike most anti-malware security software, which cannot detect new outbreaks until data is collected and a software update is published.

NOTE: Some of the pre-requisite tasls for this scenario have been configured ahead of time, such as disclaimers. The creation of disclaimers for this exercise is similar to those experienced in the previous scenario.

Steps

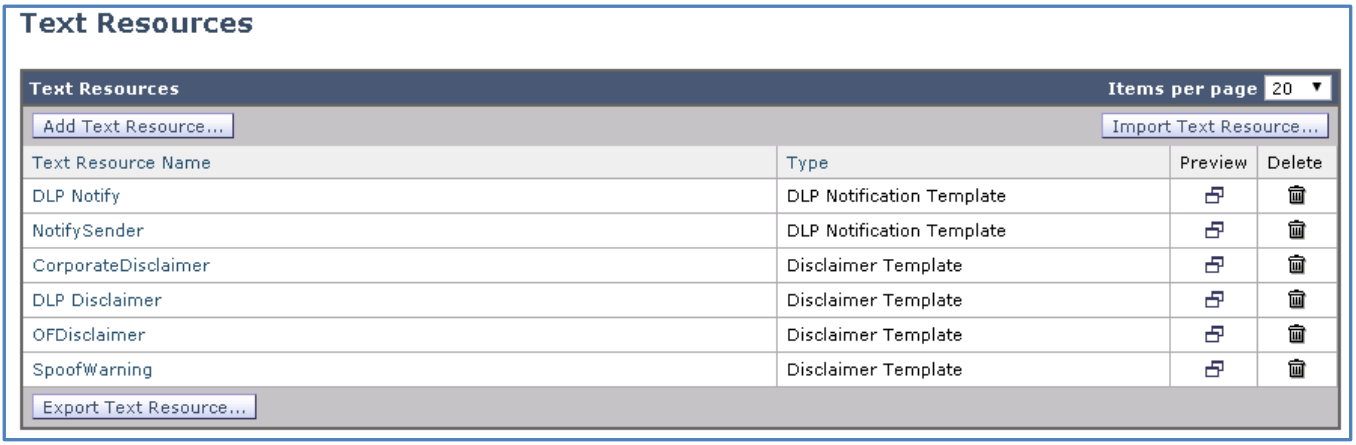
Task - Verify Outbreak Filter Disclaimers (Estimated time to complete: 2 min)

Similar to the previous scenario text resources play an important role in policy configuration on the Cisco Email Security Solution. For outbreak filters, they allow valuable information and feedback to be displayed to users when the solution applies a policy that prevents an action from being completed.

1. Within disclaimers action variables can also be used to provide more specific information, for example with outbreak filters the following action variables are available:

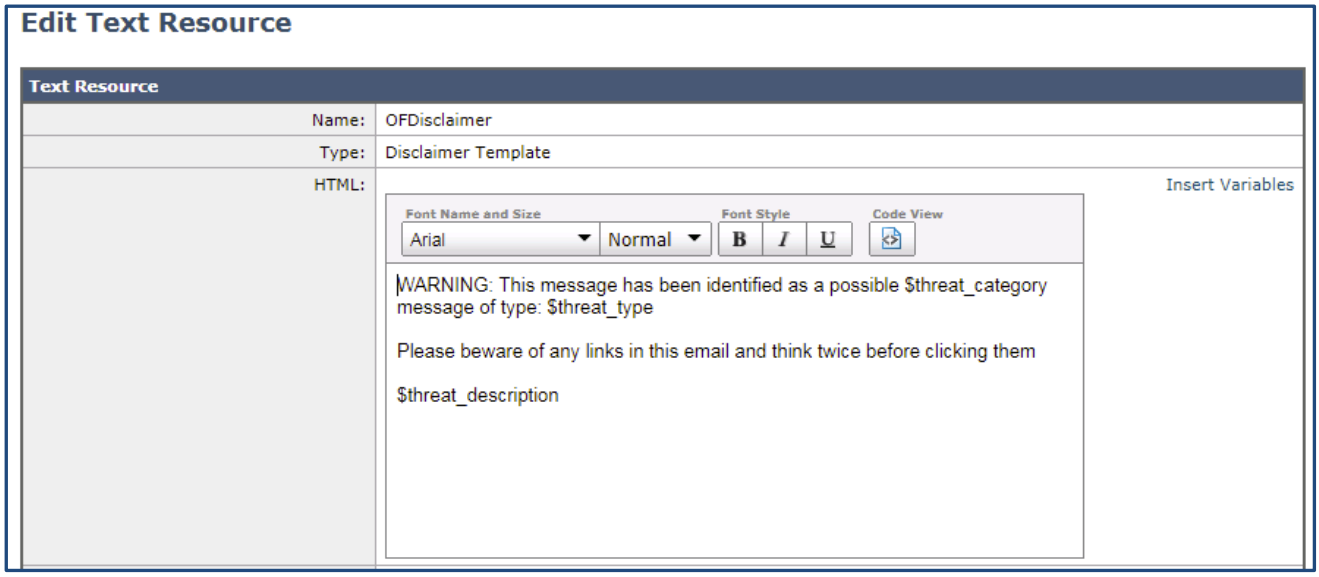
$threat_category	Replaced with the type of Outbreak Filters threat, such as phishing, virus, scam, or malware.
$threat_type	Replaced by a subcategory of the Outbreak Filters threat category. For example, can be a charity scam, a financial phishing attempt, a fake deal, etc.
$threat_description	Replaced by a description of the Outbreak Filters threat.
$threat_level	Replaced by the message's threat level (score 0 - 5).
$threat_verdict	Replaced by Yes or No, depending on the Message Modification Threat Level threshold. If the viral or non-viral threat level of a message is greater than or equal to the message modification threat level threshold, the value of this variable is set to Yes.

2. For this task, verify and review the pre-configured Outbreak Filter Disclaimer.
3. Navigate to **Mail Policies > Text Resources** and click the pre-configured **OFDisclaimer** from the list of text resources.



4. This type of disclaimer utilizes HTML text as well as action variables. When a text resource containing both HTML-based and plain text messages is applied to an email message, the HTML-based text resource message is applied to the text/html part of the email message, and the plain text message is applied to the text/plain part of the email message.

5. When an HTML-based text resource is edited, the GUI includes a rich text edit that allows the entering of rich text without having to manually write HTML code.



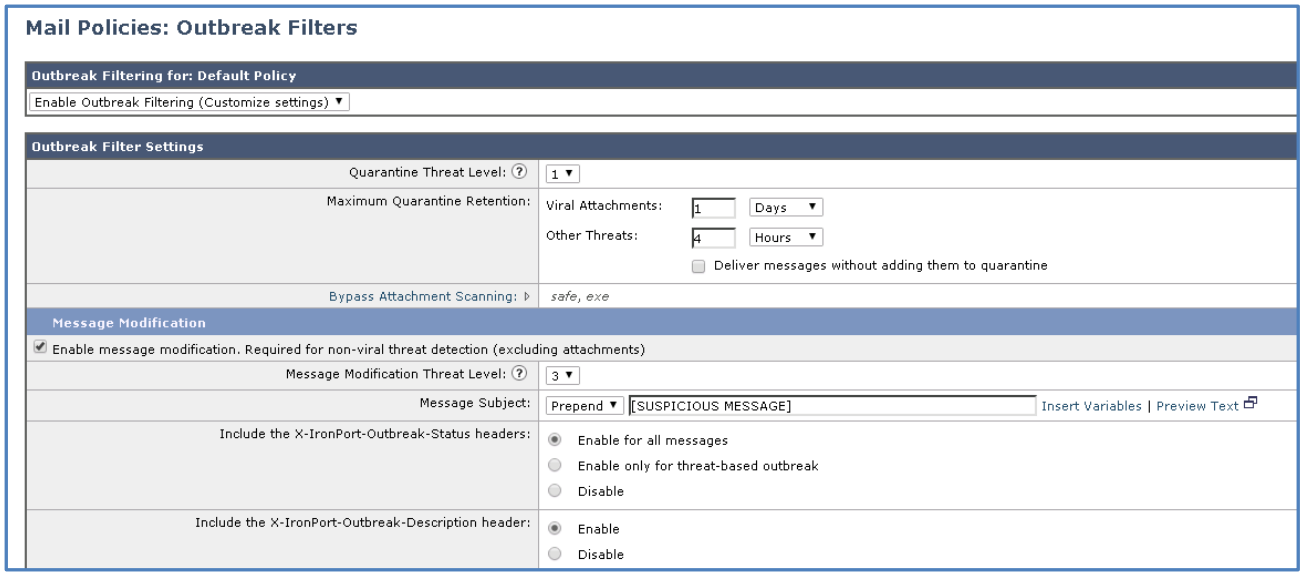
6. Click the **Cancel** button to revert to the previous screen, no changes needed.

Task - Configure Outbreak Filter setting (Estimated time to complete: 2 min)

An Outbreak Filter rule is basically a Threat Level (e.g. 4) associated with a set of characteristics for an email message and attachment — things such as file size, file type, file name, message content, and so on. For example, assume the Cisco SIO notices an increase in the occurrences of a suspicious email message carrying a .exe attachment that is 143 kilobytes in size, and whose file name includes a specific keyword (hello for example). An Outbreak Rule is published increasing the Threat Level for messages matching this criterion. The Cisco Email Security Solution checks for and downloads newly published Outbreak and Adaptive Rules every 5 minutes by default. On the solution, a threshold is set for quarantining suspicious messages. If the Threat Level for a message is equal to or exceeds the quarantine threshold, the message is sent to the Outbreak quarantine area.

1. Edit the Outbreak policy to modify messages, click the link under the **Outbreak Filters** column **(Retention Time: Virus 1 day)** to open the Outbreak Filters page.

2. Under the Message Modification section, place a check mark against the Enable message modification. This is required for non-viral threat detection (excluding attachments). Click Submit.



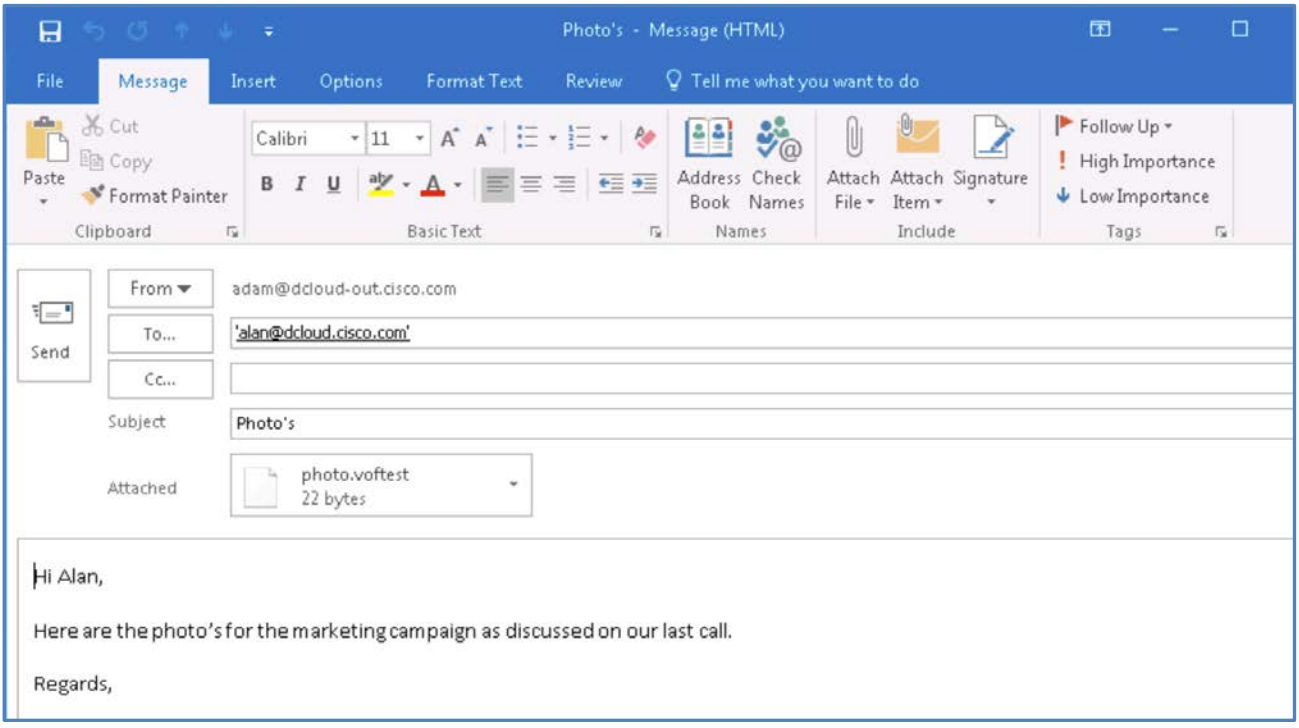
3. Once complete, ensure the changes are applied by clicking the **Commit Changes** button, adding optional comments if desired.

Task - Testing Outbreak filters (Estimated time to complete: 5 min)

To demonstrate how the Outbreak Filter works, send an email from Adam to Alan, this simulates a message coming into the organization from an external user as per our earlier topology.

Initiate a CLI session

1. Prior to preparing the message, initiate a connection to the Cisco Email Security solution from the CLI in order to view, using the tail command, the mail logs to see the message being processed and the actions being applied as it works its way through the pipeline, repeat the same steps to initiate this from the previous scenario.
2. From the workstation launch Outlook from the desktop and from Adams mailbox create an email with the following parameters:
   - To: alan@dcloud.cisco.com
   - Subject: Photos
   - Body: Here are the photos of the new product design mentioned on our call.
   - Attach: Attach the following file photo.voftest - located on the desktop under the Outbreak sub folder.



3. Send the email - Force the synchronization process by clicking **Send/Receive Folder** or by pressing the **F9** key.

NOTE: The attachment contains enough information to trigger an action from as Outbreak Rule ID 190 is in fact a system test, verify this in **Security Services > Outbreak Filters**

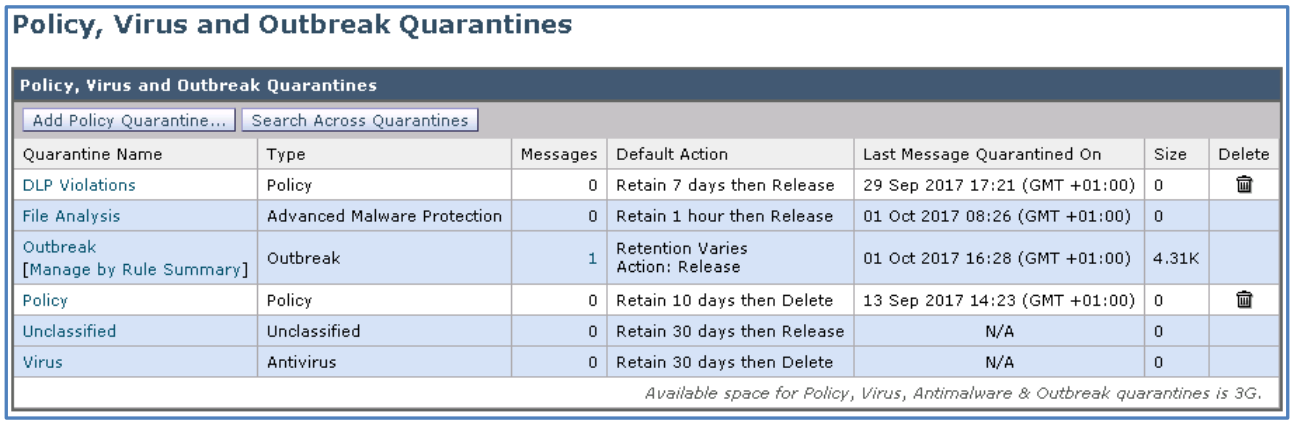
4. Navigate to the CLI shell opened previously and look for the message that implies the message has been quarantined. Note, the Threat Level of 3, this indicates that either the message is part of a confirmed outbreak or there is a medium to large risk of its content being a threat, also note how the anti-virus engines delivered a clean result.

```
Sun Oct  1 16:28:57 2017 Info: MID 279793 ICID 6468 From: <adam@dcloud-out.cisco.com>
Sun Oct  1 16:28:57 2017 Info: MID 279793 ICID 6468 RID 0 To: <alan@dcloud.cisco.com>
Sun Oct  1 16:28:57 2017 Info: MID 279793 Message-ID '<004701d33aca$01151500$033f3f00$@dcloud-out.cisco.com>'
Sun Oct  1 16:28:57 2017 Info: MID 279793 Subject "Photo's"
Sun Oct  1 16:28:57 2017 Info: MID 279793 ready 3628 bytes from <adam@dcloud-out.cisco.com>
Sun Oct  1 16:28:57 2017 Info: MID 279793 attachment 'photo.voftest'
Sun Oct  1 16:28:57 2017 Info: MID 279793 matched all recipients for per-recipient policy DEFAULT in the inbound table
Sun Oct  1 16:28:58 2017 Info: MID 279793 interim verdict using engine: CASE negative
Sun Oct  1 16:28:58 2017 Info: MID 279793 using engine: CASE spam negative
Sun Oct  1 16:28:58 2017 Info: MID 279793 interim AV verdict using Sophos CLEAN
Sun Oct  1 16:28:58 2017 Info: MID 279793 antivirus negative
Sun Oct  1 16:28:58 2017 Info: MID 279793 using engine: GRAYMAIL negative
Sun Oct  1 16:28:58 2017 Info: MID 279793 Outbreak Filters: verdict positive
Sun Oct  1 16:28:58 2017 Info: MID 279793 Threat Level=3 Category=Virus Type=Viral Attachment
Sun Oct  1 16:28:58 2017 Info: MID 279793 Virus Threat Level=3
Sun Oct  1 16:28:58 2017 Info: MID 279793 attachment types voftest
Sun Oct  1 16:28:58 2017 Info: MID 279793 rewritten to MID 279794 by add-heading filter 'Heading Stamping'
Sun Oct  1 16:28:58 2017 Info: Message finished MID 279793 done
Sun Oct  1 16:28:58 2017 Info: MID 279794 quarantined to "Outbreak" (Outbreak rule:OUTBREAK_0000190)
Sun Oct  1 16:28:58 2017 Info: Message finished MID 279794 done
Sun Oct  1 16:28:59 2017 Info: ICID 6468 close
```

5. Make note of the MID and note what final action was applied to the message – Quarantine.

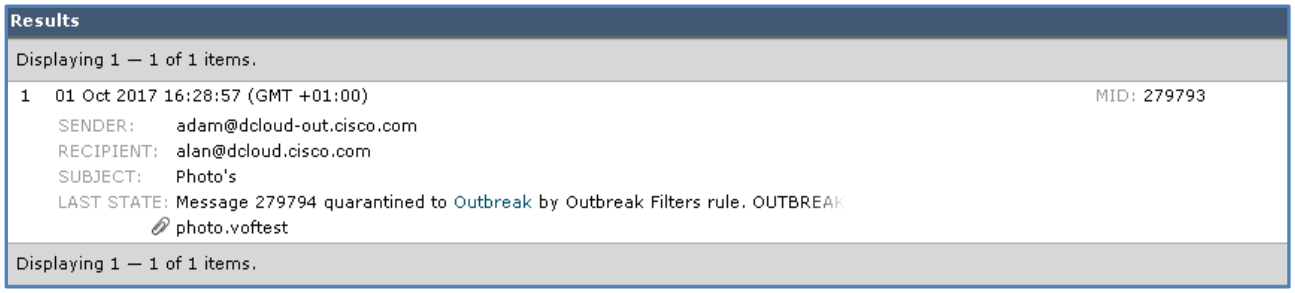
```
Sun Oct  1 16:28:57 2017 Info: MID 279793 ICID 6468 From: <adam@dcloud-out.cisco.com>
Sun Oct  1 16:28:57 2017 Info: MID 279793 ICID 6468 RID 0 To: <alan@dcloud.cisco.com>
Sun Oct  1 16:28:57 2017 Info: MID 279793 Message-ID '<004701d33aca$01151500$033f3f00$@dcloud-out.cisco.com>'
Sun Oct  1 16:28:57 2017 Info: MID 279793 Subject "Photo's"
Sun Oct  1 16:28:57 2017 Info: MID 279793 ready 3628 bytes from <adam@dcloud-out.cisco.com>
Sun Oct  1 16:28:57 2017 Info: MID 279793 attachment 'photo.voftest'
Sun Oct  1 16:28:57 2017 Info: MID 279793 matched all recipients for per-recipient policy DEFAULT in the inbound table
Sun Oct  1 16:28:58 2017 Info: MID 279793 interim verdict using engine: CASE negative
Sun Oct  1 16:28:58 2017 Info: MID 279793 using engine: CASE spam negative
Sun Oct  1 16:28:58 2017 Info: MID 279793 interim AV verdict using Sophos CLEAN
Sun Oct  1 16:28:58 2017 Info: MID 279793 antivirus negative
Sun Oct  1 16:28:58 2017 Info: MID 279793 using engine: GRAYMAIL negative
Sun Oct  1 16:28:58 2017 Info: MID 279793 Outbreak Filters: verdict positive
Sun Oct  1 16:28:58 2017 Info: MID 279793 Threat Level=3 Category=Virus Type=Viral Attachment
Sun Oct  1 16:28:58 2017 Info: MID 279793 Virus Threat Level=3
Sun Oct  1 16:28:58 2017 Info: MID 279793 attachment types voftest
Sun Oct  1 16:28:58 2017 Info: MID 279793 rewritten to MID 279794 by add-heading filter 'Heading Stamping'
Sun Oct  1 16:28:58 2017 Info: Message finished MID 279793 done
Sun Oct  1 16:28:58 2017 Info: MID 279794 quarantined to "Outbreak" (Outbreak rule:OUTBREAK_0000190)
Sun Oct  1 16:28:58 2017 Info: Message finished MID 279794 done
Sun Oct  1 16:28:59 2017 Info: ICID 6468 close
```

6. Return to Outlook client and click the Inbox for Alan. The message will not be present since it has been quarantined by our content filter created earlier. Navigate to **Monitor > Policy, Virus and Outbreak Quarantines** and note there is a message now in the *Outbreak* quarantine.



7. Click the value in the *Message Column* to view the message, note the reason it was quarantined.

8. Click **View** under Tracking to launch *Message Tracking* and scroll down towards the *Results* section to view the message, the MID should reference what was noted earlier.



Results

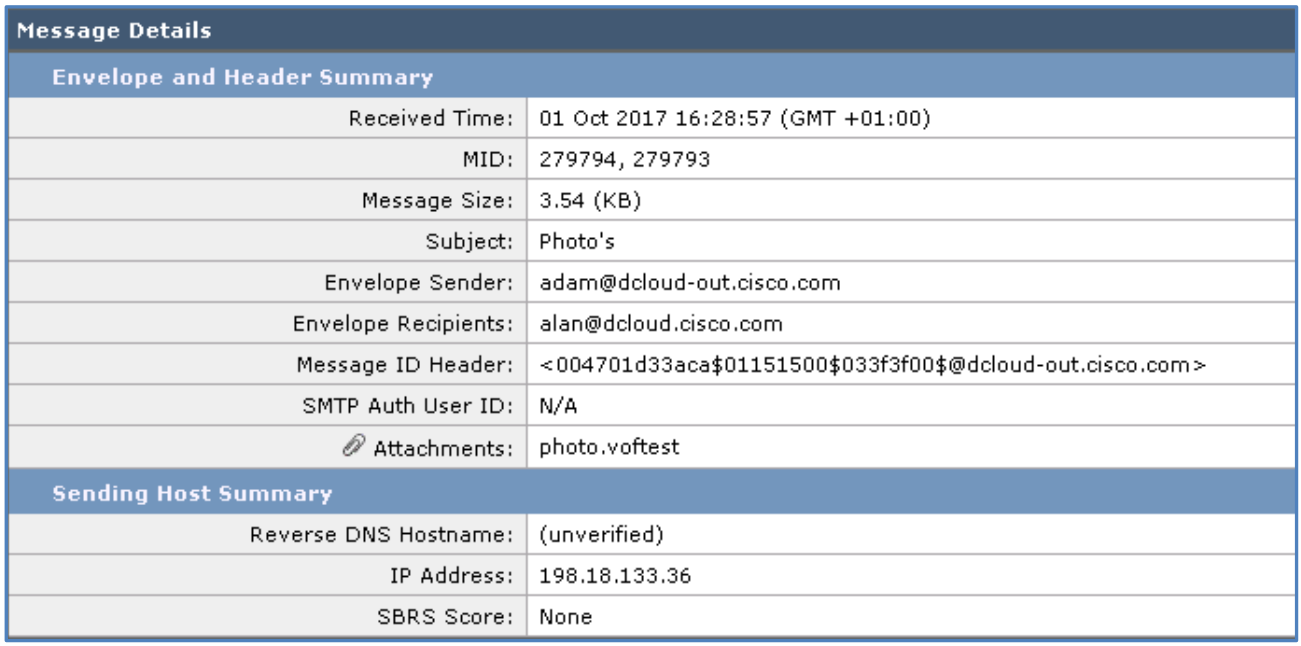
Displaying 1 — 1 of 1 items.

1 01 Oct 2017 16:28:57 (GMT +01:00) MID: 279793

SENDER: adam@dcloud-out.cisco.com
RECIPIENT: alan@dcloud.cisco.com
SUBJECT: Photo's
LAST STATE: Message 279794 quarantined to Outbreak by Outbreak Filters rule. OUTBREAK
photo.voftest

Displaying 1 — 1 of 1 items.

9. Click **Show Details** to get further details on how this message was processed by the Cisco Email Security Solution and the impact of the various engines. Finally, the outbreak filter verdict and final action – send to quarantine.



Message Details

Envelope and Header Summary	
Received Time:	01 Oct 2017 16:28:57 (GMT +01:00)
MID:	279794, 279793
Message Size:	3.54 (KB)
Subject:	Photo's
Envelope Sender:	adam@dcloud-out.cisco.com
Envelope Recipients:	alan@dcloud.cisco.com
Message ID Header:	<004701d33aca$01151500$033f3f00$@dcloud-out.cisco.com>
SMTP Auth User ID:	N/A
Attachments:	photo.voftest
Sending Host Summary	
Reverse DNS Hostname:	(unverified)
IP Address:	198.18.133.36
SBRS Score:	None

Processing Details

	MAIL POLICY "DEFAULT" MATCHED THESE RECIPIENTS: alan@dcloud.cisco.com
01 Oct 2017 16:28:57 (GMT +01:00)	Protocol SMTP interface Network (IP 198.18.133.146) on incoming connection (ICID 6468) from sender IP 198.18.133.36. Reverse DNS host None verified no.
01 Oct 2017 16:28:57 (GMT +01:00)	(ICID 6468) ACCEPT sender group UNKNOWNLIST match sbrs[none] SBRS None country None
01 Oct 2017 16:28:57 (GMT +01:00)	Start message 279793 on incoming connection (ICID 6468).
01 Oct 2017 16:28:57 (GMT +01:00)	Message 279793 enqueued on incoming connection (ICID 6468) from adam@dcloud-out.cisco.com.
01 Oct 2017 16:28:57 (GMT +01:00)	Message 279793 on incoming connection (ICID 6468) added recipient (alan@dcloud.cisco.com).
01 Oct 2017 16:28:57 (GMT +01:00)	Message 279793 contains message ID header '<004701d33aca$01151500$033f3f00$@dcloud-out.cisco.com>'.
01 Oct 2017 16:28:57 (GMT +01:00)	Message 279793 original subject on injection: Photo's
01 Oct 2017 16:28:57 (GMT +01:00)	Message 279793 (3628 bytes) from adam@dcloud-out.cisco.com ready.
01 Oct 2017 16:28:57 (GMT +01:00)	Message 279793 contains attachment 'photo.voftest'.
01 Oct 2017 16:28:57 (GMT +01:00)	Message 279793 matched per-recipient policy DEFAULT for inbound mail policies.
01 Oct 2017 16:28:58 (GMT +01:00)	Message 279793 scanned by Anti-Spam engine: CASE. Interim verdict: negative
01 Oct 2017 16:28:58 (GMT +01:00)	Message 279793 scanned by Anti-Spam engine CASE. Interim verdict: definitely negative.
01 Oct 2017 16:28:58 (GMT +01:00)	Message 279793 scanned by Anti-Spam engine: CASE. Final verdict: Negative
01 Oct 2017 16:28:58 (GMT +01:00)	Message 279793 scanned by Anti-Virus engine Sophos. Interim verdict: CLEAN
01 Oct 2017 16:28:58 (GMT +01:00)	Message 279793 scanned by Anti-Virus engine. Final verdict: Negative
01 Oct 2017 16:28:58 (GMT +01:00)	Message 279793 scanned by Outbreak Filters. Verdict: Positive
01 Oct 2017 16:28:58 (GMT +01:00)	Message 279793 Virus Threat Level=3
01 Oct 2017 16:28:58 (GMT +01:00)	Message 279793 contains attachment types voftest
01 Oct 2017 16:28:58 (GMT +01:00)	Message 279793 rewritten as new message 279794 by add-heading Heading Stamping filter
01 Oct 2017 16:28:58 (GMT +01:00)	Message 279794 quarantined to Outbreak by Outbreak Filters rule. OUTBREAK_0000190

10. Close the window to return to the Message Tracking window
11. Click the **Back to Quarantine** hyperlink, just below the Results section.

Results

Displaying 1 — 1 of 1 items.

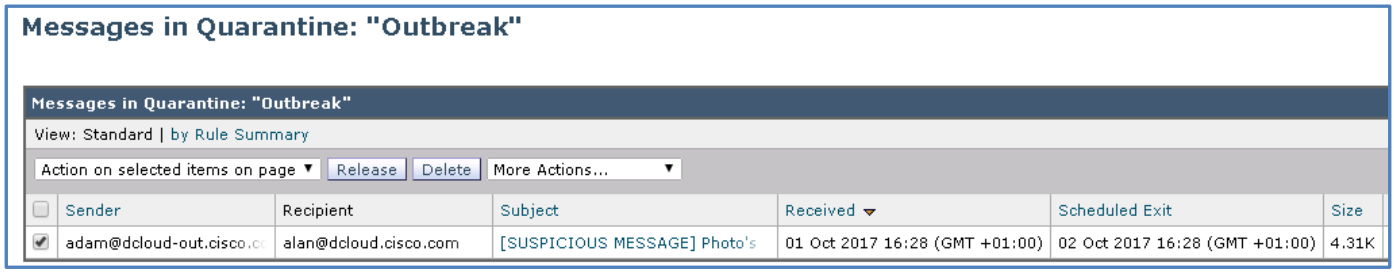
1 01 Oct 2017 16:28:57 (GMT +01:00) MID: 279793

SENDER: adam@dcloud-out.cisco.com
RECIPIENT: alan@dcloud.cisco.com
SUBJECT: Photo's
LAST STATE: Message 279794 quarantined to Outbreak by Outbreak Filters rule. OUTBREAK
photo.voftest

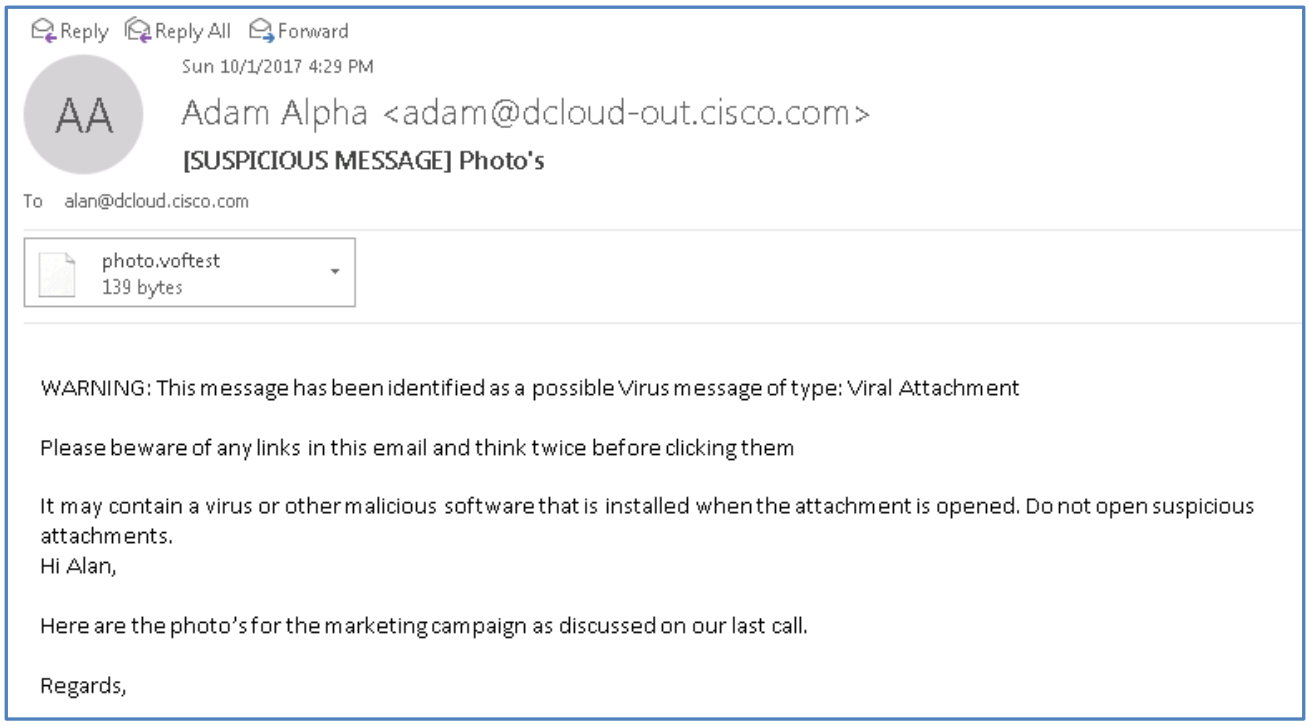
Displaying 1 — 1 of 1 items.

Back to Quarantine

12. Note the subject header, place a checkmark against the message and click the **Release** button, acknowledging the action when prompted



13. Navigate back to the outlook client and force the mailboxes to synchronize, the message will now appear in Alan's inbox and the subject header has been pre-pended as per our policy and warning information applied to the body of the file advising the recipient to exercise caution.



14. Navigate back to the CLI window, and note how once the message is

Scenario 4. Forged Email Detection

Use Case

Business leaders congregated for a conference to discuss the next generation of Internet of Things (IoT) challenges the customers of Voyage and its partners will potentially face over the coming years in order to address the rapid acceleration connected devices and the security challenges that will unfold. Voyage see this as great opportunity to gain further market share with their current offerings and mandated that key members of the business development team attend. Several market researchers were present and additional information that was needed on the back of key meetings was to be distributed after the event by email.

On return from the event the Director of operations reported receiving an email demanding immediate payment for an overdue invoice. Upon closer examination of the request additional confirmation of its authenticity was sought and it then materialised that this request was not legitimate.

Security Control

The Cisco Email Security solution can detect fraudulent messages with forged sender address *(From: header)* and perform specified actions on such messages.

For example, it is possible to detect messages with forged sender address and replace the *From:* header with the Envelope Sender. In this case, the employee will see the email address of the real sender (fraudsters) instead of the forged email address.

Objective

This scenario demonstrates how Forged Email Detection (FED) protects a selected targeted user or group (typically executives that have high levels of corporate access, fiduciary and financial control) from phishing attacks.

Low volume, targeted threats can be difficult to detect. Forging, or spoofing, email is easy to do. It can be done from within a LAN or from an external environment using Trojans. Forged email is often used in spam and phishing campaigns.

This scenario focuses on the resolution of spoofs that come from outside an organization when a sender impersonates an employee.

NOTE: Some of the basic pre-requisites for this scenario have been configured ahead of time, such as disclaimers. The creation of disclaimers for this exercise is similar to those experienced in the previous scenario.

Steps

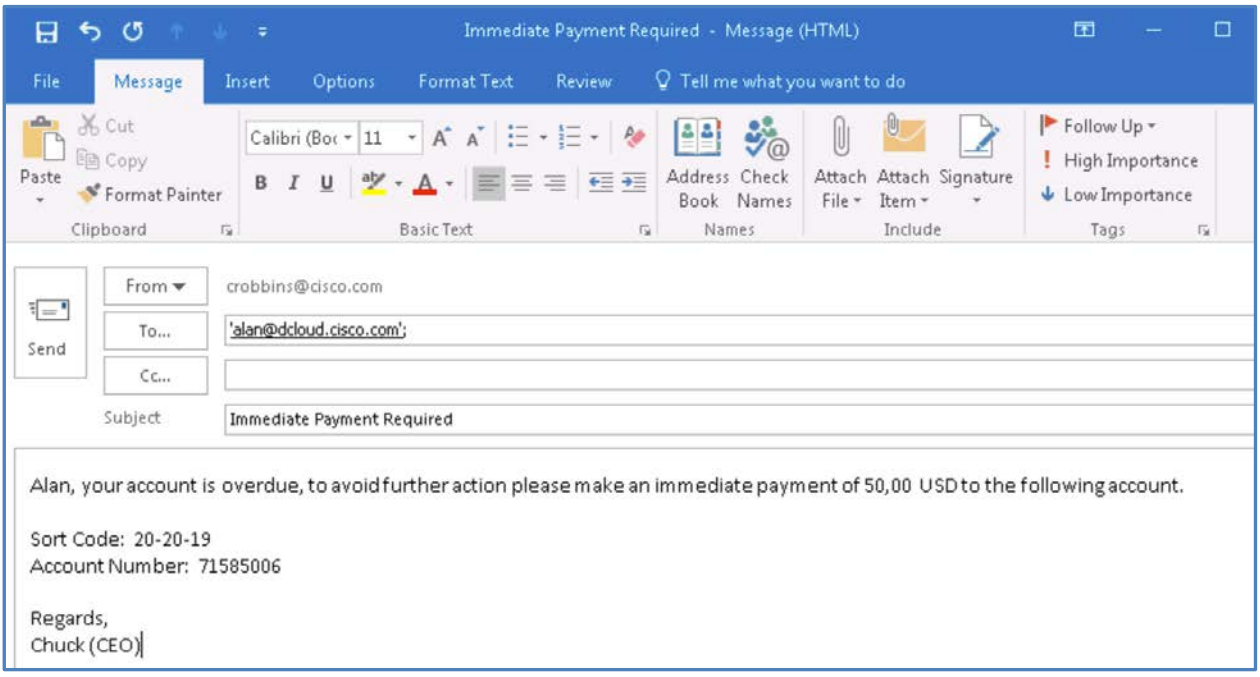
Task - Sending a Spoofed email (Estimated time to complete: 3 min)

This task will demonstrate what a potentially forged email looks like and how easy it is to craft and send using basic skills. At first glance as the message lands in the mailbox of the indented target it can look like the email has come from the spoofed sender.

1. From the workstation launch Microsoft Outlook and from Adams inbox, prepare a new message with the following parameters.
   - From: crobbins@cisco.com
   - To: alan@dcloud.cisco.com
   - Subject: Immediate Payment Required
   - Body: Alan, your account is overdue, to prevent further action please make an immediate payment of 50,000 USD to the following account:

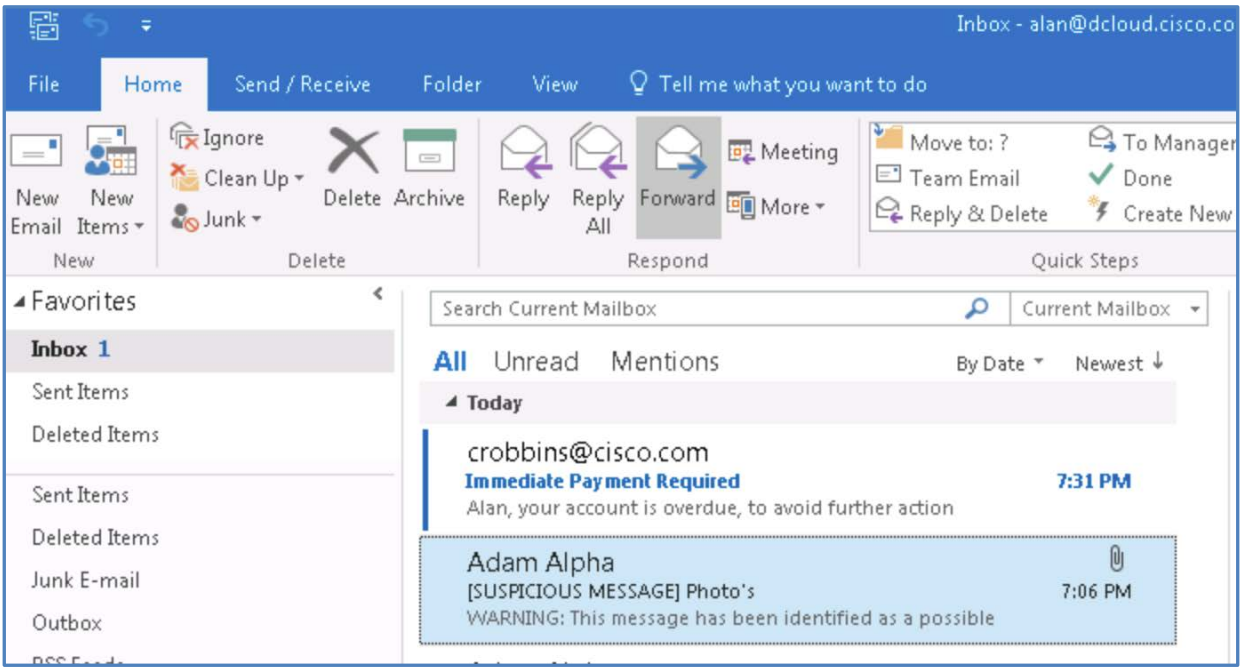
     Sort Code: 20-20-19
     Account: 71584006

     Regards,
     Chuck (CEO).



2. Send the email - Force the synchronization process by clicking **Send/Receive Folder** or by pressing the **F9** key.

3. Examine Alan's inbox to verify receipt of the message. It should appear as if it has indeed come from *Chuck Robbins* at first.



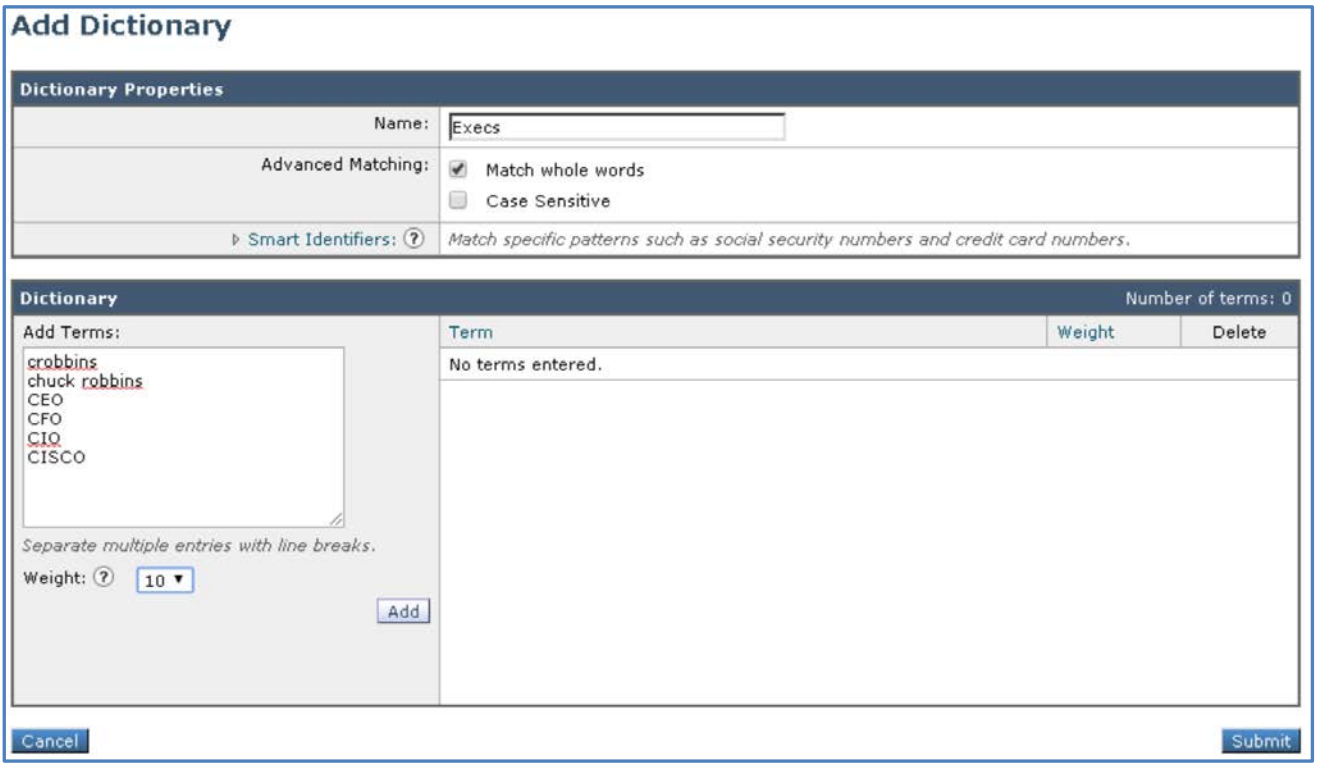
Task - Creating a Content Dictionary of Terms

The first task in tackling this undesired behavior is to create a content dictionary containing the names of high-profile figures that are most likely to be targeted by this type of attack.

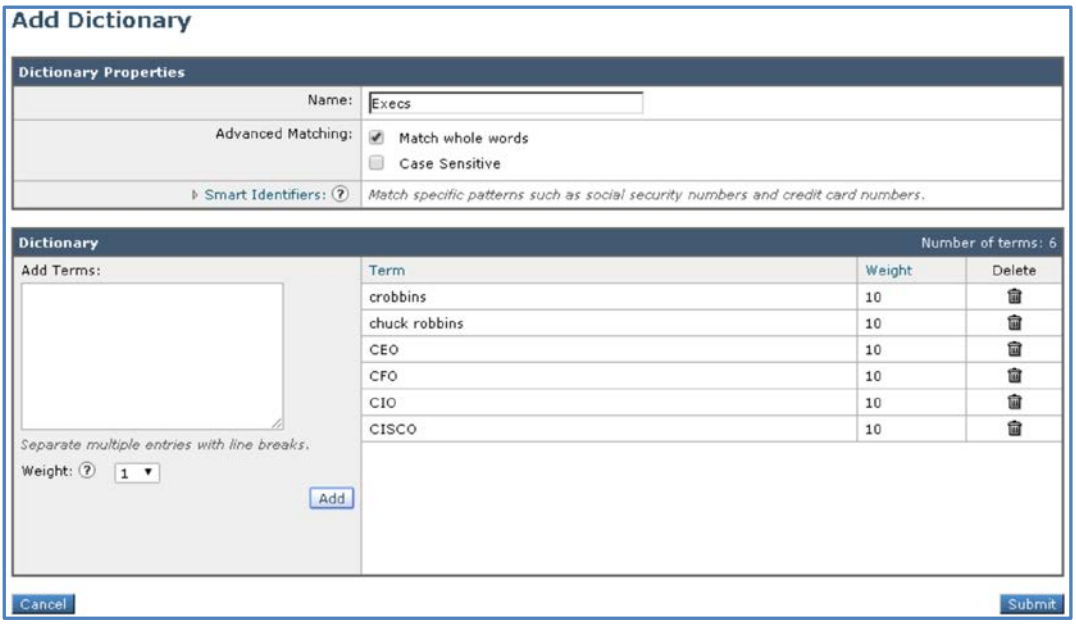
Content dictionaries are groups of words or entries that work in conjunction with the Body Scanning feature on the solution and are available to both content and message filters. Dictionaries can also be used to define to scan messages, message headers, and message attachments for terms included in the dictionary in order to take appropriate action in accordance with your corporate policies. This task, will create a content dictionary to list the names of potential targets internal to our organization.

1. From the workstation access the GUI and navigate to **Mail Policy > Dictionaries** from the resulting window, click **Add Dictionary** - this will create the custom dictionary with the names of the identified users.
2. Populate the dictionary with the following information:
   - Name: Execs
   - Add Terms: crobbins
     chuck robbins
     CEO
     CFO
     CIO
     CISCO
   - Weight: 10

NOTE: Multiple terms can be added to the dictionary in one go by separating each term with a line break



3. Click the **Add** Button to add the terms to the dictionary.



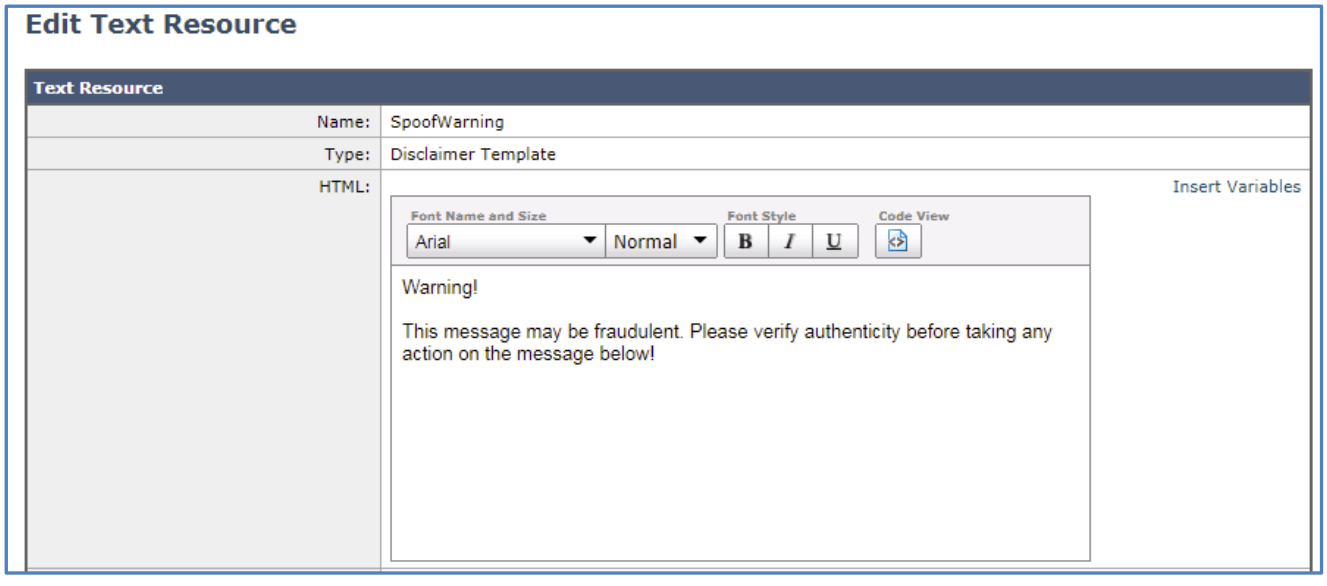
4. Click **Submit** to create the dictionary.

5. Ensure changes are applied by clicking the **Commit Changes** button, adding optional comments if desired

Task - Reviewing the Disclaimer Template (Estimated time to complete: 1 min)

Ahead of this lab a custom disclaimer was created that will be inserted into the email of the intended target. This task will review the warning that is presented to the recipient of the email with custom text advising them of potential inconsistencies within the email message.

1. Navigate to **Mail Policies > Text Resources** and click the pre-configured text resource **SpoofWarning**
2. Similar to the other disclaimer this text resource is fully customisable with HTML style input to suits an organization's needs. The purpose of this message is to advise the recipient to heed caution when addressing this message.

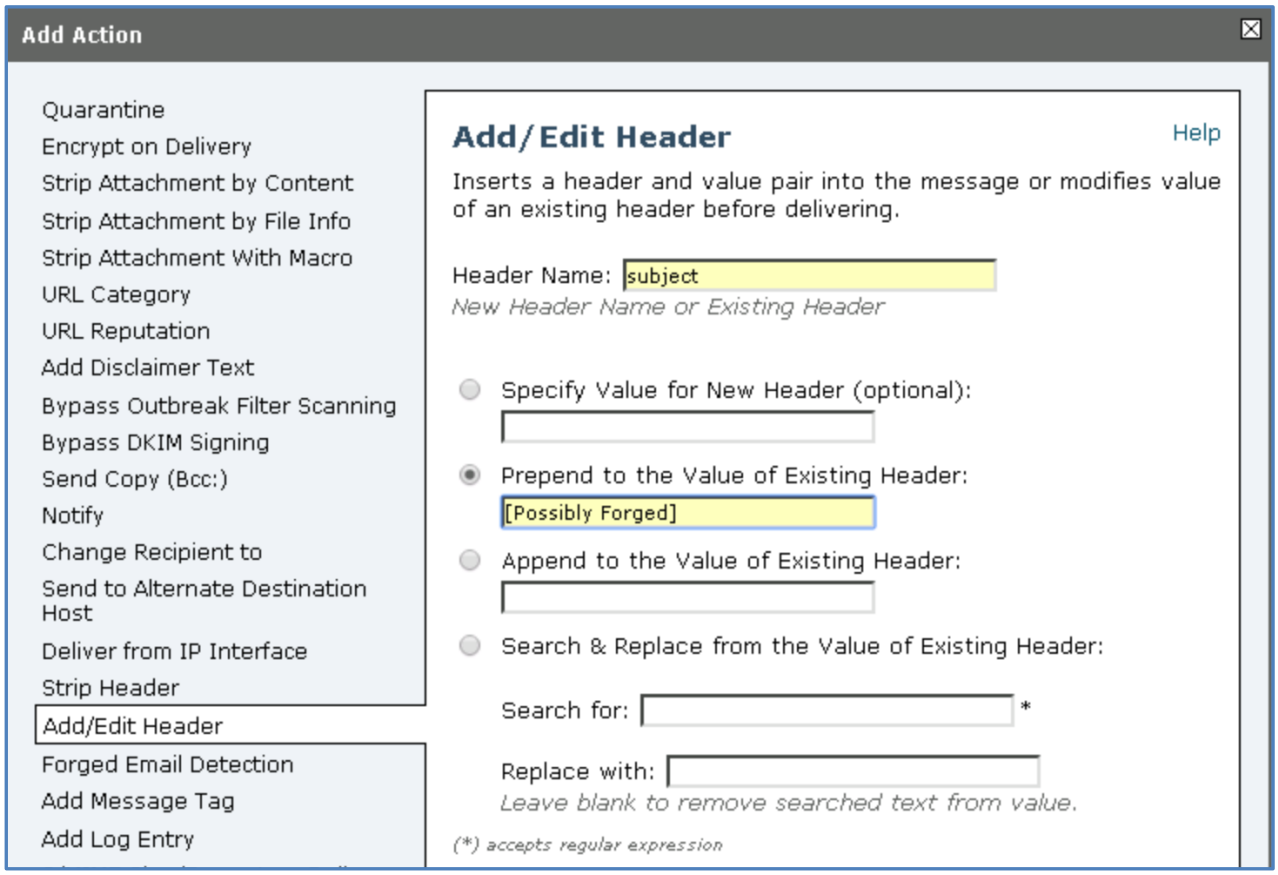


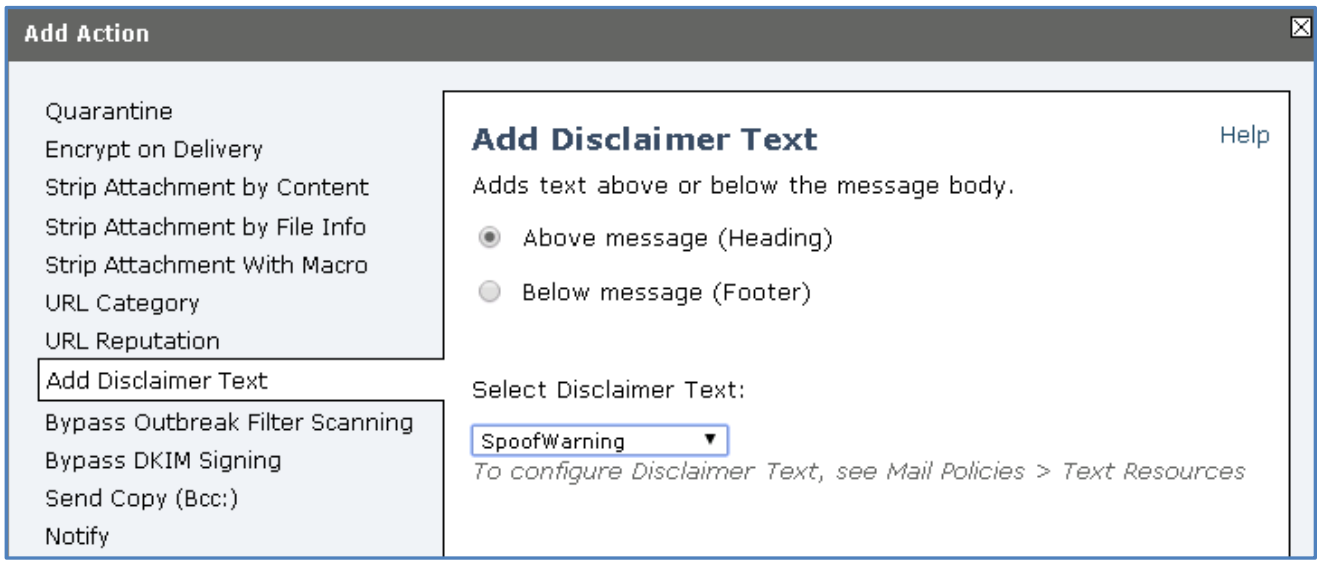
3. Edit the warning if required, or alternatively exit the screen by clicking the **Cancel**.

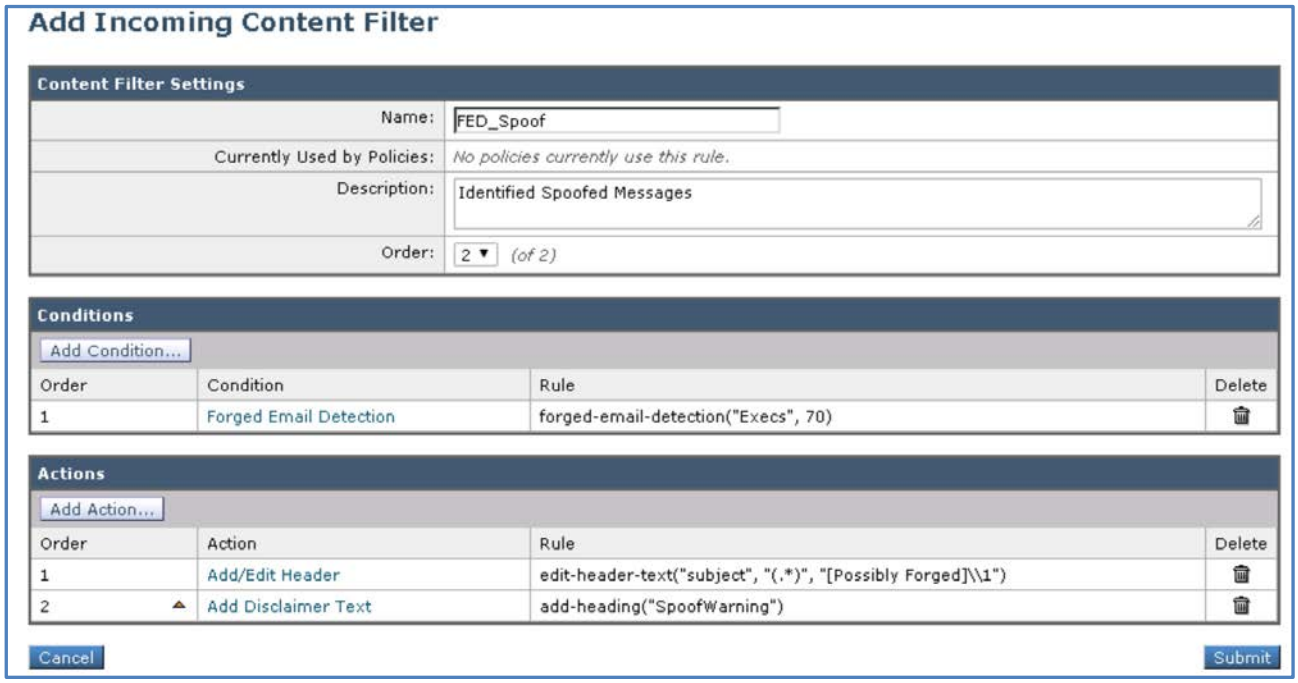
Task - Configuring a Content Filter (Estimated time to complete: 3 min)

Similar to Outbreak Filters in the previous scenario, content filters allow for granularity in policies to identify content. This task will create a new content filter and use the content dictionary created in the previous step.

1. From the workstation access the GUI and navigate to **Mail Policy > Incoming Content Filters** and click **Add Filter** using the following settings configure the Conditions and Actions.
   - Name: FED_Spoof
   - Description: Identify Forged Email Messages
   - Conditions: Forged Email Detection>Content Dictionary: Execs, Similarity score 70
   - Action 1: Add/Edit Header>Header Name: subject
     Prepend to the Value of Existing Header: [Possibly Forged]
   - Action 2: Add Disclaimer Text>Select Disclaimer Text: SpoofWarning

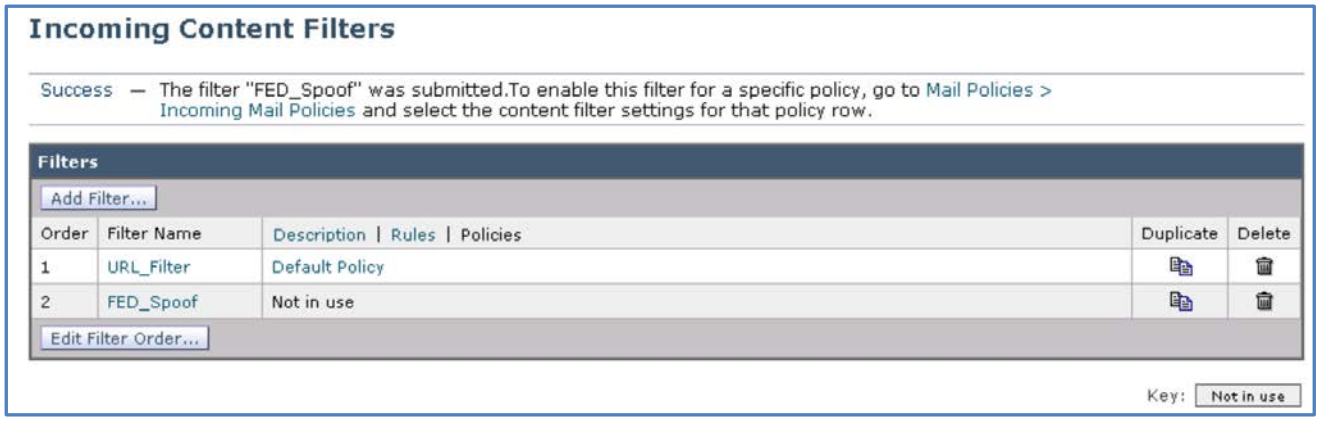




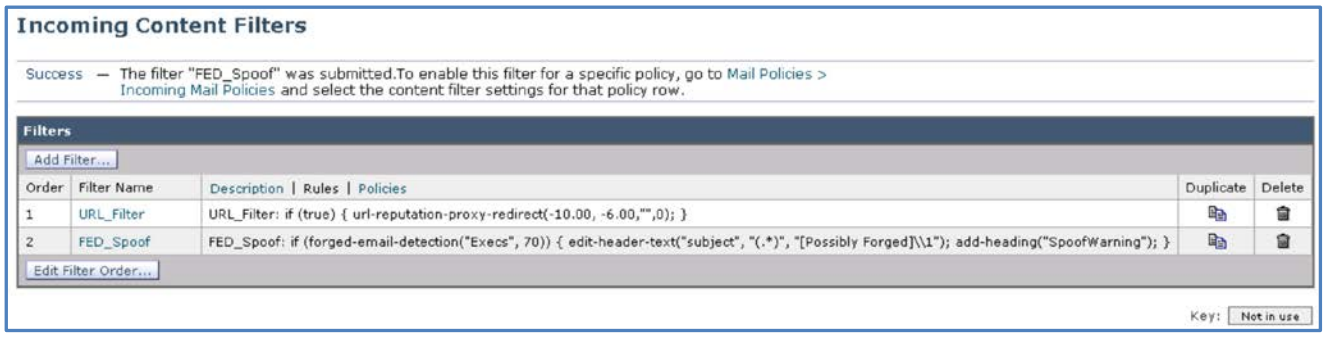


NOTE: Content filters typically comprise Conditions and then Actions. The condition here is using the Execs dictionary and a similarity score to determine the likelihood of a forged email. The higher the score, between 1-100, the more likely a message is forged.

2. Click **Submit** to create the content Filter. Once complete ensure the changes are applied by clicking the **Commit Changes** button, adding optional comments if desired.



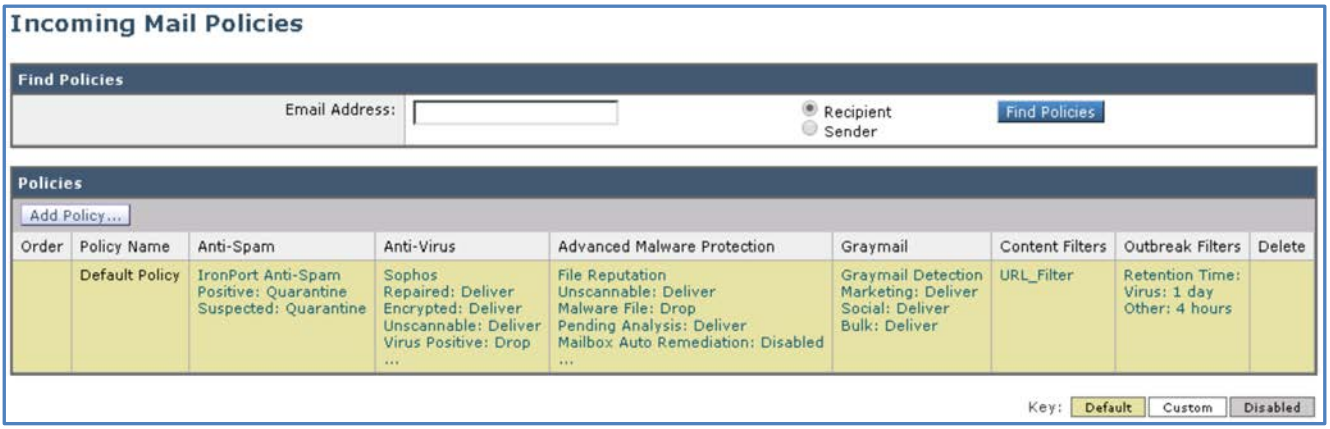
3. The content filter is not in use as it has not been tied to an incoming mail policy yet.
4. Click on **Rules** to display the syntax of the filter, this is exactly what would need to be input if this was a Message Filter as opposed to a Content Filter.



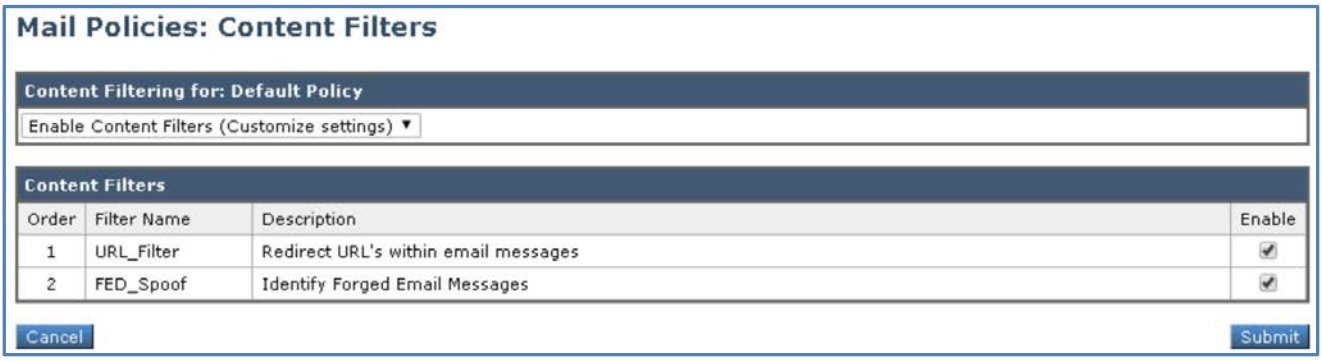
Task - Edit Incoming Mail Policy (Estimated time to complete: 1 min)

The final task is to modify the default incoming mail policy so the content filter comes into effect.

1. Navigate to **Mail Policy > Incoming Mail Policies** and click within the Content Filters box of the Default Policy.

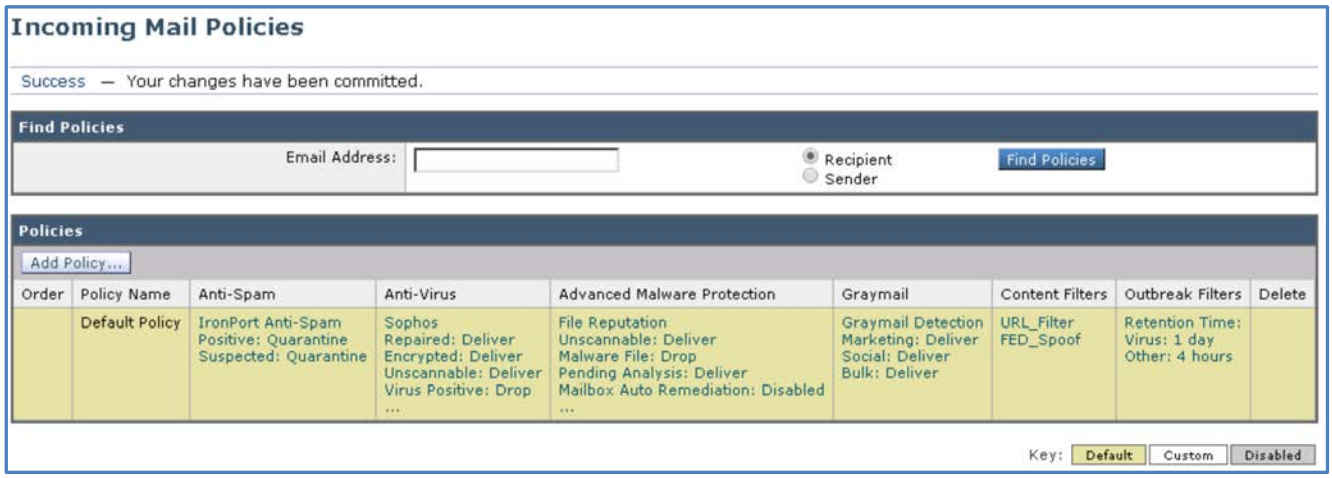


2. Place a checkmark against the content filter FED_Spoof created in the previous step to enable it.



3. Click **Submit** to create the content Filter. Once complete ensure the changes are enabled by clicking the **Commit Changes** button, adding optional comments if desired.

4. Finally verify the Default Policy has the FED_Spoof has been added.



Task - Testing Forged Email Detection (Estimated time to complete: 5 min)

With the configuration in place, the Forged Email Detection feature can be tested by repeating the first task that was carried out for this scenario, once again sending a message with exactly the same text.

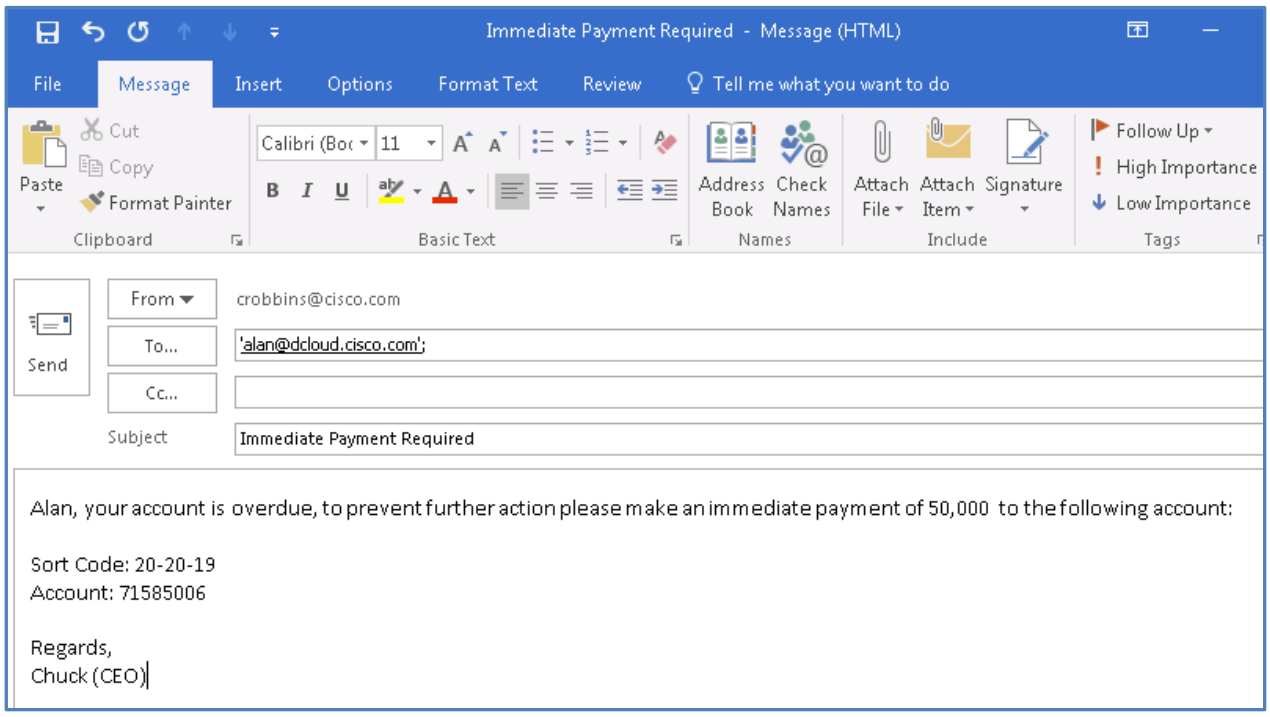
Initiate a CLI session

Prior to preparing the message, initiate a connection to the Cisco Email Security solution from the CLI in order to view, using the tail command, the mail logs to see the message being processed and the actions being applied as it works its way through the pipeline, repeat the same steps to initiate this from the previous scenario.

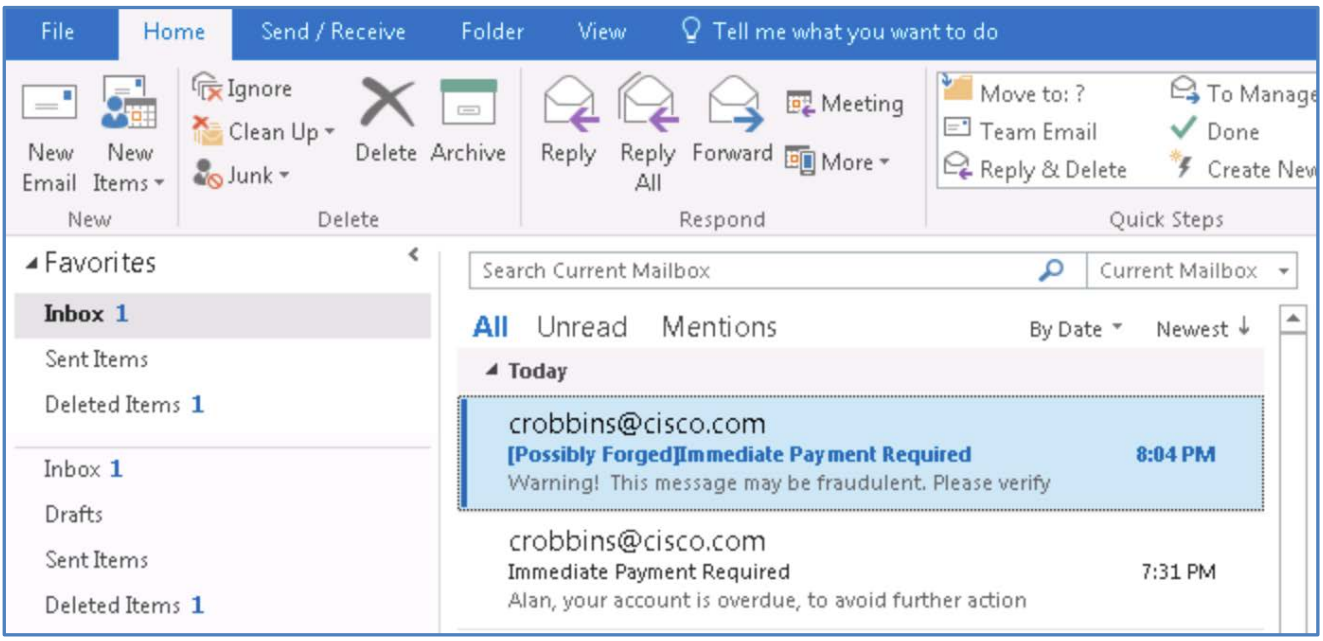
1. From the workstation launch Microsoft Outlook and from Adams inbox, prepare a new message with the following parameters.
    - From: crobbins@cisco.com
    - To: alan@dcloud.cisco.com
    - Subject: Immediate Payment Required
    - Body: Alan, your account is overdue, to prevent further action please make an immediate payment of 50,000 USD to the following account:

      Sort Code: 20-20-19
      Account: 71584006

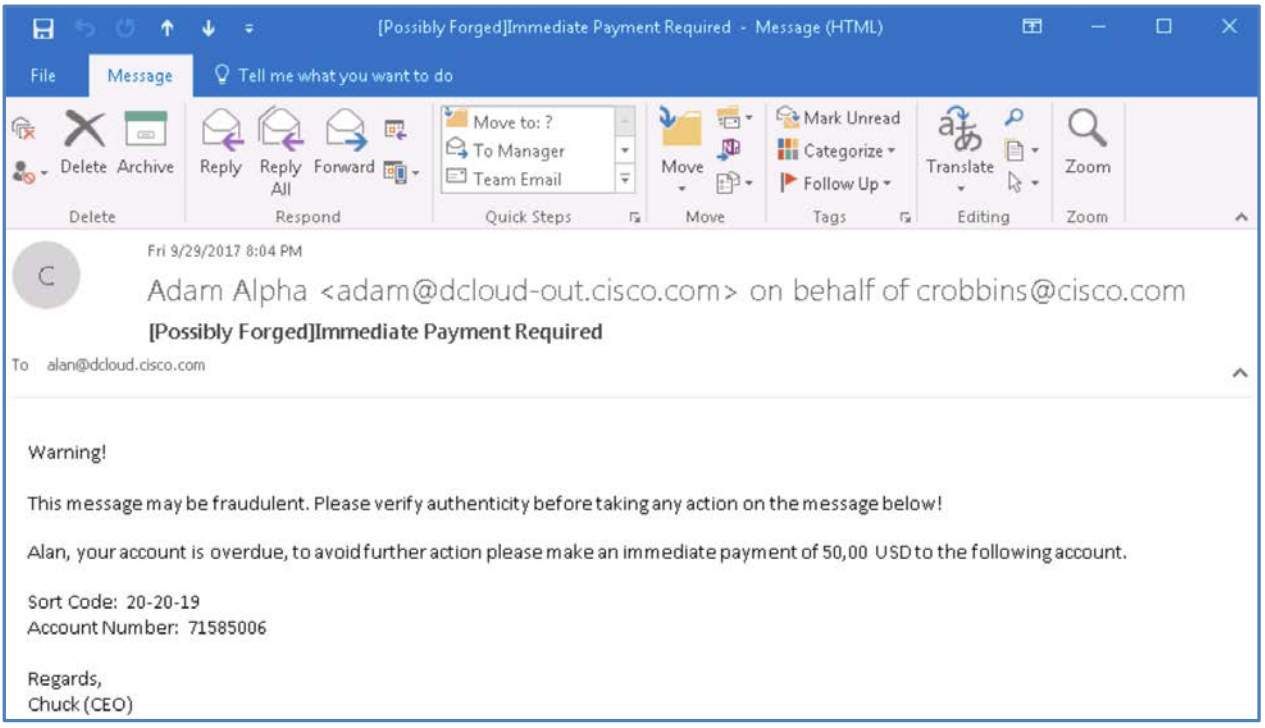
      Regards,
      Chuck (CEO).



2. Send the email - Force the synchronization process by clicking **Send/Receive Folder** or by pressing the **F9** key.
3. Examine Alan's inbox to verify receipt of the message. It should appear as if it has indeed come from *Chuck Robbins* at first glance, however some modifications should now be evident from what was observed from the first task.
4. Firstly, the subject header has been modified – prepended with additional custom text to advise the mail recipient immediately that there is something not right about this incoming message.



5. Secondly, when opening the message, a disclaimer has been added advising the mail recipient to exercise caution when responding to this message.

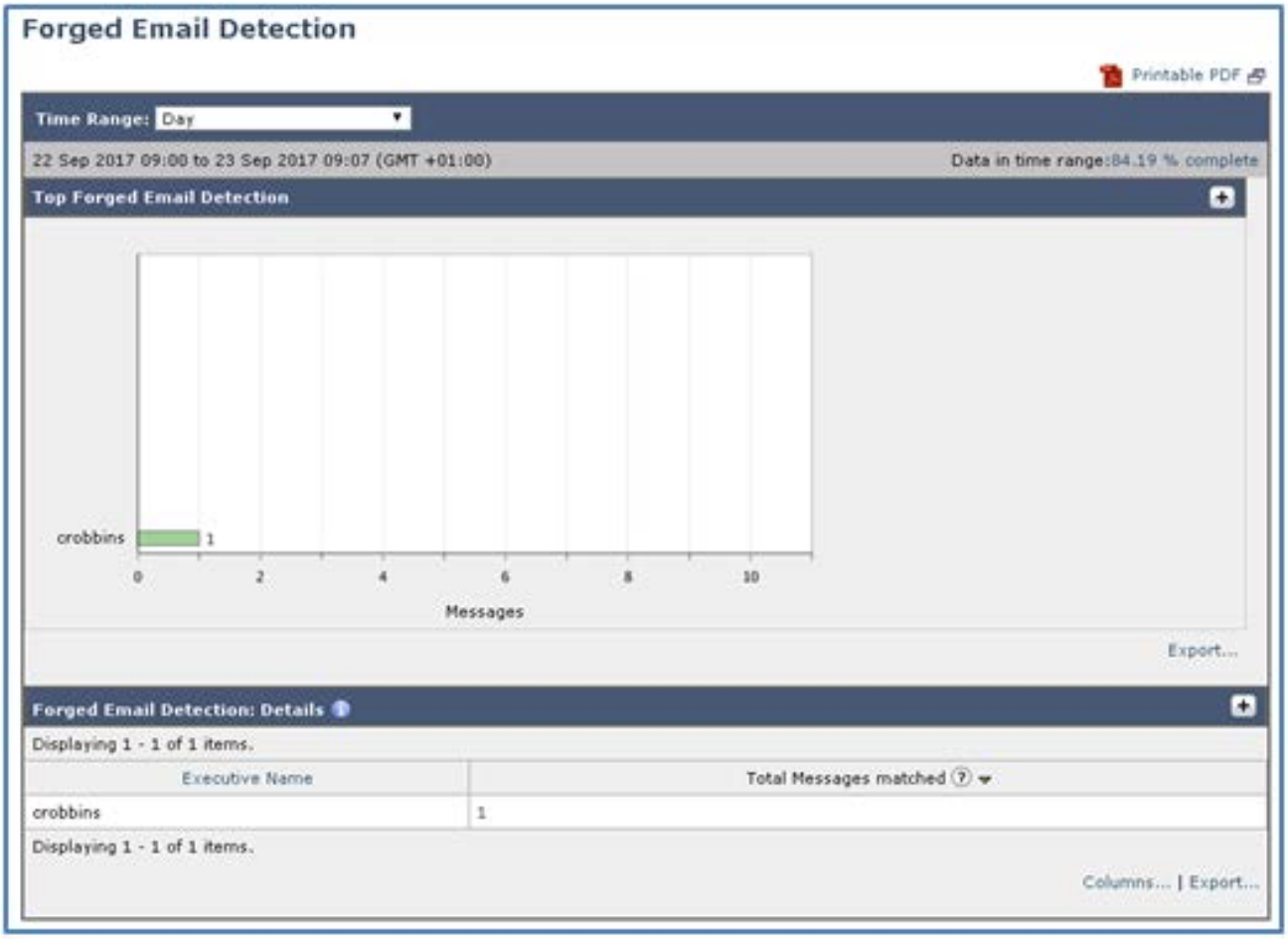


6. Navigate back to the CLI window, and note how this type of message is handled by the engine.

```
Fri Sep 29 20:04:02 2017 Info: Start MID 279762 ICID 6446
Fri Sep 29 20:04:02 2017 Info: MID 279762 ICID 6446 From: <adam@dcloud-out.cisco.com>
Fri Sep 29 20:04:02 2017 Info: MID 279762 ICID 6446 RID 0 To: <alan@dcloud.cisco.com>
Fri Sep 29 20:04:02 2017 Info: MID 279762 Message-ID '<005801d33955$b708b180$251a1480$@cisco.com>'
Fri Sep 29 20:04:02 2017 Info: MID 279762 Subject 'Immediate Payment Required'
Fri Sep 29 20:04:02 2017 Info: MID 279762 ready 3516 bytes from <adam@dcloud-out.cisco.com>
Fri Sep 29 20:04:02 2017 Info: MID 279762 matched all recipients for per-recipient policy DEFAULT in the inbound table
Fri Sep 29 20:04:03 2017 Info: MID 279762 interim verdict using engine: CASE spam negative
Fri Sep 29 20:04:03 2017 Info: MID 279762 using engine: CASE spam negative
Fri Sep 29 20:04:03 2017 Info: MID 279762 interim AV verdict using Sophos CLEAN
Fri Sep 29 20:04:03 2017 Info: MID 279762 antivirus negative
Fri Sep 29 20:04:03 2017 Info: MID 279762 AMP file reputation verdict : SKIPPED (no attachment in message)
Fri Sep 29 20:04:03 2017 Info: MID 279762 using engine: GRAYMAIL negative
Fri Sep 29 20:04:03 2017 Info: MID 279762 Forged Email Detection on the From: header with score of 76, against the dictionary
 entry chuck robbins
Fri Sep 29 20:04:03 2017 Info: MID 279762 Outbreak Filters: verdict negative
Fri Sep 29 20:04:03 2017 Info: MID 279762 rewritten to MID 279763 by add-heading filter 'Heading Stamping'
Fri Sep 29 20:04:03 2017 Info: Message finished MID 279762 done
Fri Sep 29 20:04:03 2017 Info: MID 279763 queued for delivery
Fri Sep 29 20:04:03 2017 Info: New SMTP DCID 2551 interface 198.18.133.146 address 198.18.133.2 port 25
Fri Sep 29 20:04:03 2017 Info: Delivery start DCID 2551 MID 279763 to RID [0]
Fri Sep 29 20:04:03 2017 Info: Message done DCID 2551 MID 279763 to RID [0]
Fri Sep 29 20:04:03 2017 Info: MID 279763 RID [0] Response '2.6.0 <005801d33955$b708b180$251a1480$@cisco.com> [InternalId=11]
 Queued mail for delivery'
Fri Sep 29 20:04:03 2017 Info: Message finished MID 279763 done
```

7. Finally, further information about these events can be seen in the Monitor of the GUI.

8. From the workstation access the GUI and navigate to **Monitor > Forged Email Detection** to view what is being reported.



Scenario 5. Macro Detection

Use Case

Voyage Corp recently starting taking new custom from a newly formed organization across the state, this was seen as a potentially key account going forward and the Sales team insisted that all orders were processed quickly in order to remove any risk this company would seek to conduct its business elsewhere having experienced delays with their previous partner.

The average on boarding time for a new account is between 5-10 business days; this involved getting the account registered with the credit system as well as completes the necessary due-diligence by the in house legal teams prior to the online portal registering the customer for internet access.

To prevent any further delays and risk losing the business the regional account director asked for all orders in the interim to be accepted by email, citing the strategic importance of the account as a reason to expedite the process. Orders were sent via email for the first two days to a sales order analyst without any issue, one morning an email containing a Microsoft Excel file was received and opened and immediately caused local host instability, upon closer examination the local support teams declared the infected computer inoperable as the *TrojanDownloader: W97M/Adnel* infection had hidden itself inside a macro within that document that once opened spread very quickly. Immediately a decision was made to no longer accept messages with macro enabled attachments.

Security Control

Macros are a series of commands that can be run automatically to perform a task. Macrocode is embedded in Office documents written in a programming language known as Visual Basic for Applications (VBA). Macros could be used maliciously to drop malware, download malware, etc. Malicious macro files usually are received in Word documents or Excel spreadsheets but other formats do exist.

The Cisco Email Security Solution provides the ability to filter attachments, detect advanced malware and to scan for macro-based threats in attachments. The macro detection feature is designed to detect such macros using Content or Message filters.

Objective

This scenario walks through the configuration of the macro detection feature within the Cisco Email Security to drop potentially malicious macro embedded files.

Steps

Task - Configuring a Content Filter (Estimated time to complete: 3 min)

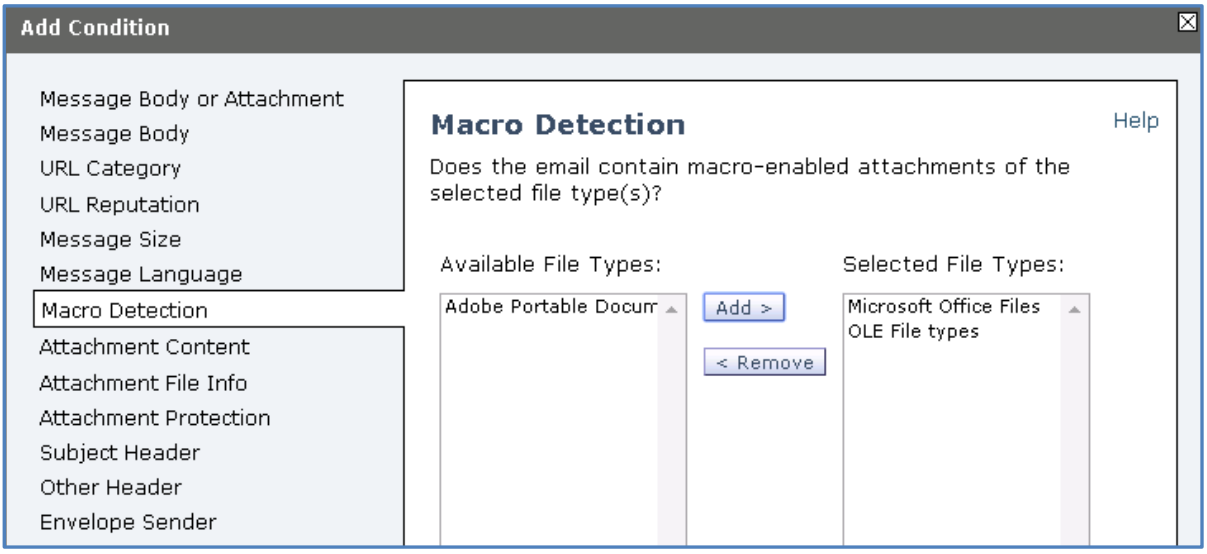
Similar to Forged Email Detection in the previous scenario, content filters help us get granular in policies to identify content. This task will create a new content filter to identify macros in documents and subsequently remove them.

1. From the workstation access the GUI and navigate to **Mail Policy > Incoming Content Filters** and click **Add Filter**.

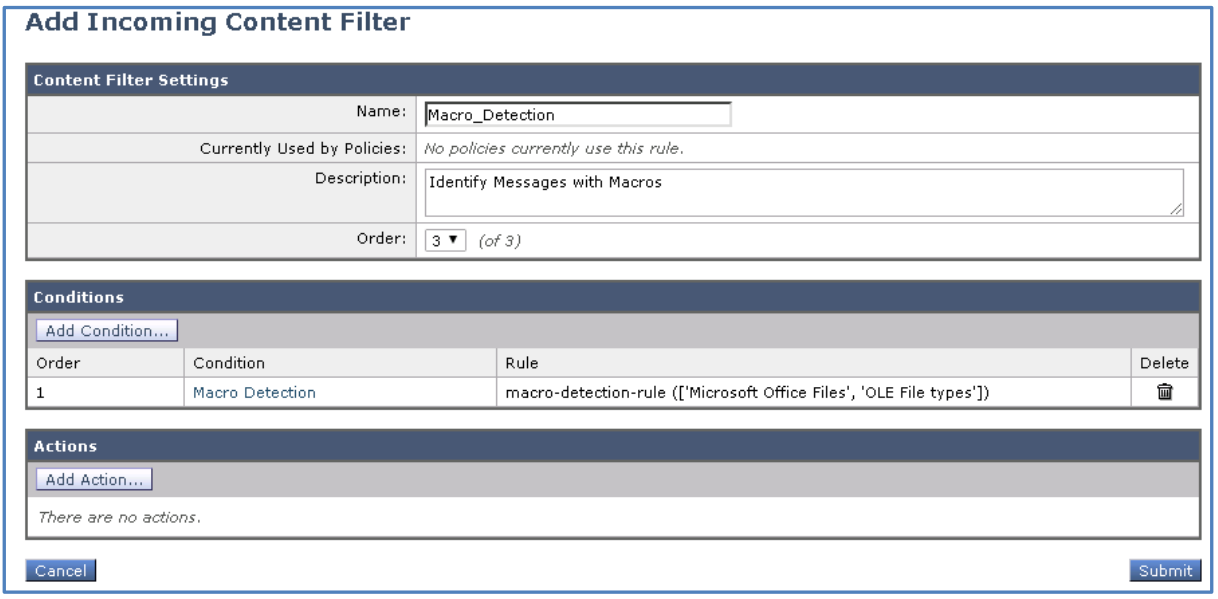
2. Using the following settings configure the *Conditions* and *Actions*.

   - Name: Macro_Detection
   - Description: Identify Messages with Macros
   - Conditions: Macro Detection>Available File Types>Microsoft Office Files, OLE File Types
   - Action 1: Strip Attachment with Macro>Available File Types> Microsoft Office Files, OLE File Types

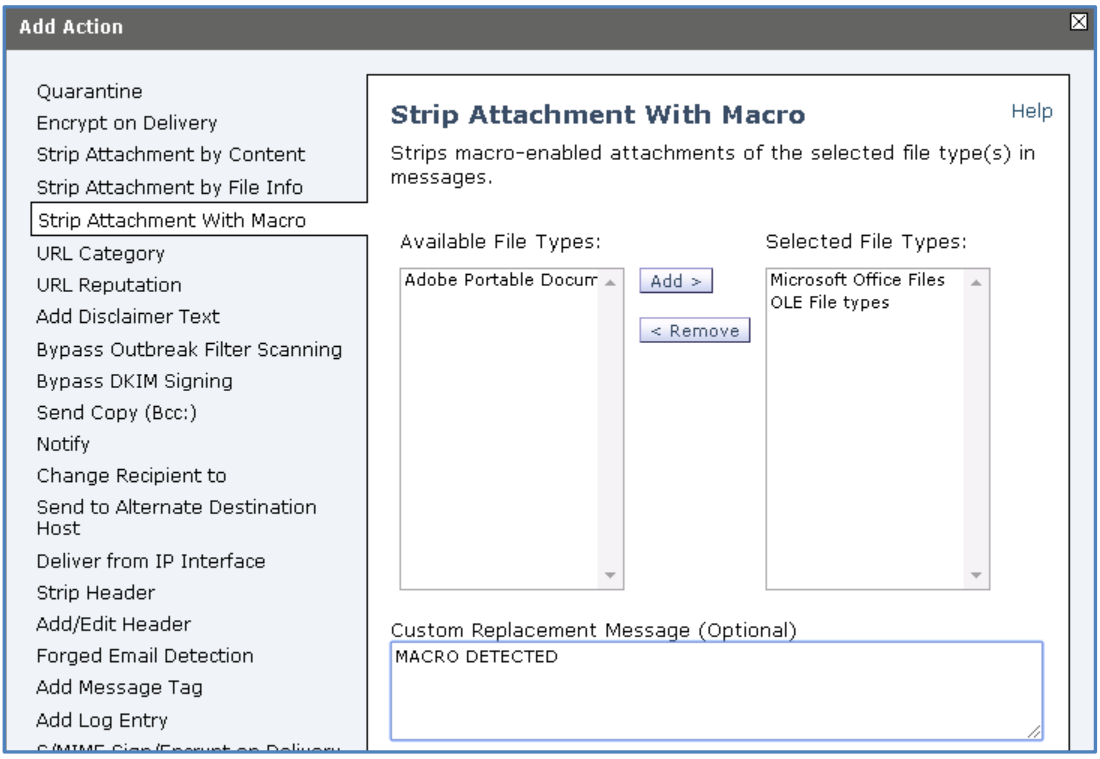
     Custom Replacement Message (Optional) : MACRO DETECTED



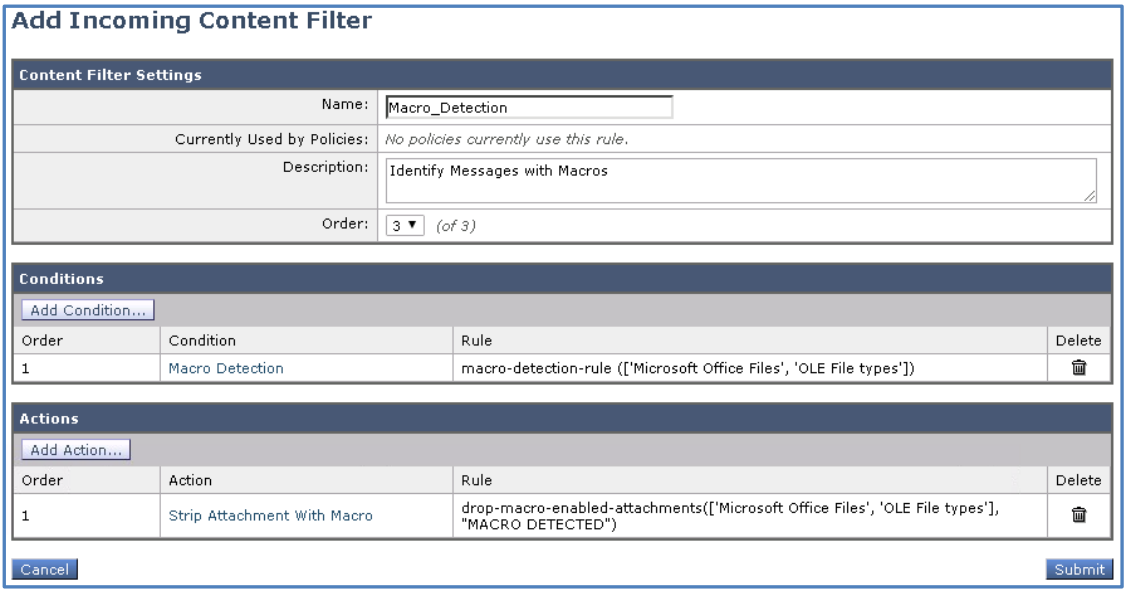
3. Click **OK**



4. Click **Add Action.**



5. Click **OK.**

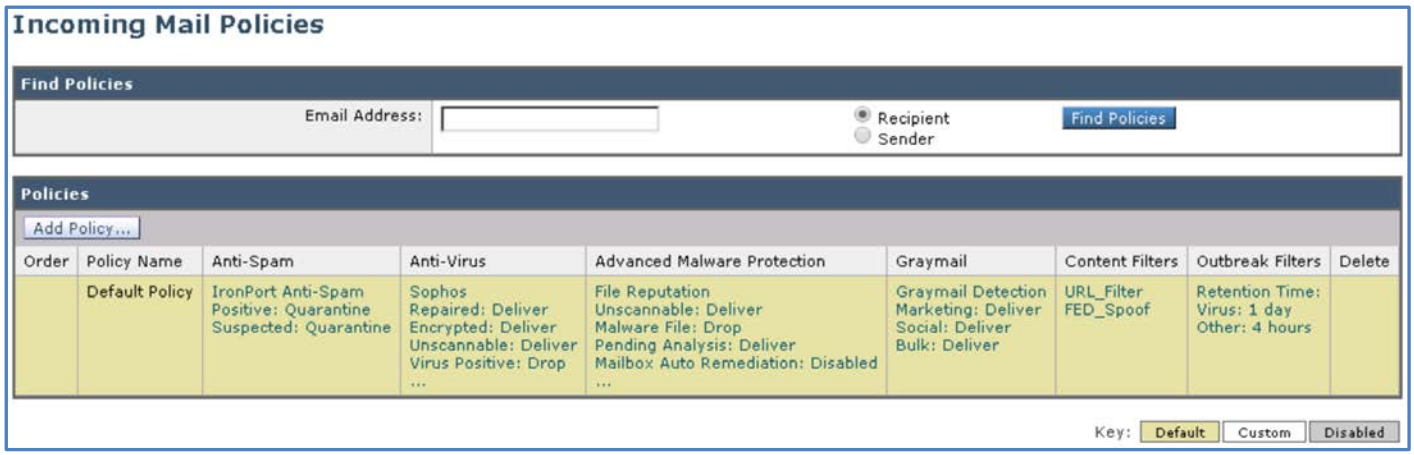


6. Click **Submit** to create the content Filter. Once complete, ensure you apply the change by clicking the **Commit Changes** button, adding optional comments if desired.

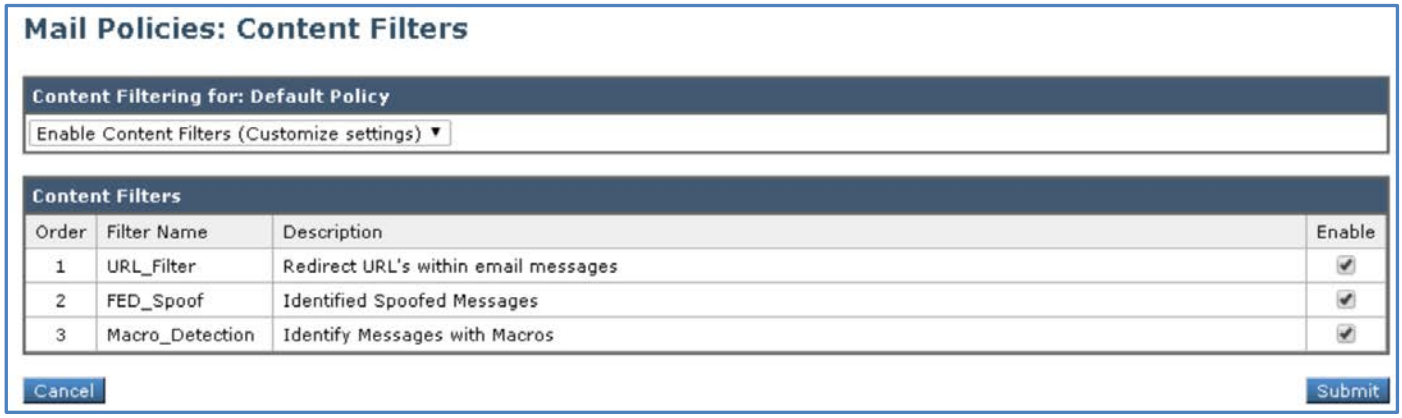
Task - Edit Incoming Mail Policy (Estimated time to complete: 1 min)

The final task is to modify the default incoming mail policy so the content filter comes into effect.

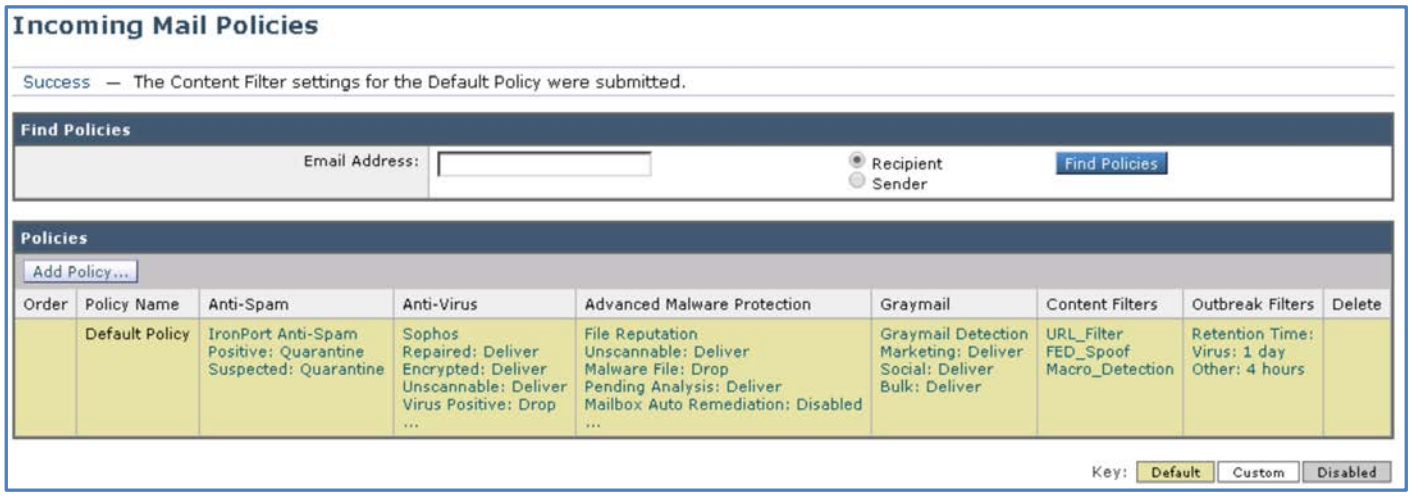
1. From the workstation access the GUI and navigate to **Mail Policy > Incoming Mail Policies** and click within the Content Filters box of the Default Policy.



2. Place a checkmark against the content filter Macro_Detection_In created in the previous step to enable it.



3. Click **Submit** to create the content filter and verify the policy.



4. Once complete, ensure the change is applied by clicking the **Commit Changes** button, adding optional comments if desired.

Task - Testing Macro Detection (Estimated time to complete: 5 min)

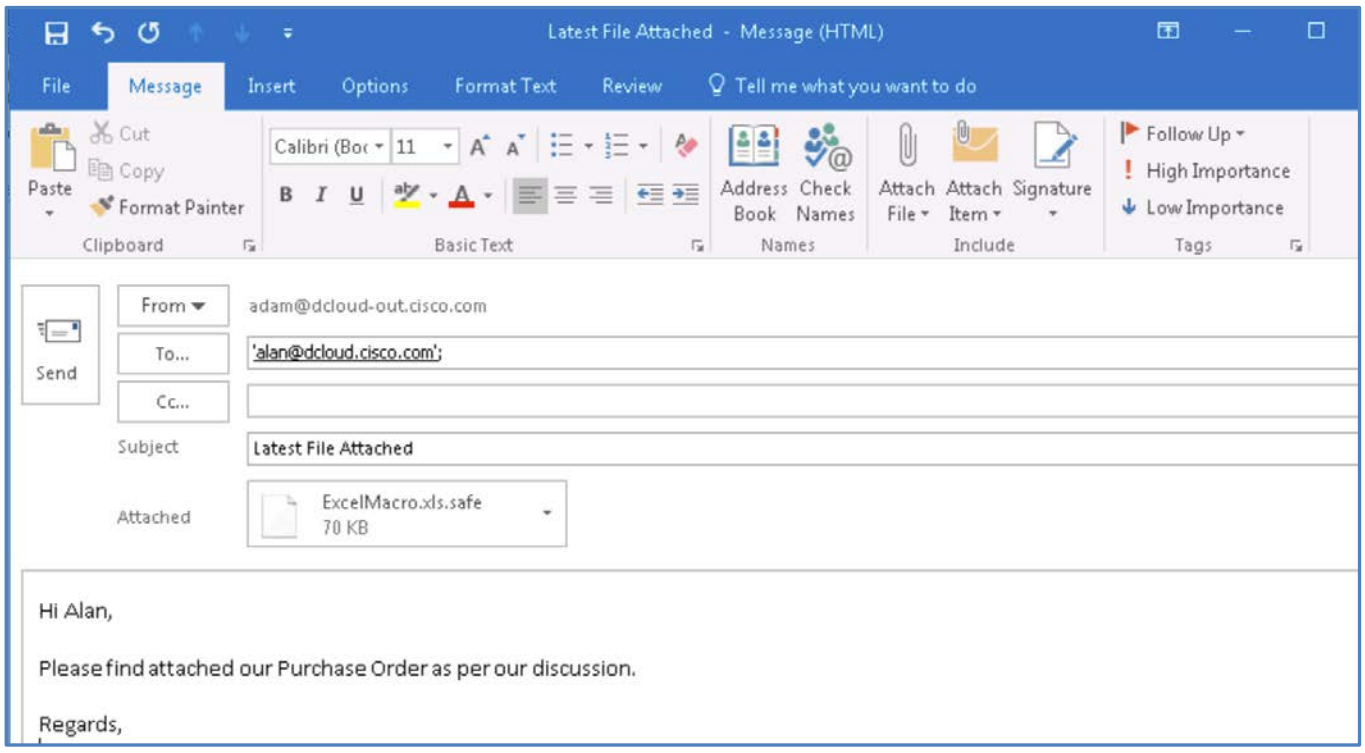
With the entire configuration in place, the Macro Detection feature can be tested by sending an email to Alan from external user Adam which contains an attachment that has a Macro within it.

Initiate a CLI session

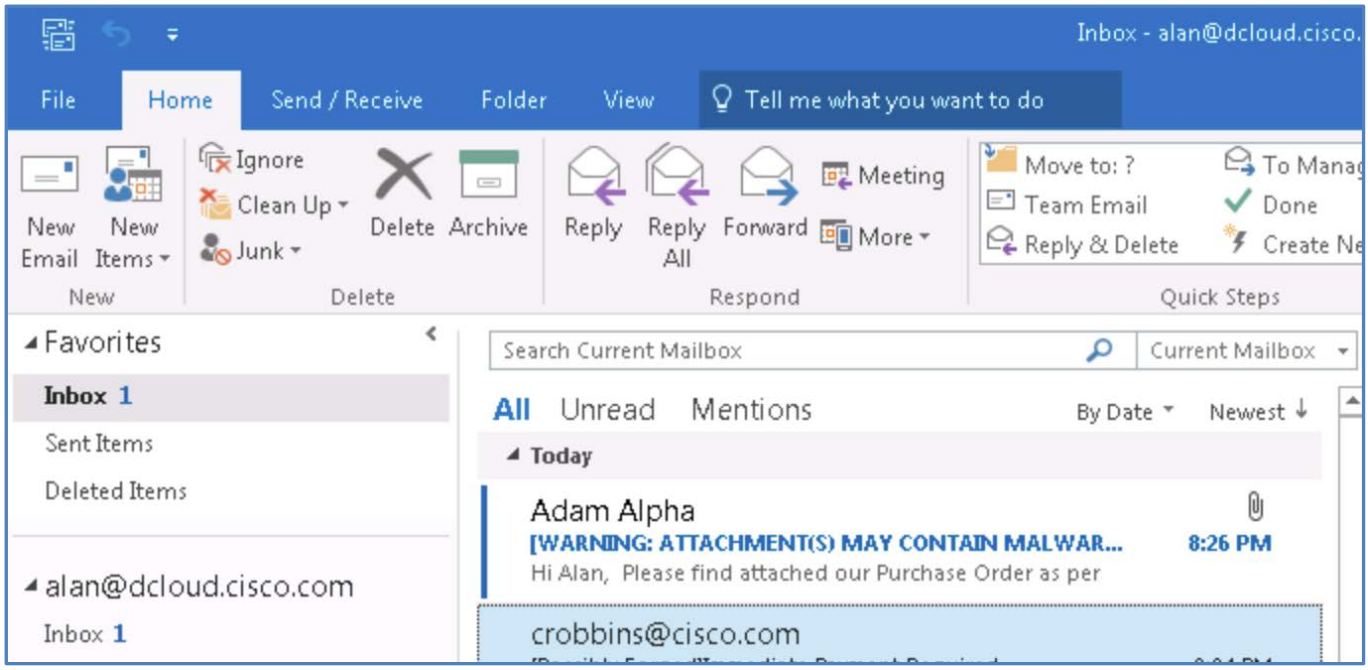
Prior to preparing the message, initiate a connection to the Cisco Email Security solution from the CLI in order to view, using the tail command, the mail logs to see the message being processed and the actions being applied as it works its way through the pipeline, repeat the same steps to initiate this from the previous scenario.

1. From the workstation launch Microsoft Outlook and from Adams inbox, prepare a new message with the following parameters.
   - To: alan@dcloud.cisco.com
   - Subject: Latest File Attached
   - Body: Hi,

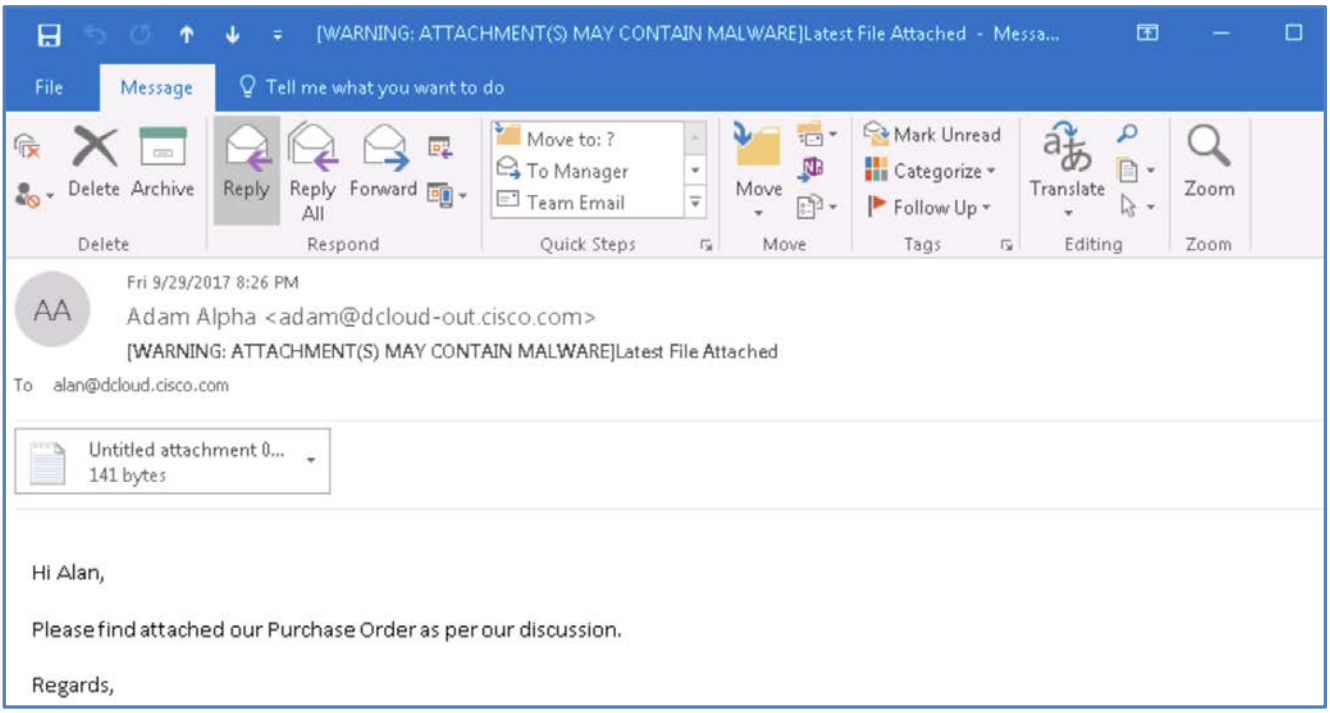
     Please find attached document as per our discussion.
   - Attachment: ExcelMacro.xls.safe- located on the desktop under the Macro-Enabled Detection sub-folder.



2. Send the email - Force the synchronization process by clicking **Send/Receive Folder** or by pressing the **F9** key.
3. Notice the message makes it into Alan's mailbox and the subject header has been modified advising the recipient immediately.



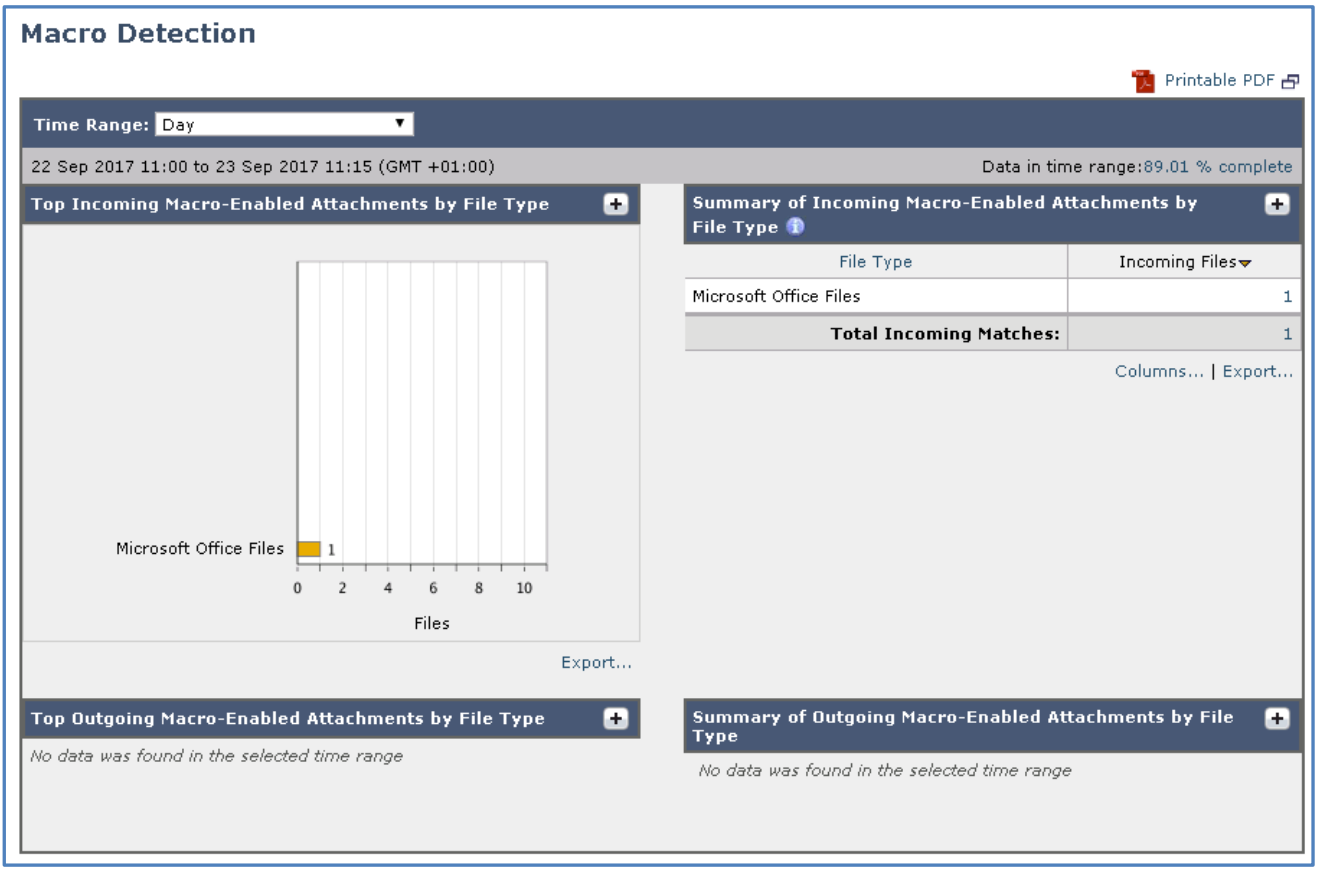
4. Open the message and confirm the attachment has been stripped.



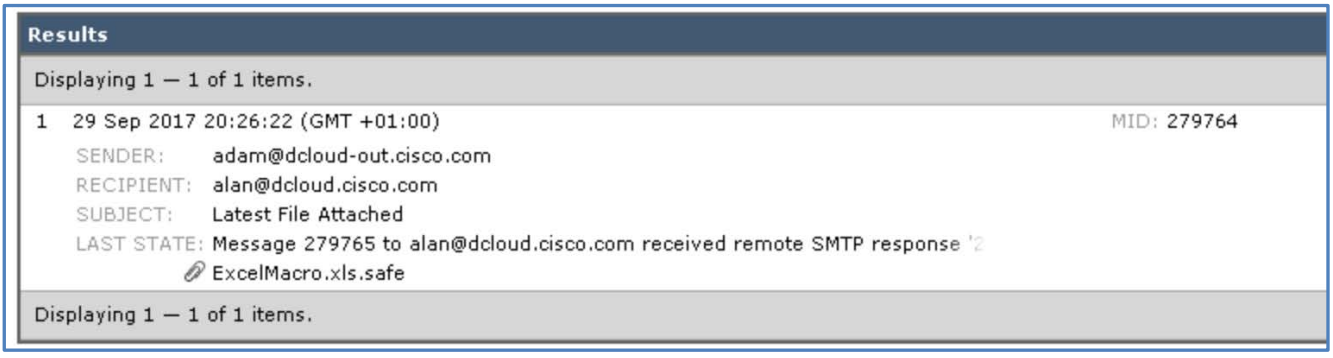
5. Navigate back to the CLI to observe the underlying mail processing and why the file was removed. Make a note of the MID.

```
Fri Sep 29 20:26:22 2017 Info: MID 279764 Subject 'Latest File Attached'
Fri Sep 29 20:26:22 2017 Info: MID 279764 ready 101506 bytes from <adam@dcloud-out.cisco.com>
Fri Sep 29 20:26:22 2017 Info: MID 279764 attachment 'ExcelMacro.xls.safe'
Fri Sep 29 20:26:22 2017 Info: MID 279764 matched all recipients for per-recipient policy DEFAULT in the inbound table
Fri Sep 29 20:26:22 2017 Info: MID 279764 interim verdict using engine: CASE spam negative
Fri Sep 29 20:26:22 2017 Info: MID 279764 using engine: CASE spam negative
Fri Sep 29 20:26:22 2017 Info: MID 279764 interim AV verdict using Sophos CLEAN
Fri Sep 29 20:26:22 2017 Info: MID 279764 antivirus negative
Fri Sep 29 20:26:23 2017 Info: MID 279764 AMP file reputation verdict : UNKNOWN(File analysis pending)
Fri Sep 29 20:26:23 2017 Info: MID 279764 SHA 30d9a3c2fe92d26c4dc85cdfe71b119bad15f9e78d778eee966c9346c1e4ab07 filename Excel
Macro.xls.safe queued for possible file analysis upload
Fri Sep 29 20:26:23 2017 Info: MID 279764 using engine: GRAYMAIL negative
Fri Sep 29 20:26:23 2017 Info: MID 279764 rewritten to MID 279765 by drop-macro-enabled-attachments filter 'Macro_Detection'
Fri Sep 29 20:26:23 2017 Info: Message finished MID 279764 done
Fri Sep 29 20:26:23 2017 Info: MID 279765 using engine: CASE using cached verdict
Fri Sep 29 20:26:23 2017 Info: CASE cache status: hits = 1, misses = 14, expires = 0, adds = 14, seconds saved = 0.69, total
seconds = 52.57
Fri Sep 29 20:26:23 2017 Info: MID 279765 Outbreak Filters: verdict negative
Fri Sep 29 20:26:23 2017 Info: MID 279765 queued for delivery
```

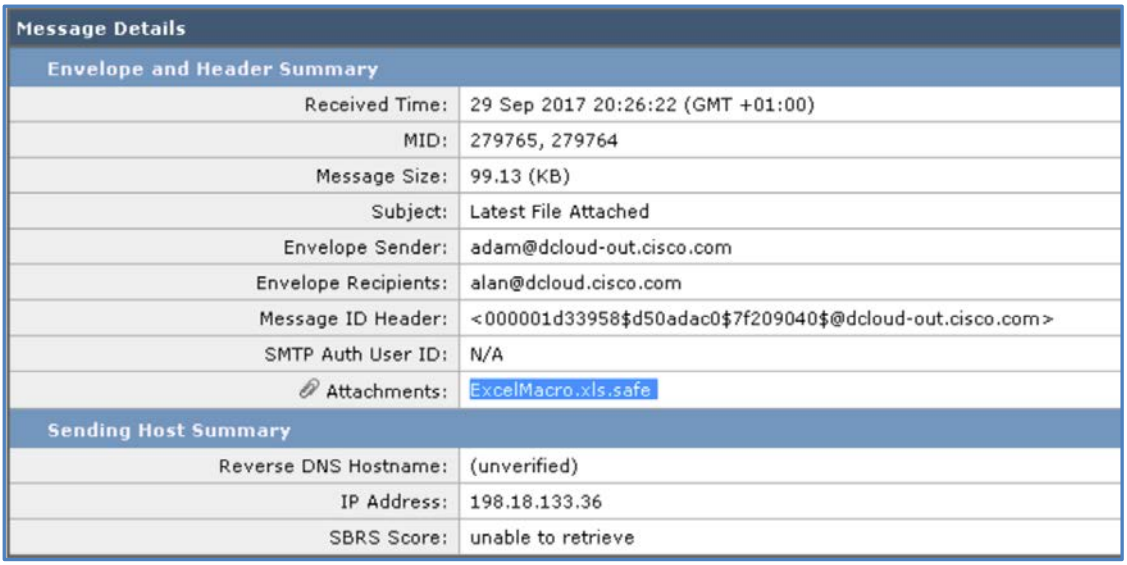
6. From the workstation access the GUI and navigate to **Monitor > Macro Detection** to view what is being reported.



7. Click on the value under *Incoming Files* to launch Message Tracking. It may take a few moments for the tracking information to be updated.



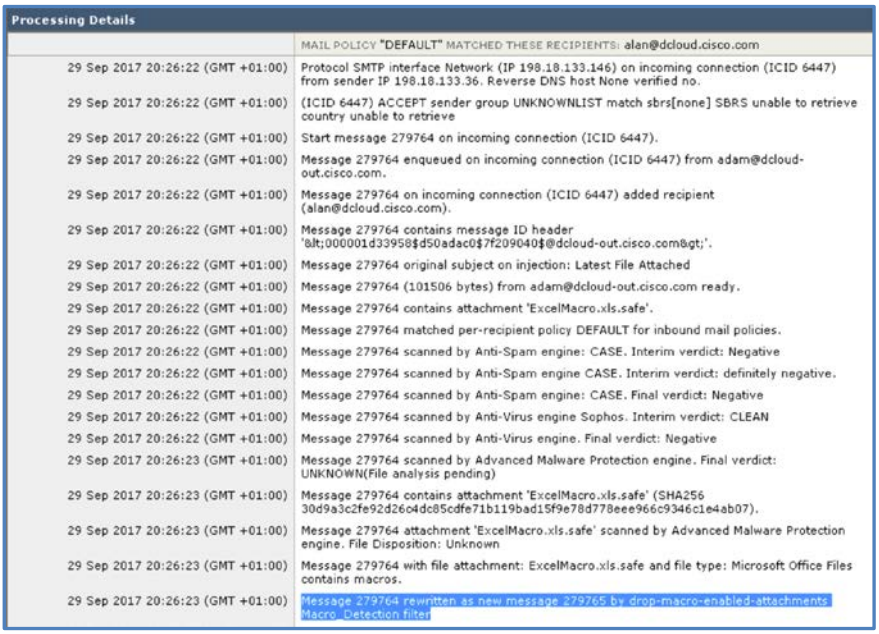
8. Click on **Show Details** to view how the engine has processed the message and what action it has applied to the attachments as a result of the policy matching.



Message Details

Envelope and Header Summary	
Received Time:	29 Sep 2017 20:26:22 (GMT +01:00)
MID:	279765, 279764
Message Size:	99.13 (KB)
Subject:	Latest File Attached
Envelope Sender:	adam@dcloud-out.cisco.com
Envelope Recipients:	alan@dcloud.cisco.com
Message ID Header:	<000001d33958$d50adac0$7f209040$@dcloud-out.cisco.com>
SMTP Auth User ID:	N/A
Attachments:	ExcelMacro.xls.safe
Sending Host Summary	
Reverse DNS Hostname:	(unverified)
IP Address:	198.18.133.36
SBRS Score:	unable to retrieve

9. The processing section provides a detailed timeline of how the message passes through the Cisco Email Security solution and the various actions that are applied by the engines that are enabled.
10. This is the same information that was seen in the CLI session, however here it is non-scrolling and available after the CLI session is closed.



Processing Details

	MAIL POLICY "DEFAULT" MATCHED THESE RECIPIENTS: alan@dcloud.cisco.com
29 Sep 2017 20:26:22 (GMT +01:00)	Protocol SMTP interface Network (IP 198.18.133.146) on incoming connection (ICID 6447) from sender IP 198.18.133.36. Reverse DNS host None verified no.
29 Sep 2017 20:26:22 (GMT +01:00)	(ICID 6447) ACCEPT sender group UNKNOWNLIST match sbrs[none] SBRS unable to retrieve country unable to retrieve
29 Sep 2017 20:26:22 (GMT +01:00)	Start message 279764 on incoming connection (ICID 6447).
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 enqueued on incoming connection (ICID 6447) from adam@dcloud-out.cisco.com.
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 on incoming connection (ICID 6447) added recipient (alan@dcloud.cisco.com).
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 contains message ID header '<000001d33958$d50adac0$7f209040$@dcloud-out.cisco.com>'.
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 original subject on injection: Latest File Attached
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 (101506 bytes) from adam@dcloud-out.cisco.com ready.
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 contains attachment 'ExcelMacro.xls.safe'.
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 matched per-recipient policy DEFAULT for inbound mail policies.
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 scanned by Anti-Spam engine CASE. Interim verdict: definitely negative.
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 scanned by Anti-Spam engine: CASE. Final verdict: Negative
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 scanned by Anti-Virus engine Sophos. Interim verdict: CLEAN
29 Sep 2017 20:26:22 (GMT +01:00)	Message 279764 scanned by Anti-Virus engine. Final verdict: Negative
29 Sep 2017 20:26:23 (GMT +01:00)	Message 279764 scanned by Advanced Malware Protection engine. Final verdict: UNKNOWN(File analysis pending)
29 Sep 2017 20:26:23 (GMT +01:00)	Message 279764 contains attachment 'ExcelMacro.xls.safe' (SHA256 30d9a3c2fe92d26e4dc85cdfe71b119bad15f9e78d778eee966c9346c1e4ab07).
29 Sep 2017 20:26:23 (GMT +01:00)	Message 279764 attachment 'ExcelMacro.xls.safe' scanned by Advanced Malware Protection engine. File Disposition: Unknown
29 Sep 2017 20:26:23 (GMT +01:00)	Message 279764 with file attachment: ExcelMacro.xls.safe and file type: Microsoft Office Files contains macros.
29 Sep 2017 20:26:23 (GMT +01:00)	Message 279764 rewritten as new message 279765 by drop-macro-enabled-attachments Macro_Detection filter

11. Close the detailed Message Tracking window to return to the main Message Tracking screen.

Scenario 6. Geolocation Based Filtering

Use Case

Voyage Corp expanded its operations into Western Europe in 2015 driven primarily by the expansion of its key customers who have a significant presence in the United Kingdom, Italy, France and Spain and some minor territories. Business was strong, reporting 10% growth year on year and it seemed that would increase dramatically however the decision for the United Kingdom leaving the European Union (EU) had an impact on most of its top 10 customers, who bound by legislation had to abandon trade with the UK once it had severed its political ties with the EU.

Security Control

The Cisco Email Security can handle incoming mail connections or messages from specific geolocations and perform appropriate actions on them, for example:

- Prevent email threats coming from specific geographic regions.
- Allow or disallow emails coming from specific geographic regions

This feature can be used in the following ways:

- SMTP Connection Level using Sender Groups
- Content Filter Level

Objective

This scenario walks through the configuration of Geolocation based filtering using Content Filters and the Host Access Table to handle incoming or outgoing messages from particular countries that have been selected.

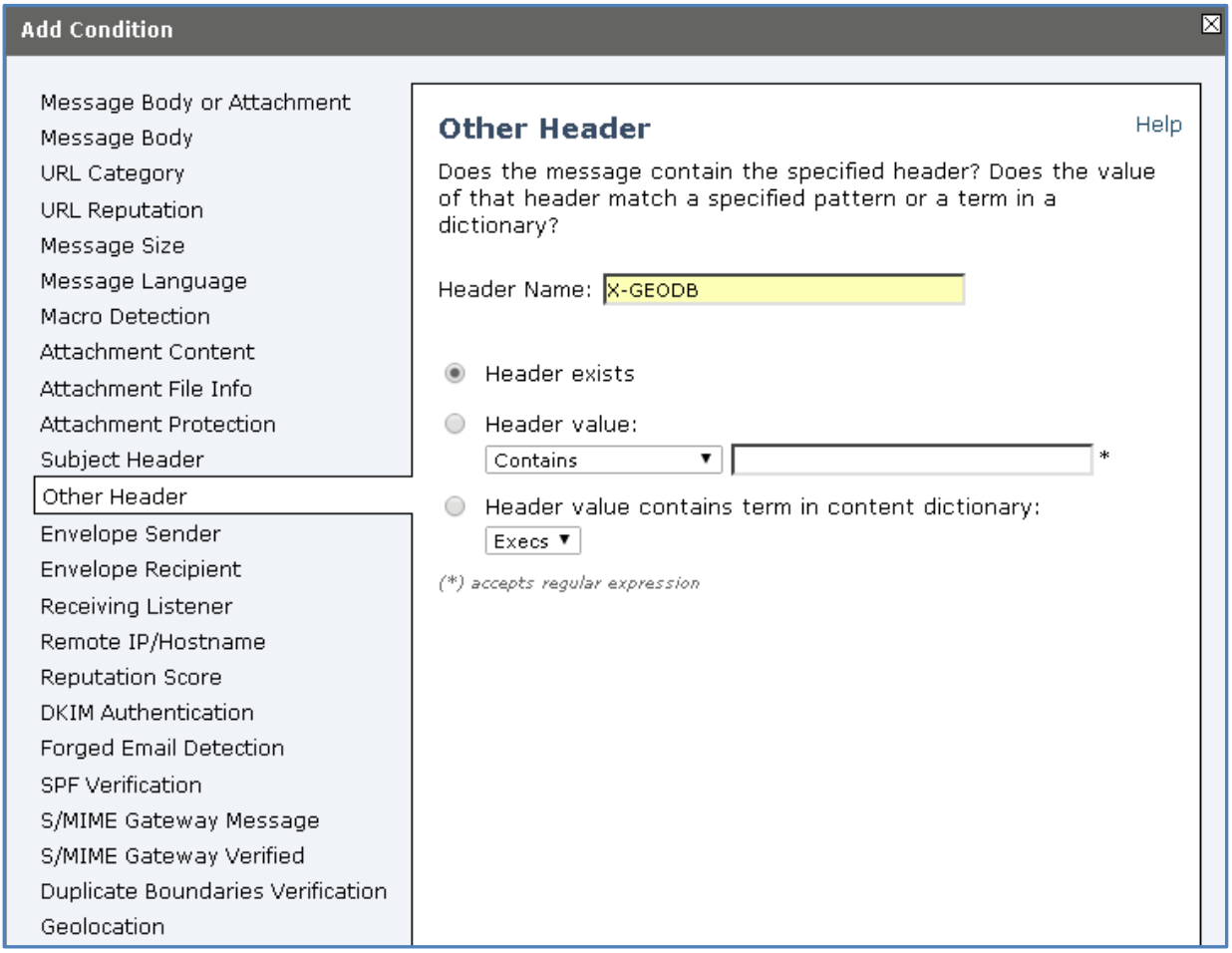
Steps

Task - Configuring a Content Filter (Estimated time to complete: 3 min)

Similar to previous scenarios, content filters help granularity in policies to identify content. In this task, a new content filter will be created to identify to which countries control should be prohibited.

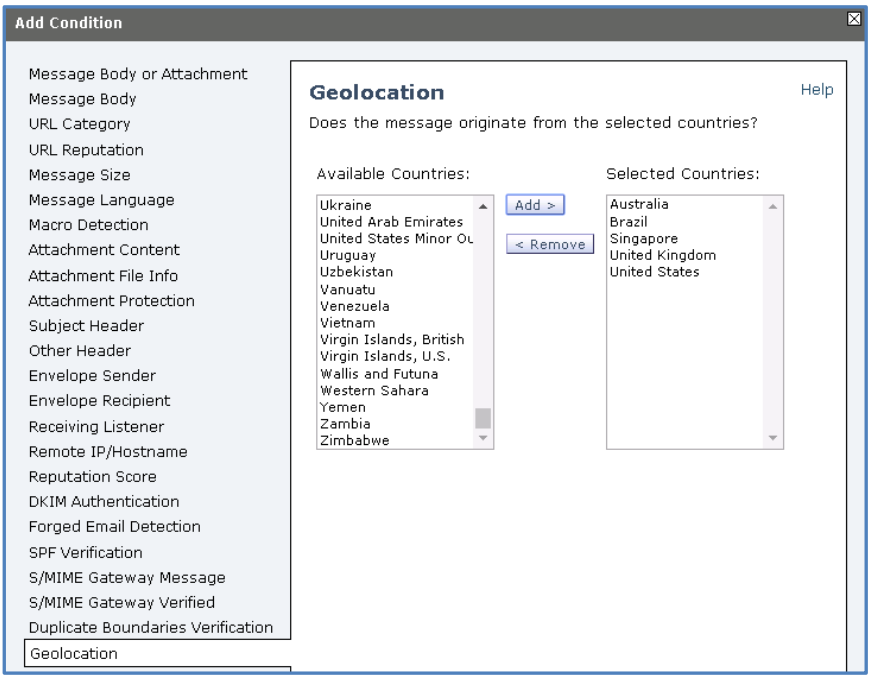
1. From the workstation access the GUI and navigate to **Mail Policy > Incoming Content Filters** and click **Add Filter**.

2. Using the following settings configure the Conditions and Actions.
   - Name: Block_GeoDB
   - Description: Location based Filtering
   - Condition 1: Other Header>Header Name: X-GEODB
   - Condition 2: Geolocation>Australia, Brazil, Singapore, United Kingdom, United States
   - Action 1: Drop (Final Action)



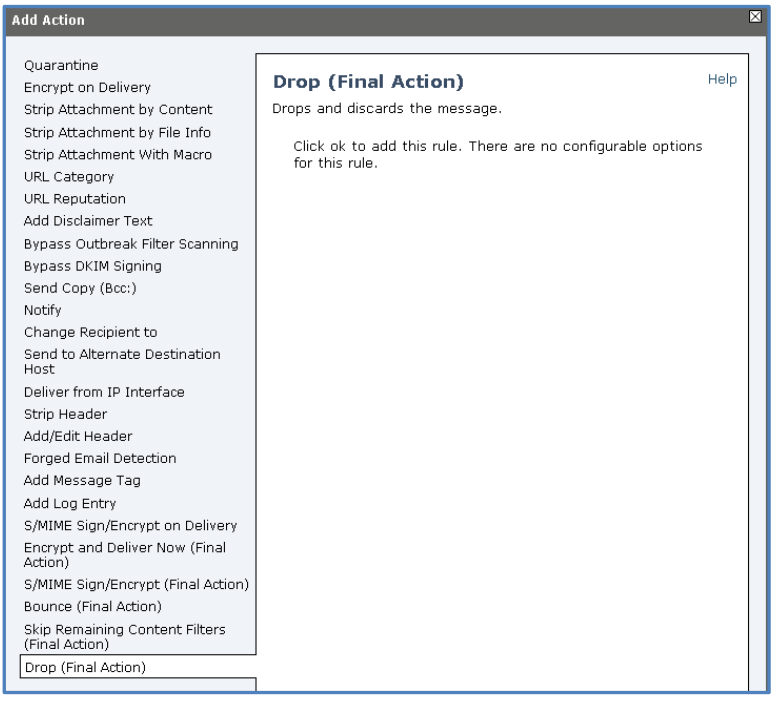
3. Click **OK**

4. Click Add Condition.

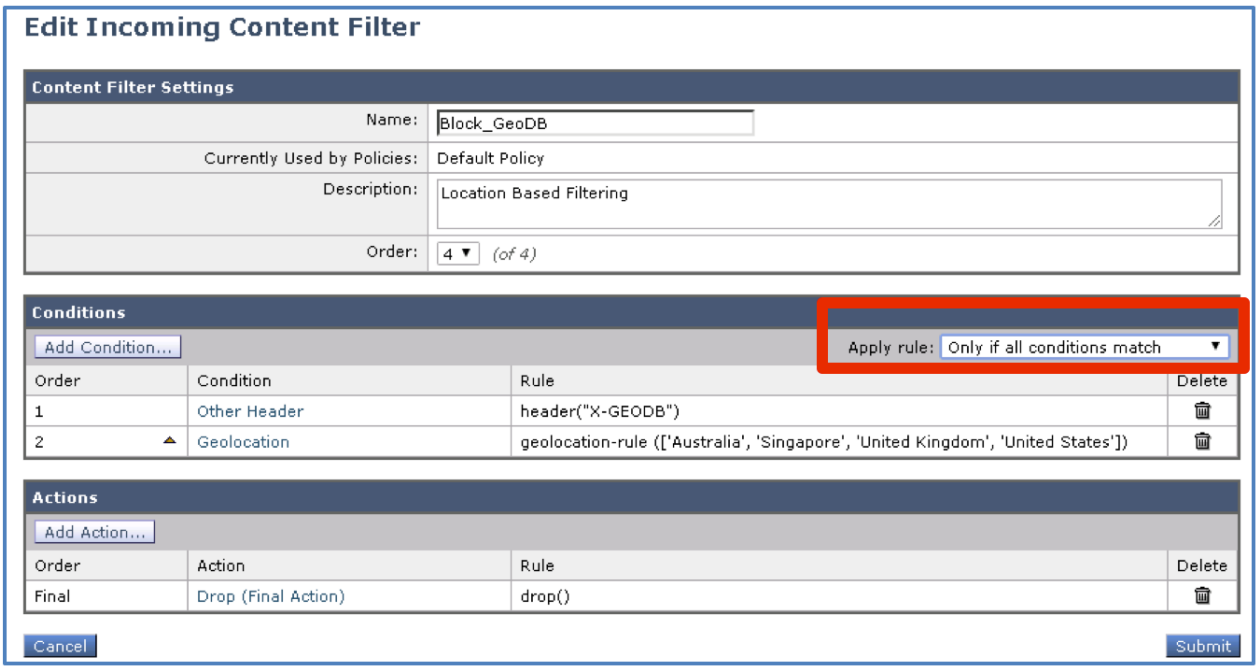


5. Click **OK**.

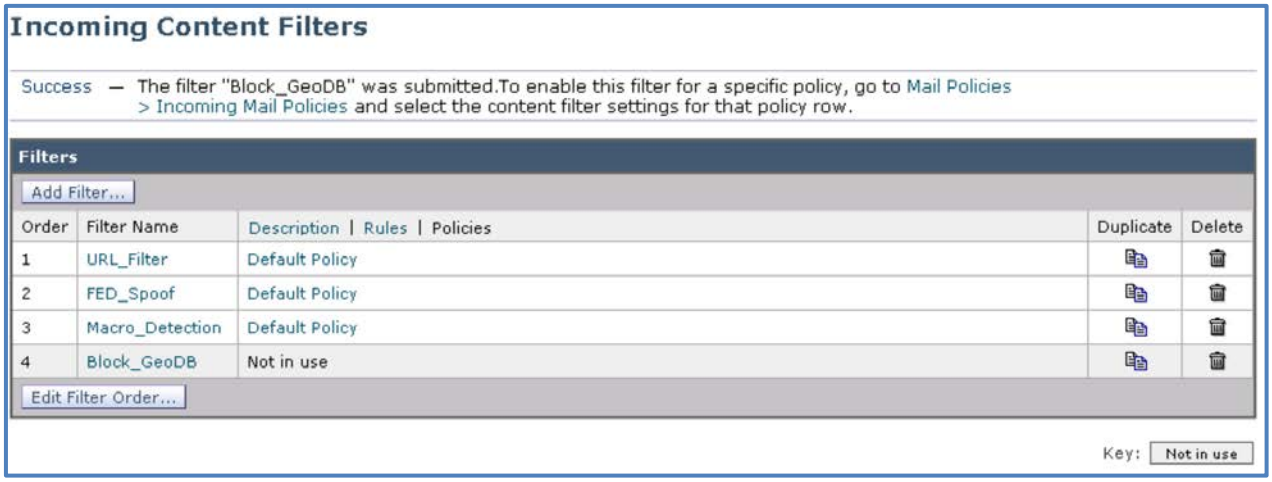
6. Click **Add Action.**



7. Finally, change how the conditions work by selecting Only if all conditions match from the *Apply Rule* drop down box.



8. Click **Submit** to create the content Filter.

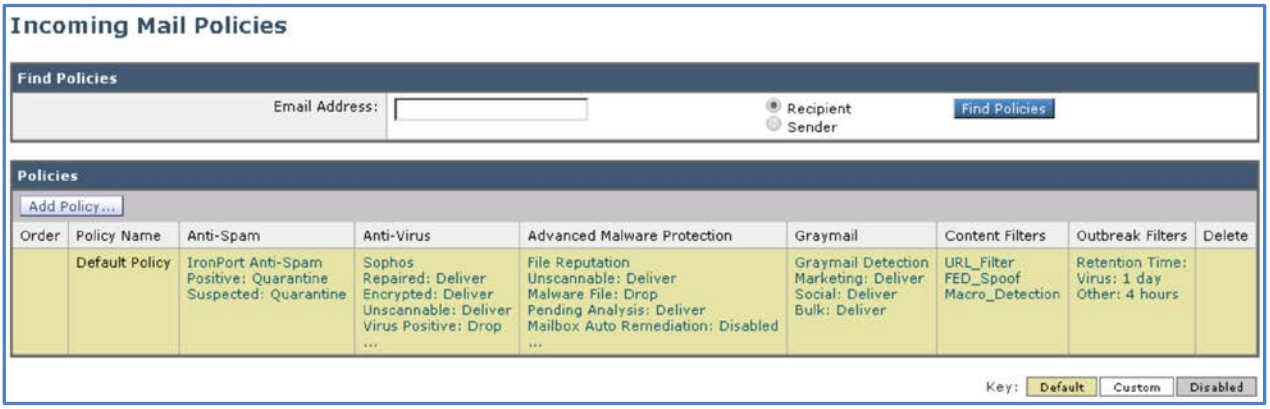


9. Once complete, ensure the changes are applied by clicking the **Commit Changes** button, adding optional comments if desired.

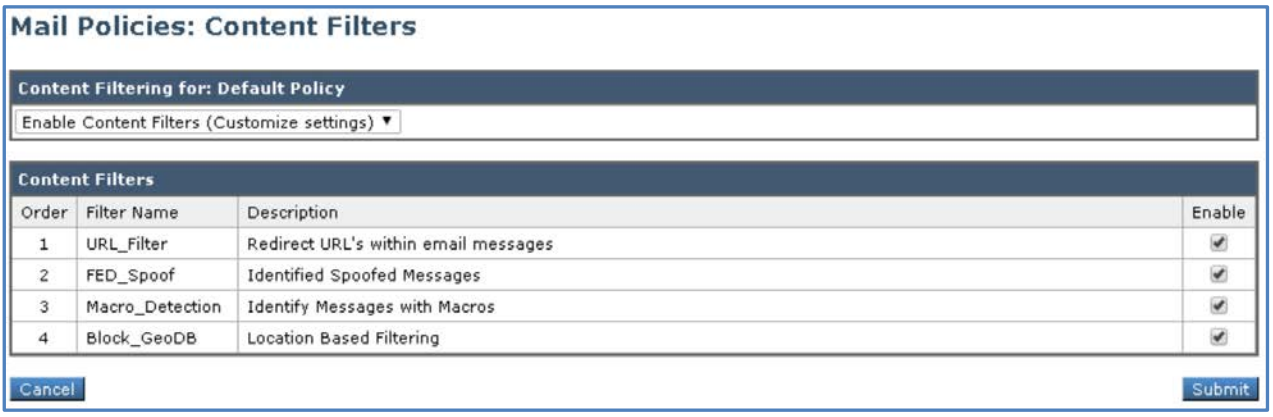
Task - Edit Incoming Mail Policy (Estimated time to complete: 1 min)

The final task is to modify the default incoming mail policy so the content filter comes into effect.

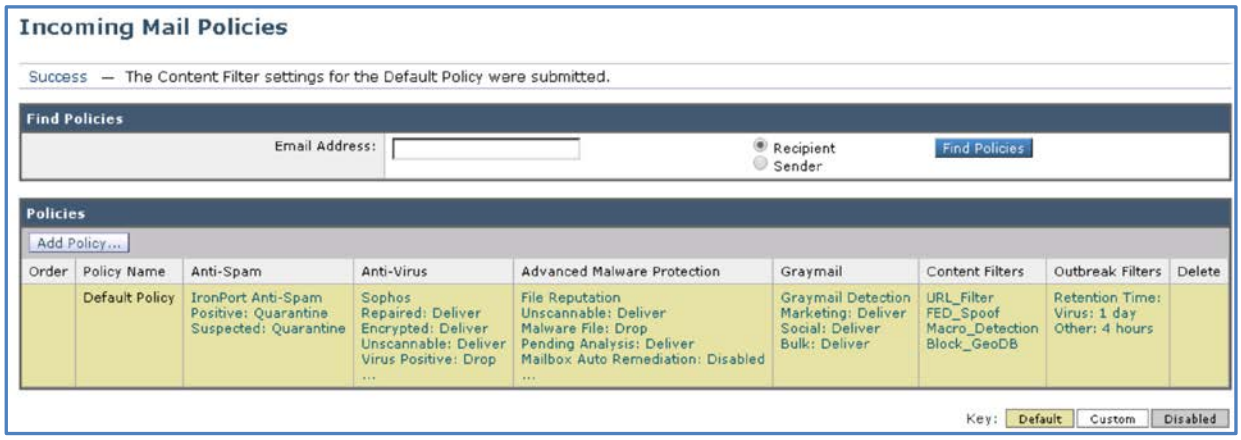
1. From the workstation access the GUI and navigate to **Mail Policy > Incoming Mail Policies** and click within the Content Filters box of the Default Policy.



2. Place a checkmark against the content filter Block_GeoDB created in the previous step to enable it.



3. Click **Submit** to create the content Filter and verify the policy.



4. Once complete, ensure the change is applied by clicking the **Commit Changes** button, adding optional comments if desired.

Task - Testing Geolocation (Estimated time to complete: 5 min)

With the entire configuration in place the Geo-location feature can be tested by sending an email to Alan from external user simulating a country that was previously specified.

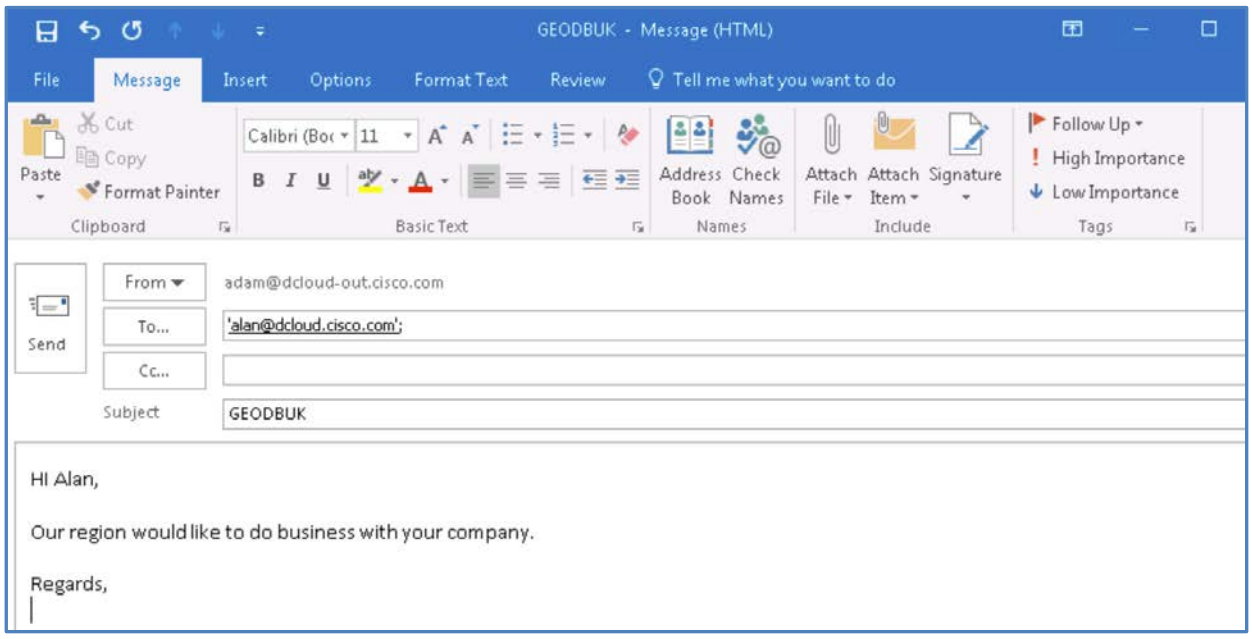
Initiate a CLI session

Prior to preparing the message, initiate a connection to the Cisco Email Security solution from the CLI in order to view, using the tail command, the mail logs to see the message being processed and the actions being applied as it works its way through the pipeline, repeat the same steps to initiate this from the previous scenario.

1. From the workstation launch Microsoft Outlook and from Adams inbox, prepare a new message with the following parameters.
   - To: alan@dcloud.cisco.com
   - Subject: GEODBUK
   - Body: Hi Alan,

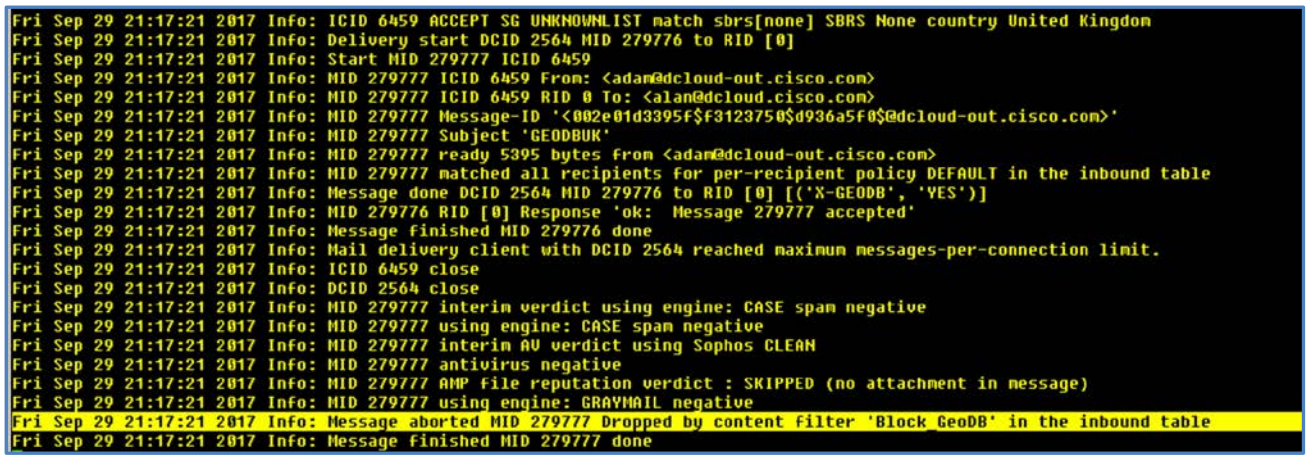
     Our region would like to do business with your company.

     Regards,

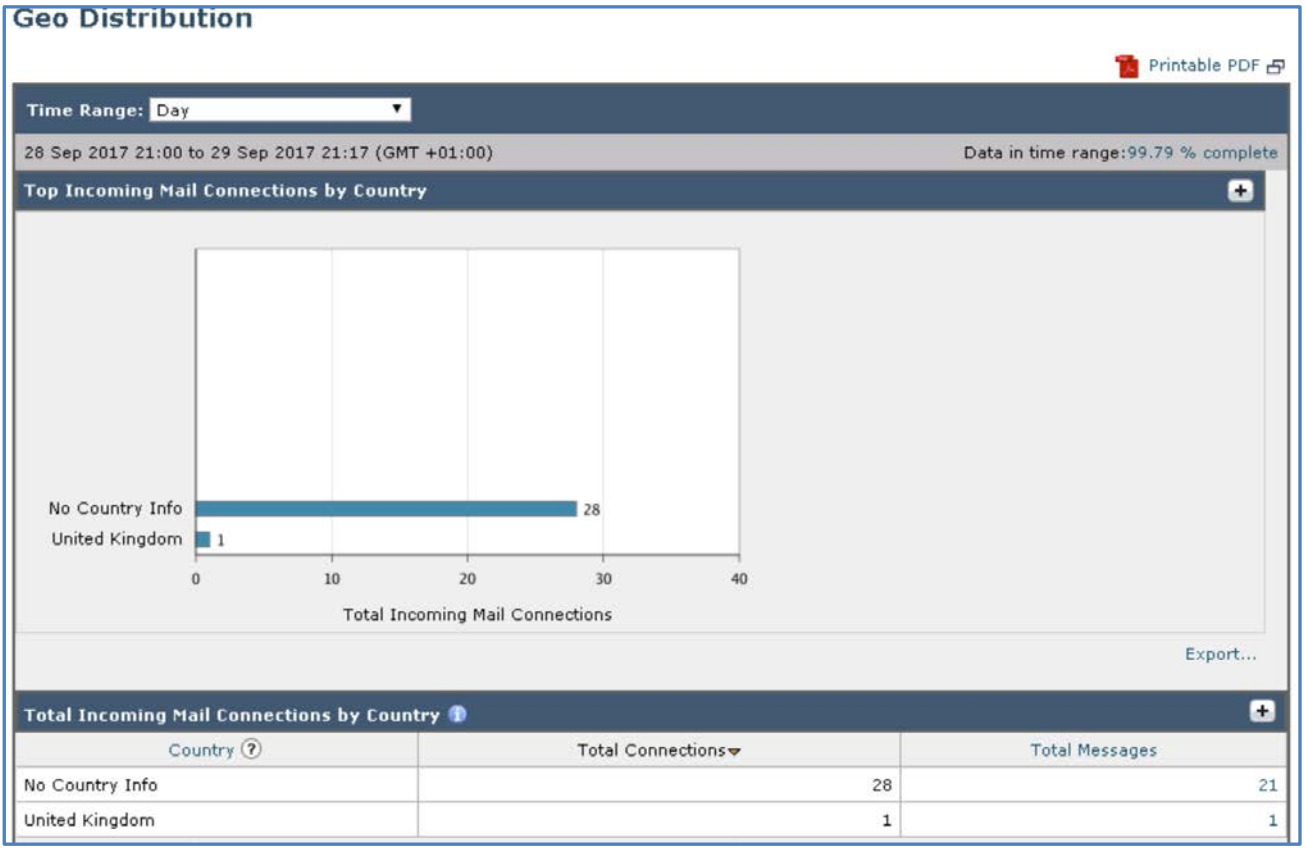


2. Send the email - Force the synchronization process by clicking **Send/Receive Folder** or by pressing the **F9** key

3. Switch back to the CLI and notice how the content filter handled the message.



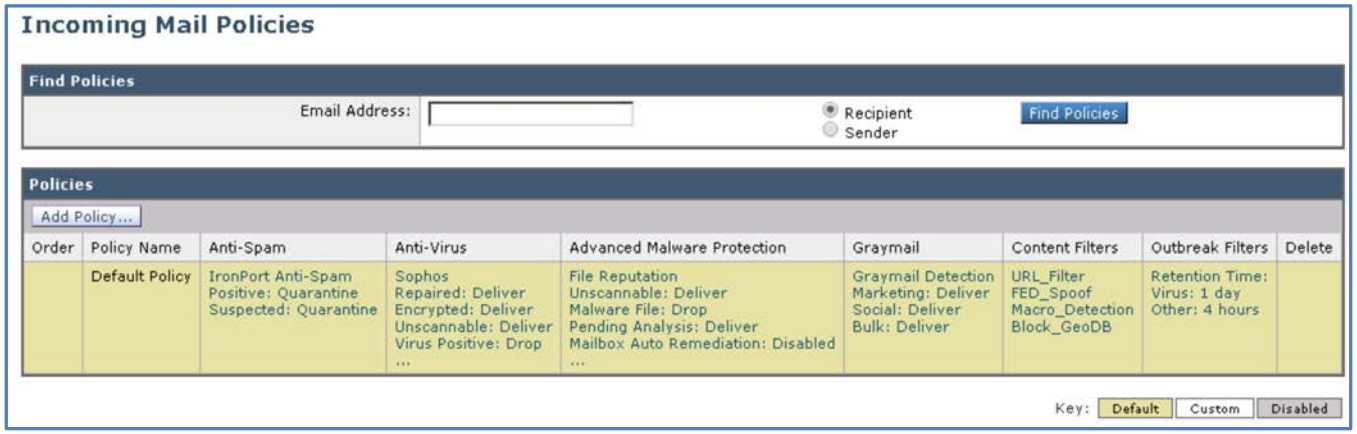
4. From the workstation access the GUI and navigate to **Monitor > Geo Distribution** to view what is being reported.



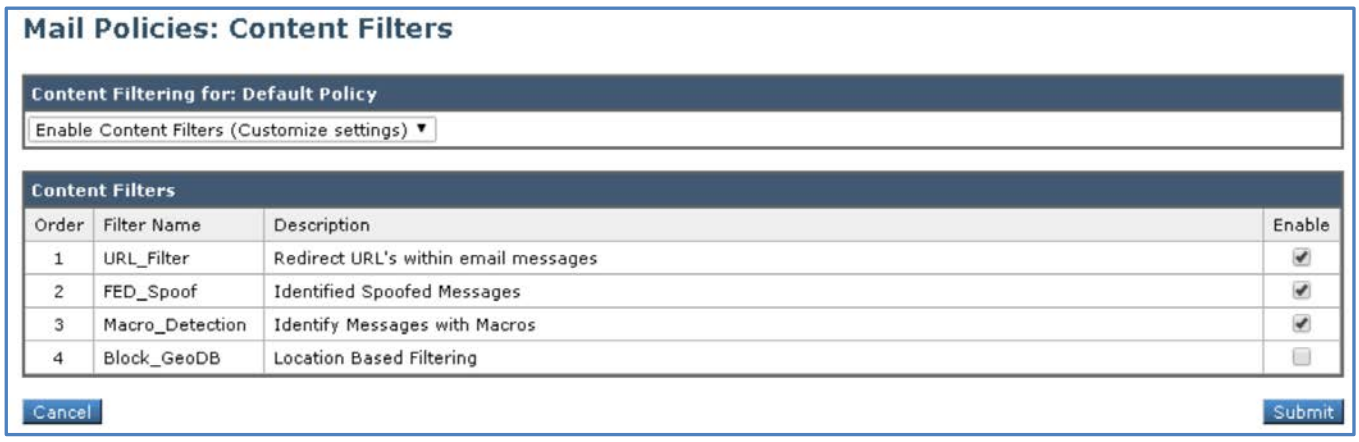
Task - Geolocation based filters at the Connection Level (Estimated time to complete: 5 min)

Geolocation based filtering can also be done at the connection level applied in the Host Access Table (HAT). The HAT maintains a set of rules that control incoming connections from remote hosts for a listener. Every configured listener has its own HAT and typically there is a public and private listener. As the names suggest Public is an external facing listener and Private internal.

1. First, remove the content filter from the default mail policy that was added in the previous task. Technically this is not required as content filters are processed later on in the email pipeline, however it will remove it to be consistent with good practice.
2. From the workstation access the GUI and navigate to **Mail Policy > Incoming Mail Policies** and click within the Content Filters box of the Default Policy.

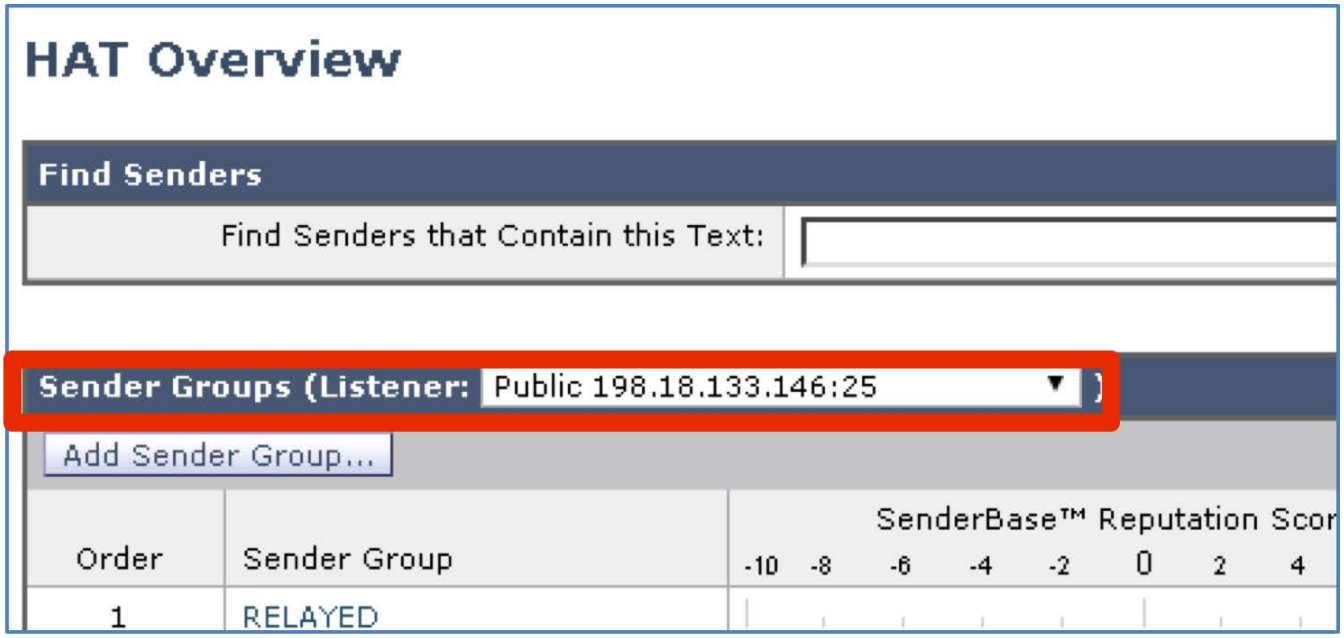


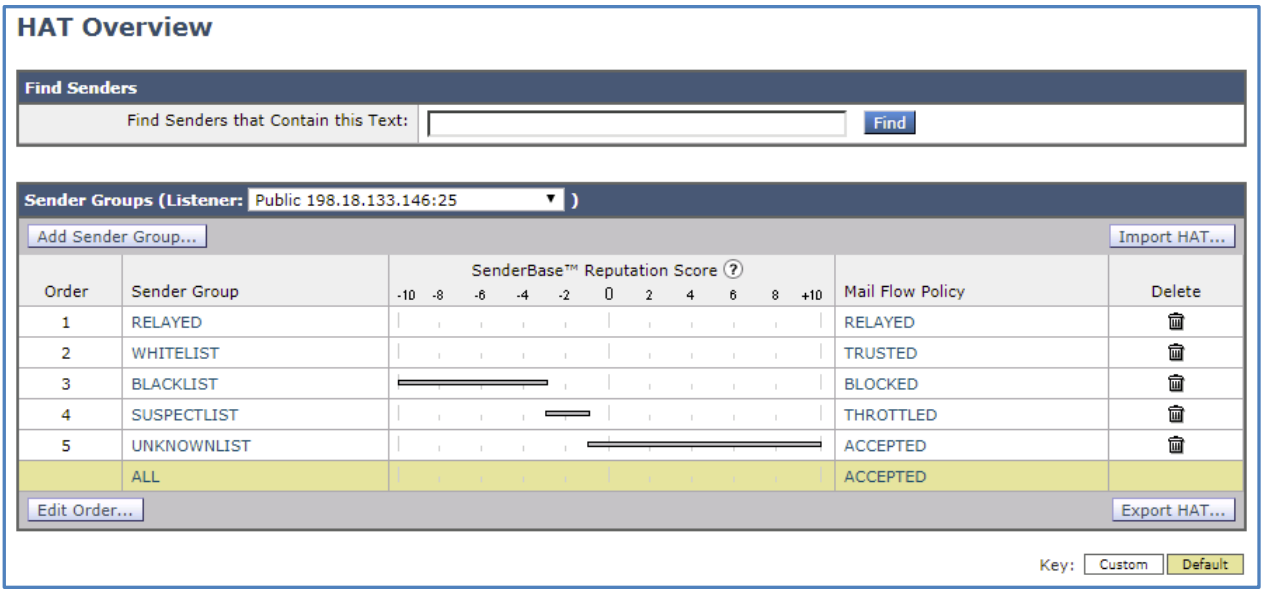
3. Remove the checkmark against the content filter Block_GeoDB created in the previous step to disable it.



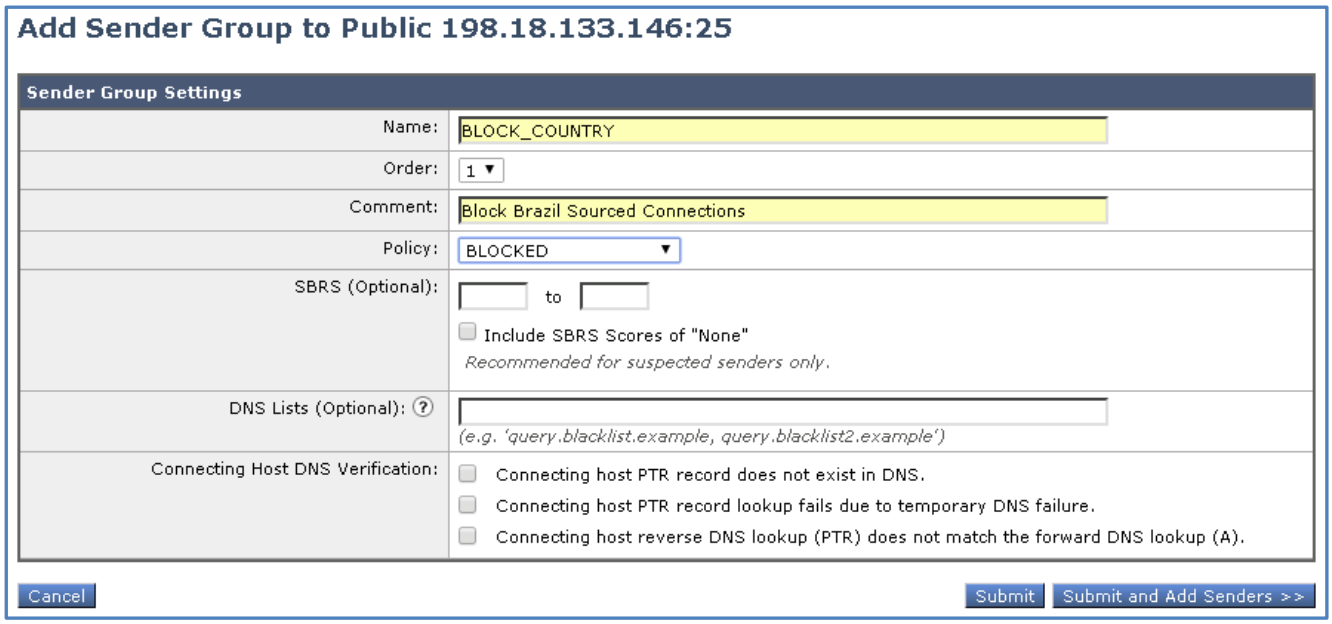
4. Click **Submit** to apply the actions. Once complete, ensure change is applied by clicking the **Commit Changes** button, adding optional comments if desired.
5. Navigate to **Mail Policy > HAT Overview** and from the resulting screen click **Add Sender Group**

6. Ensure the *Sender Groups (Listener) Public* is selected from the list of listeners.

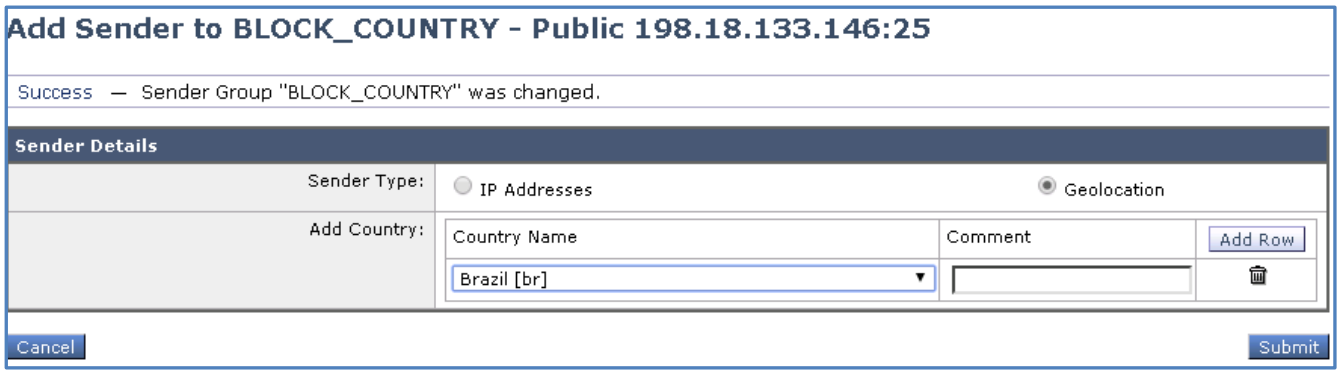




7. Create a new sender group using the following settings, where not specified please use the default setting: -
   - Name: BLOCK_COUNTRY
   - Order: 1
   - Comment: Block Brazil Sourced Connections
   - Mail Flow Policy: BLOCKED

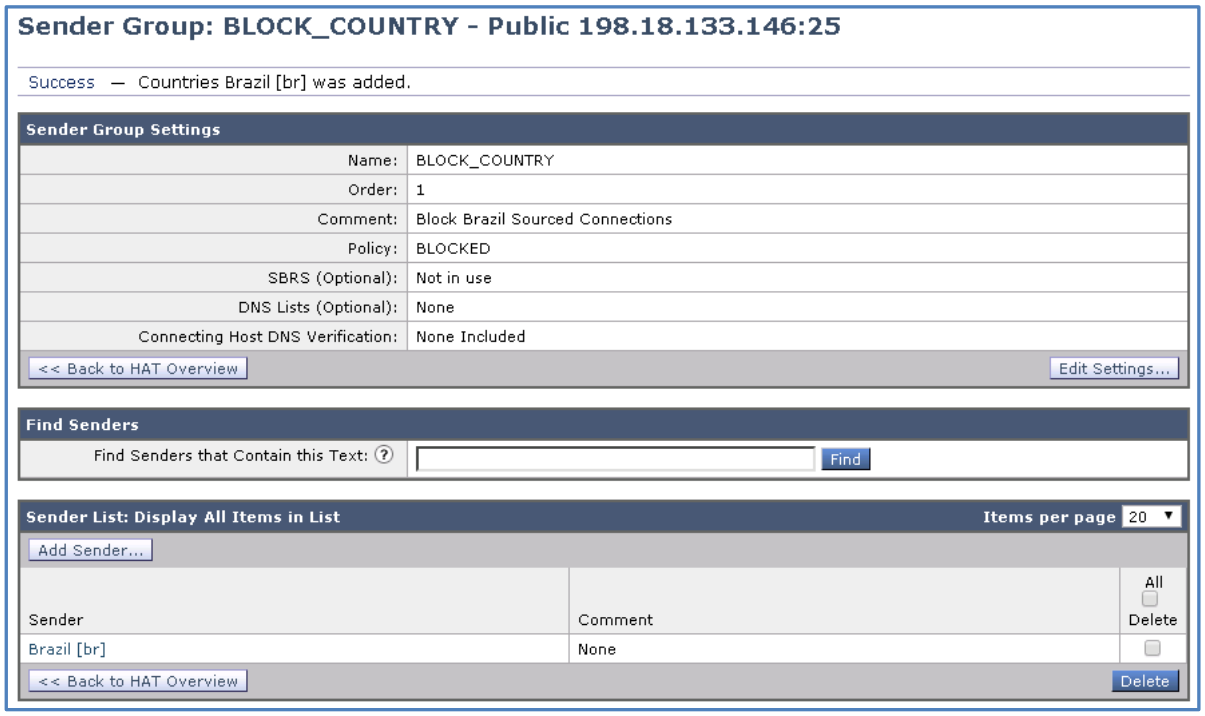


8. Click the **Submit** and **Add Senders** button.
9. From the resulting screen select the Geolocation radio button, this will then allow the countries to be selected from a preconfigured list: -



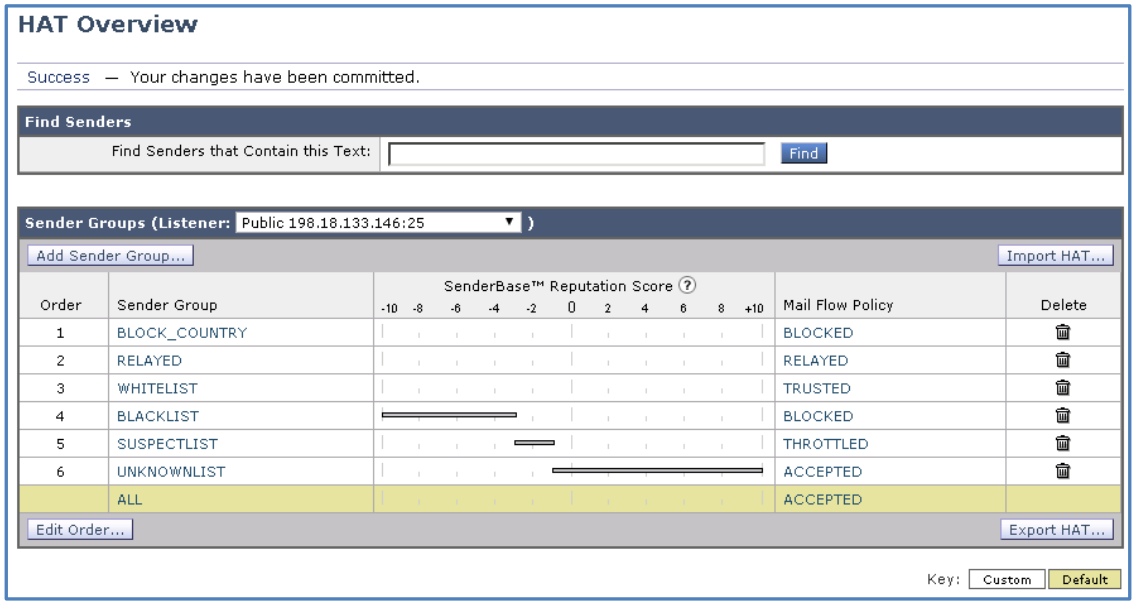
NOTE: If the Geolocation radio button is not present, revisit and confirm the Public interface was selected from the *Sender Groups.*

10. Using the dropdown, select Brazil add comments if desired and click the **Submit** button.



11. Verify Brazil has been added successfully and ensure changes are applied by clicking the **Commit Changes** button, adding optional comments if desired.

12. Verify the *Sender Group* created in the previous step is listed in the HAT Overview at the top of the order: -



Task - Testing Geolocation based filtering (Estimated time to complete: 5 min)

With the entire configuration in place, the Geolocation feature can be tested by sending an email to Alan from an external user simulating a country that connections from should be restricted.

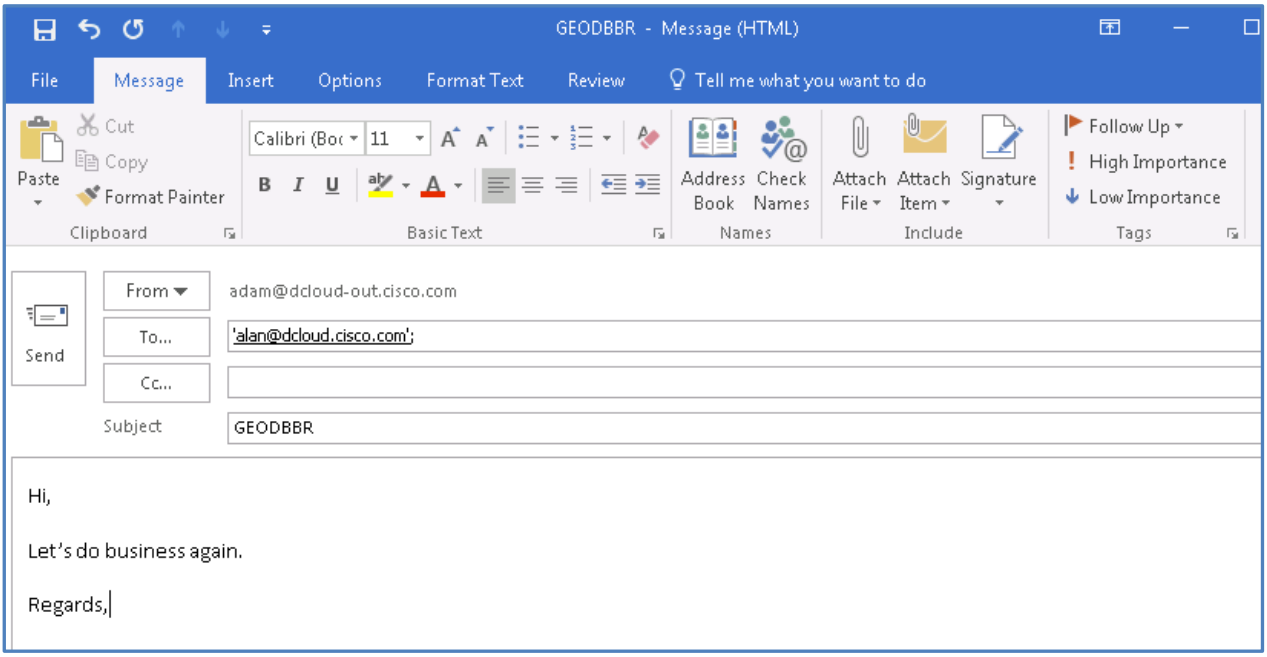
Initiate a CLI session

Prior to preparing the message, initiate a connection to the Cisco Email Security solution from the CLI in order to view, using the tail command, the mail logs to see the message being processed and the actions being applied as it works its way through the pipeline, repeat the same steps to initiate this from the previous scenario.

1. Navigate to **Monitor > Geo Distribution** to verify that no connections from Brazil have been logged. Since no connection of any kinds from this location has been previously attempted or simulated no statistics for that country should be listed.
2. From the workstation launch Microsoft Outlook and from Adams inbox, prepare a new message with the following parameters.
   - To: alan@dcloud.cisco.com
   - Subject: GEODBBR
   - Body: Hi Alan,

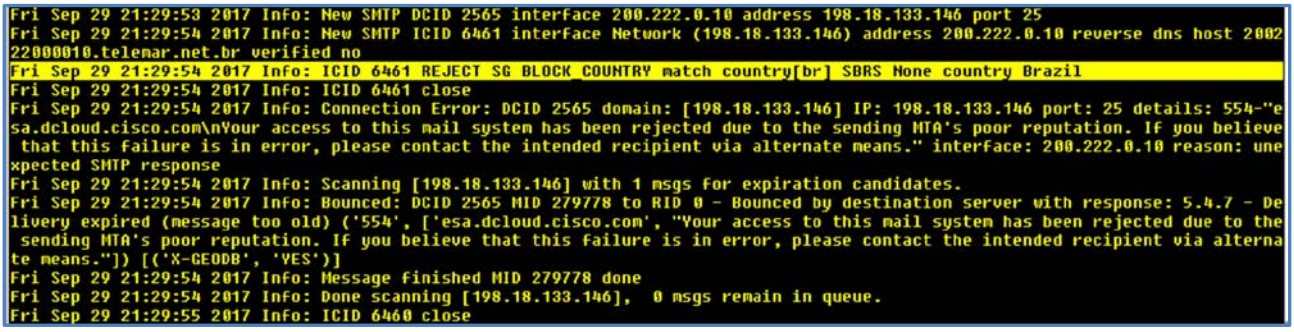
     Our region would like to do business with your company.

     Regards,

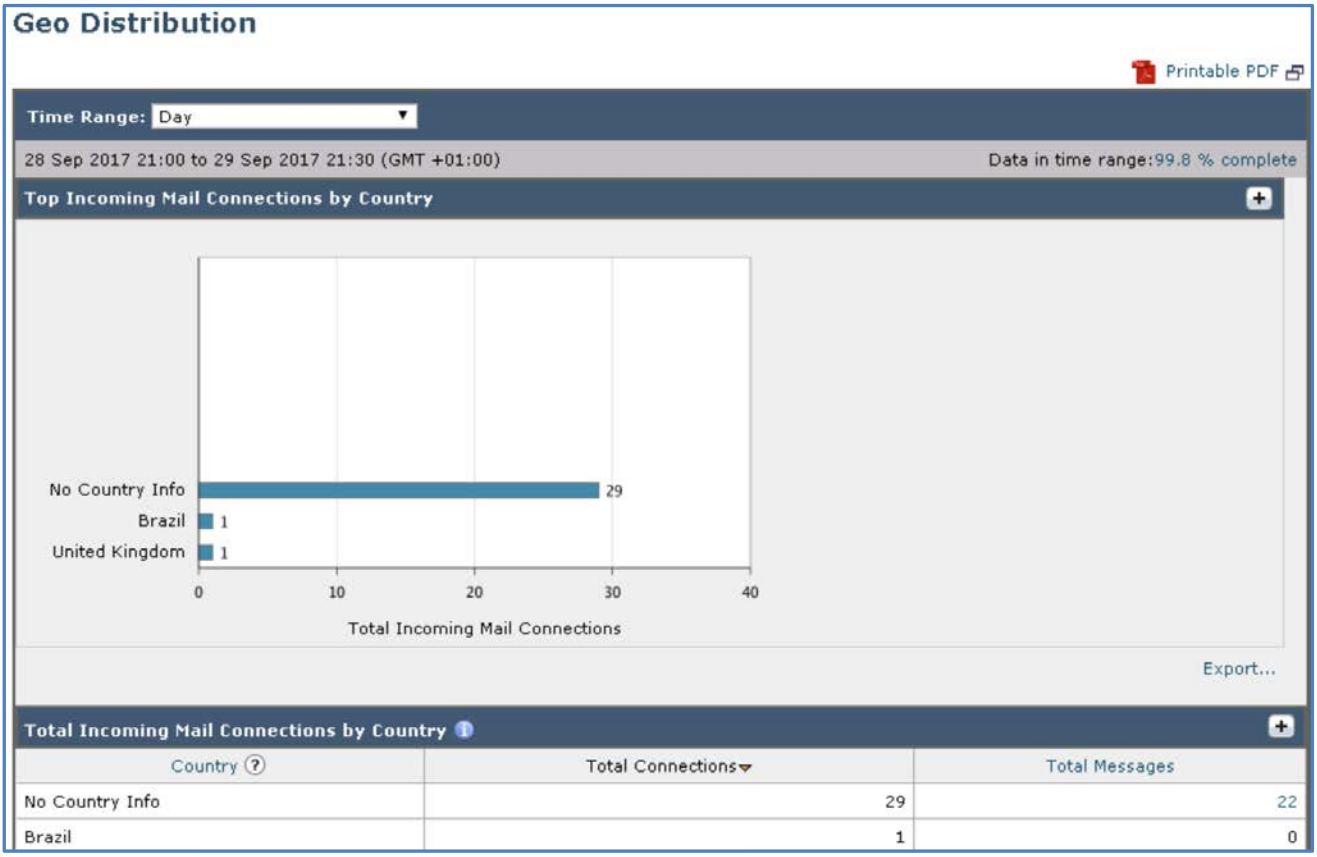


3. Send the email - Force the synchronization process by clicking **Send/Receive Folder** or by pressing the **F9** key.

4. Switch back to the CLI session, scroll through the logs and look for the log entry that advises that the country was matched and the connection was subsequently rejected. At this point processing stops and the Anti-Spam and Anti-Virus engines are not required to do any processing on this message thus saving valuable compute resources.



5. Finally, navigate the **Monitor > Geo Distribution**, refresh the screen if required, and notice the country information being populated now. Brazil will be listed in the Total Connections column and note that the Total Messages column as a 0 value, this is because the Geolocation feature is blocking at the connection level so the message is never processed beyond this.



Scenario 7. Advanced Malware Protection

Use Case

A third-party finance company recently launched a campaign offering competitive rates of credit to business within the state that wish to invest in next generation date centre equipment. The campaign was sent to all eco-partners that had a high gross spend in the previous 12 months; Voyage Corp came under this classification. A marketing assistance received one of campaigns emails, however, unbeknownst, it contained malicious payload that rendered her computer temporarily inactive. The installed Anti-Vitus solution was sufficiently configured and signature updates were set as per the recommendation of the developers of the software, however the threat manage to evade this traditional but hardy layer of defence.

Security Control

Most Anti-Virus vendors only perform signature-based detection, so any malicious file that yet known to Anti-Virus vendor can be easily bypassed by bad actors. To ensure effective security against sophisticated or even targeted attacks, AMP for Email should be considered to act as an additional layer of defence by combining point in-time detection with continuous analysis with retrospection. Modern research suggests, the overall catch rate of malware from email traffic can be improved by 50% after enabling AMP file reputation scanning on Cisco Email Security

Objective

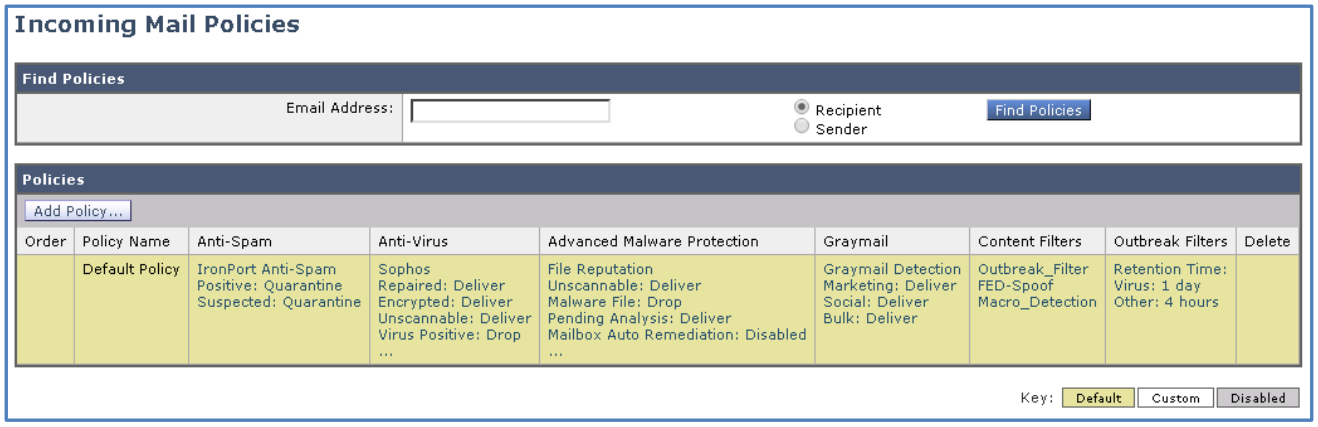
This scenario will demonstrate the File Reputation and File Analysis features of AMP by checking the reputation of a file and then sending it for File Analysis to the Cisco AMP cloud to deliver a verdict, whilst the file has been sent for a disposition the email message to the recipient will be held in quarantine.

Steps

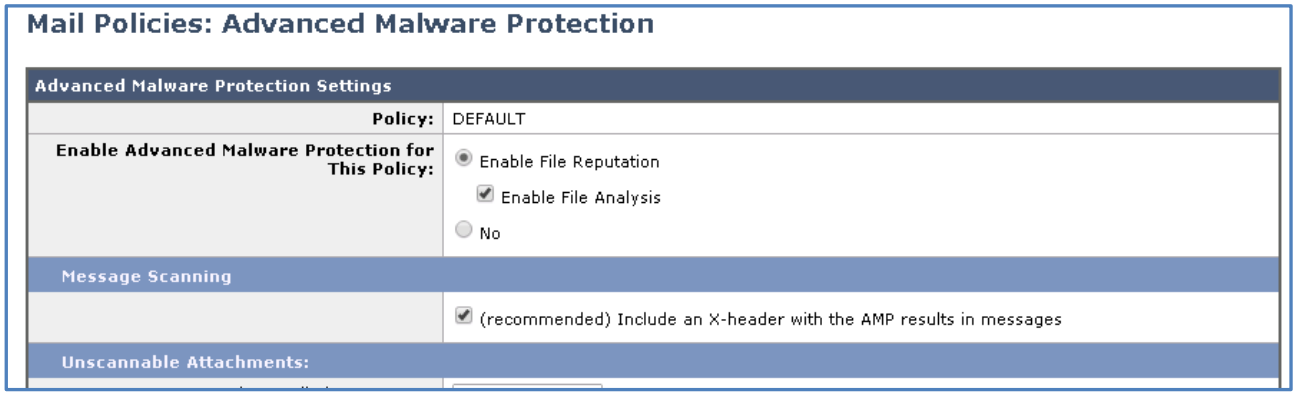
Task - Edit the AMP Policy (Estimated time to complete: 1 min)

1. Firstly, edit default policy to modify the action that will be applied to messages which have files that have been sent for analysis to the Cisco AMP cloud.

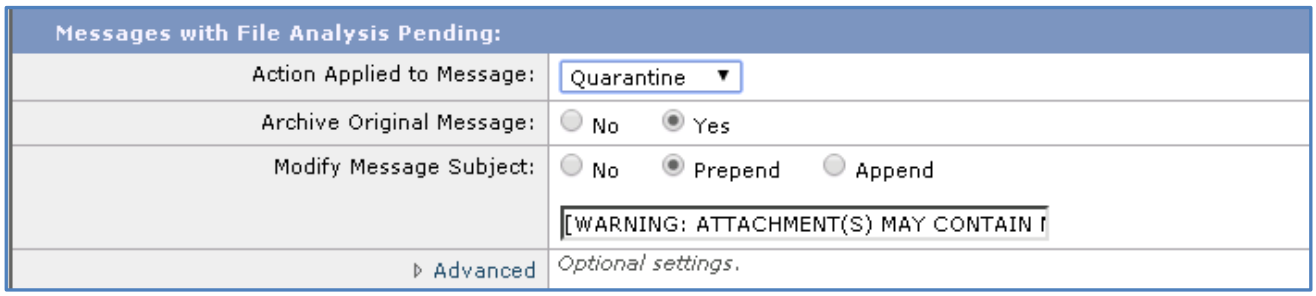
2. From the workstation access the GUI and navigate to **Mail Policy > Incoming Mail Policies** and click within the Advanced Malware Protection section of the Default Policy.



3. Verify that **File Analysis** is enabled; this allows any qualifying file that has an unknown disposition to be redirected to the Cisco ThreatGrid sandbox for expert analysis and a verdict.



4. Scroll down towards the **Message with File Analysis Pending** section and modify the *Action Applied to Message* to Quarantine.

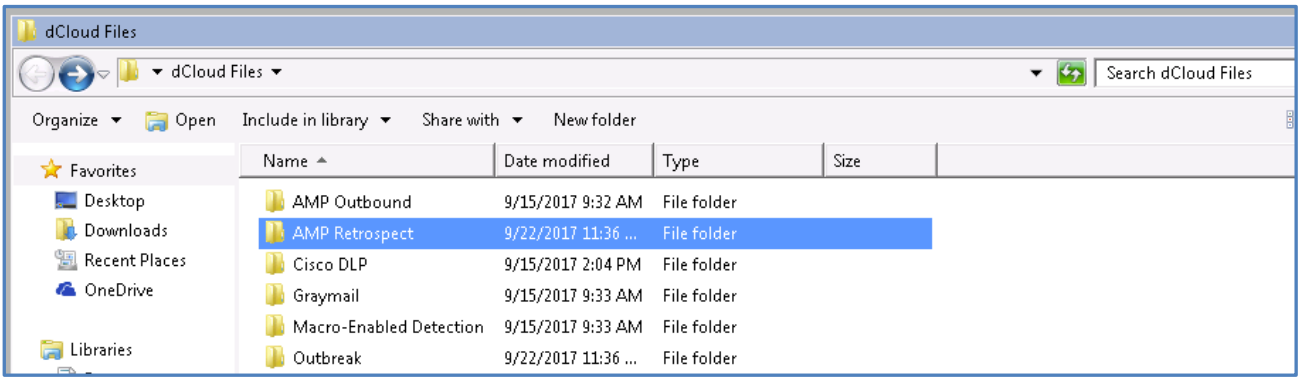


5. Click **Submit** to apply the actions and commit changes.

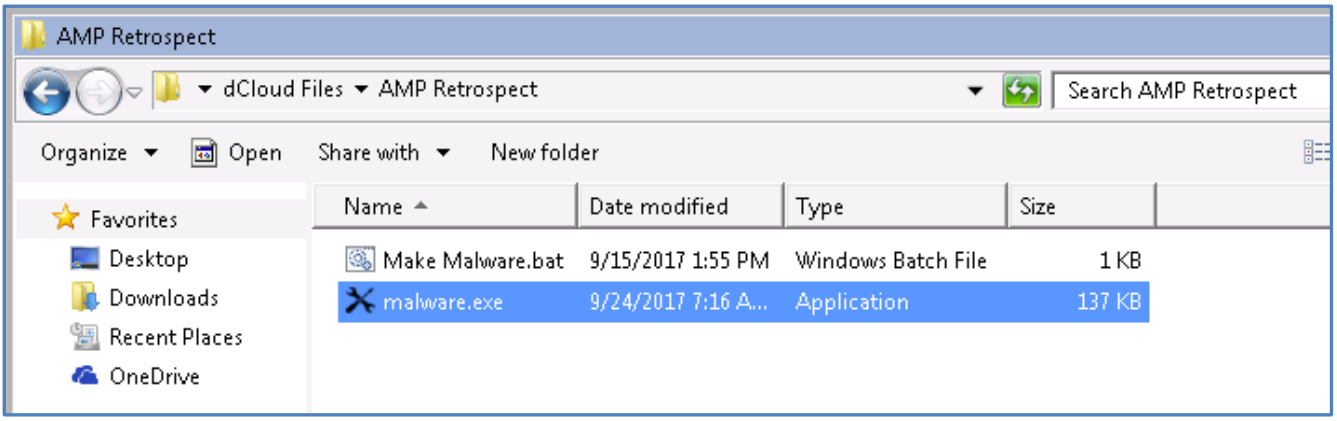
Task - Create a Malicious File (Estimated time to complete: 1 min)

To simulate this type of analysis, a benign file is generated and used within an email coming into the organization. The file itself is not capable of doing any harm, however the Cisco AMP file treats this malicious test file and performs the same actions on it as if it was carrying payload that is malicious.

1. Navigate to the desktop of the workstation, locate and open the folder called dCloud Files**,** open the folder and then open the sub-folder named AMP Retrospect.



2. Open the file Make Malware.bat this file by double clicking it, and acknowledging the **Run** button when prompted. If run successfully a second file will be present named malware.exe.



Task - Send a Message with a potentially malicious file (Estimated time to complete: 1 min)

Now that a file that contains malicious payload has been generated a file, send a message from Adam to Alan with this as an attachment, this is sufficient to trigger the AMP engines and provide the required disposition.

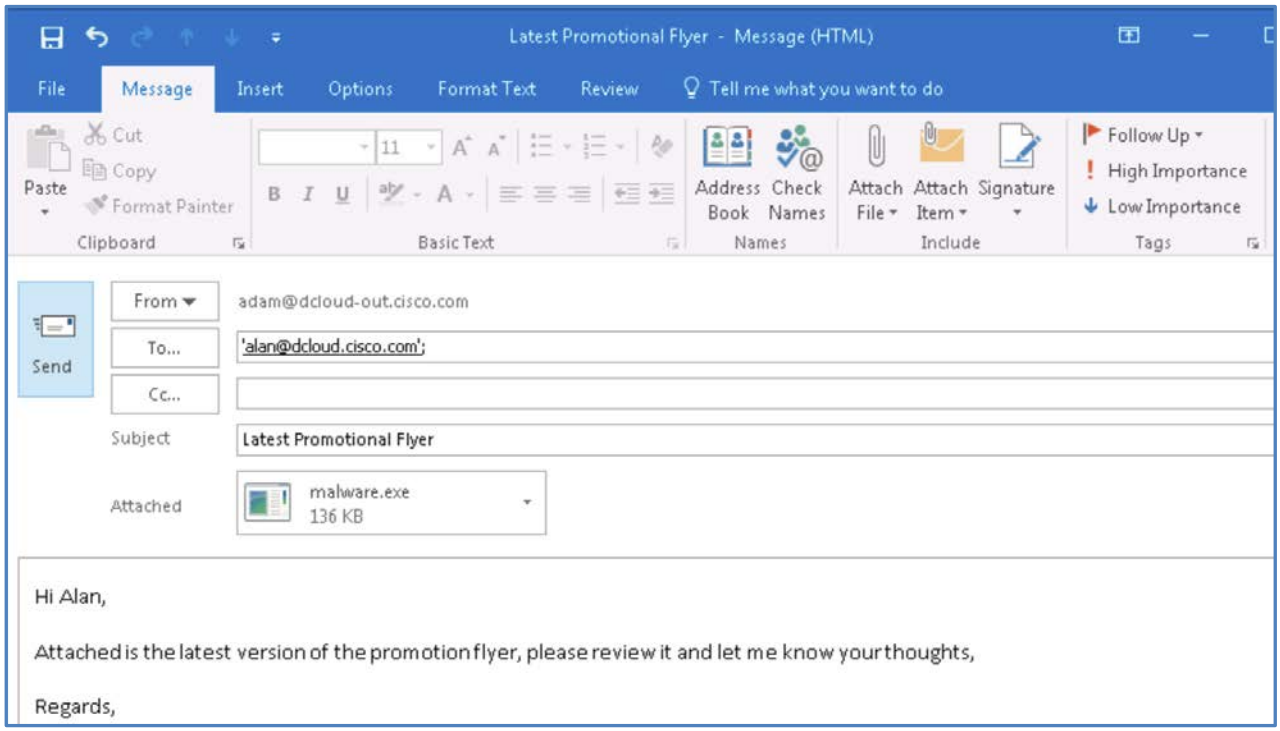
Initiate a CLI session

Prior to preparing the message, initiate a connection to the Cisco Email Security solution from the CLI in order to view, using the tail command, the mail logs to see the message being processed and the actions being applied as it works its way through the pipeline, repeat the same steps to initiate this from the previous scenario.

1. From the workstation launch Microsoft Outlook and from Adams inbox, prepare a new message with the following parameters.
   - To: alan@dcloud.cisco.com
   - Subject: Latest Promotional Flyer
   - Body: Hi Alan,

     Attached is the latest version of the promotional flyer, please review it and let me know your thoughts.

     Regards,
   - Attachment: Attach the file, Malware.exe file created in the previous step



2. Send the message – Microsoft Outlook will display a warning about unsafe files, click **Yes** to ignore this.
3. Force the synchronization process by clicking **Send/Receive Folder** or by pressing the **F9** key.

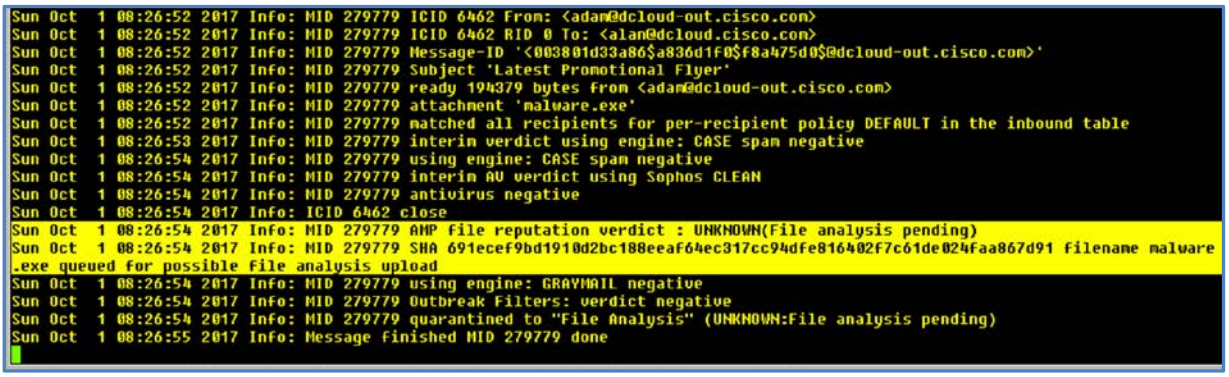
Task - Monitoring AMP (Estimated time to complete: 10 min)

This task will demonstrate how potentially malicious files are handled by the Cisco Email Security Solution and specially the AMP engine.

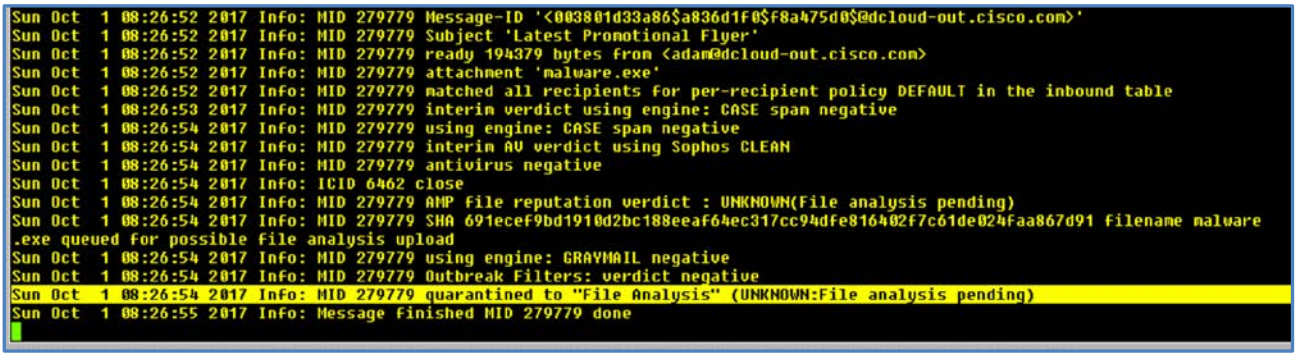
1. Navigate to the CLI session and wait for the logs to scroll, it may take a few moments for the screen to refresh with fresh activity. The first point of interest here is what happens once the SPAM and Anti-Virus engines pass their verdict.

2. The highlighted line below and the one prior to that shows the file reputation verdict – unknown therefore the file will be sent for further analysis, also note that a SHA256 has been assigned.

3. Make a note of the MID.

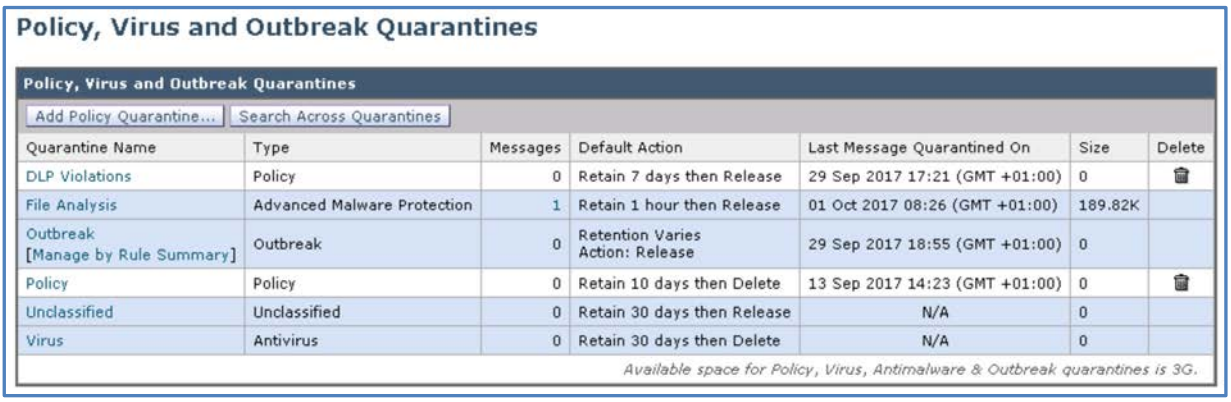


4. The next point of interest is what happens to the file whilst a finalised verdict is returned.

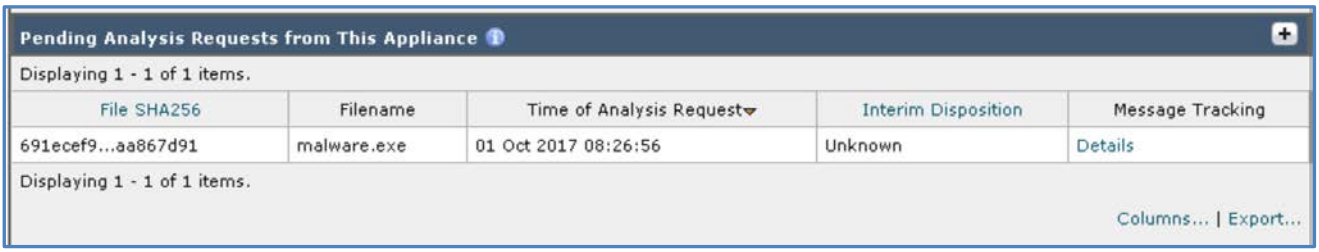


NOTE: It can take several minutes for the verdict to be returned, leave the CLI window running and proceed to the next step, or take a break!

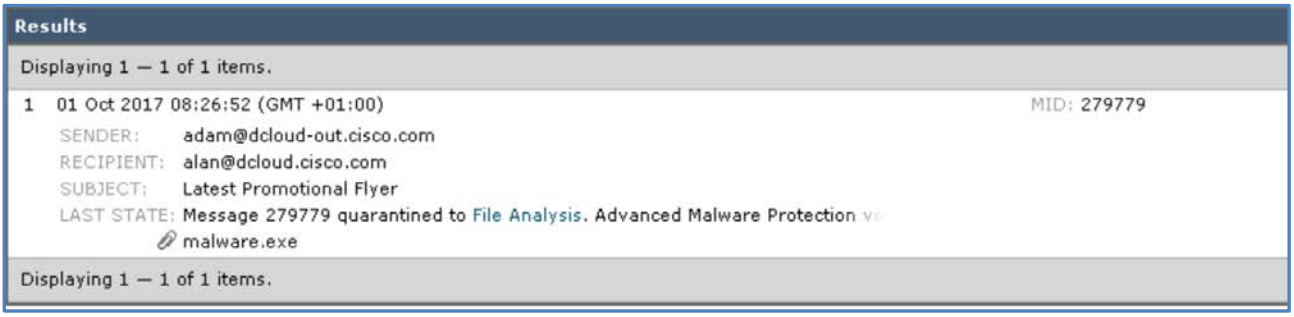
5. Navigate to **Monitor > Policy, Virus and Outbreak Quarantines**, the message is now quarantined as per the configured AMP policy while a verdict of its disposition is returned from the AMP File Reputation service.



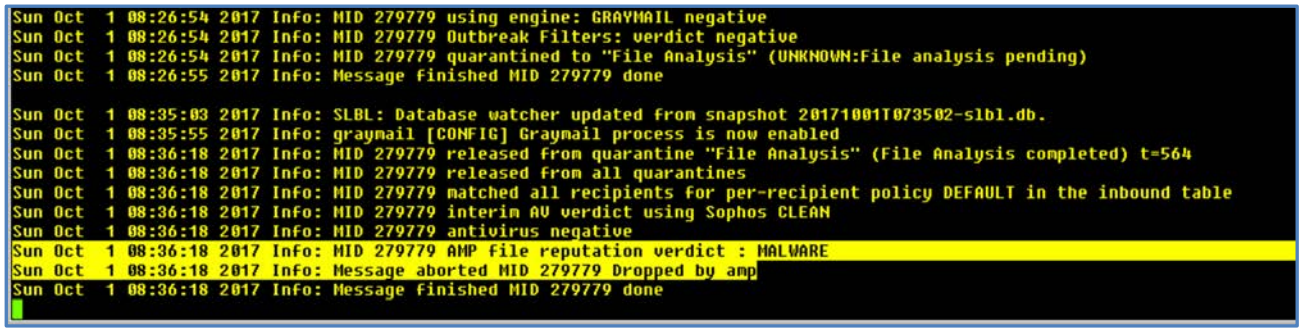
6. Navigate to **Monitor > AMP File Analysis**, note the file is not analysed yet as indicated by the *Interim Disposition*.



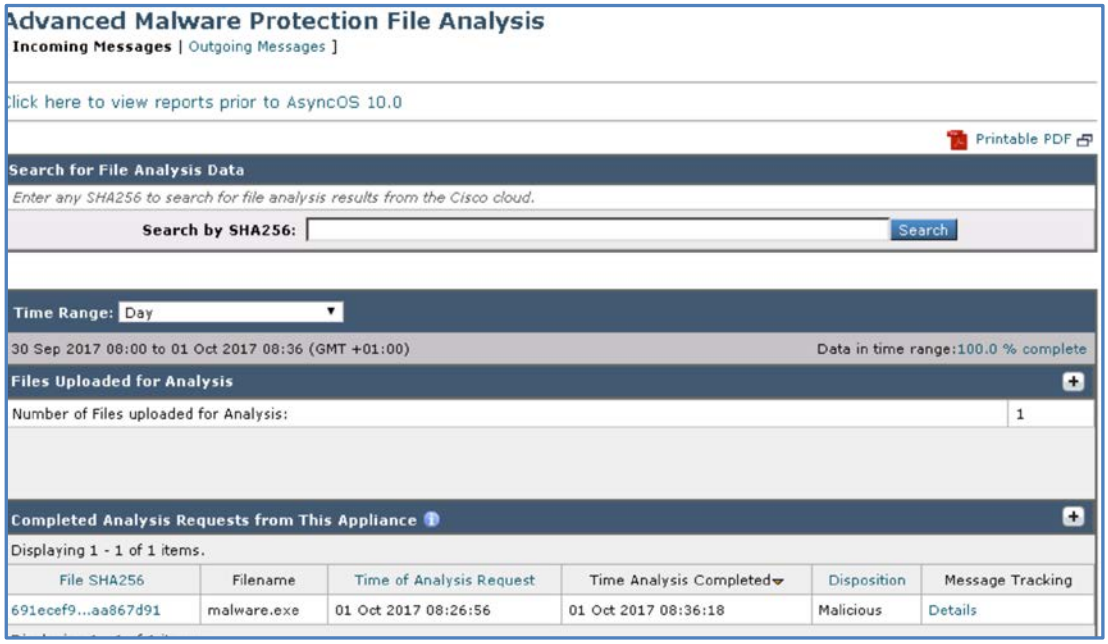
7. Click on Details to launch Message Tracking and scroll towards to the *Results* section, our message will be listed, note the MID once again matches what was observed within the CLI earlier.



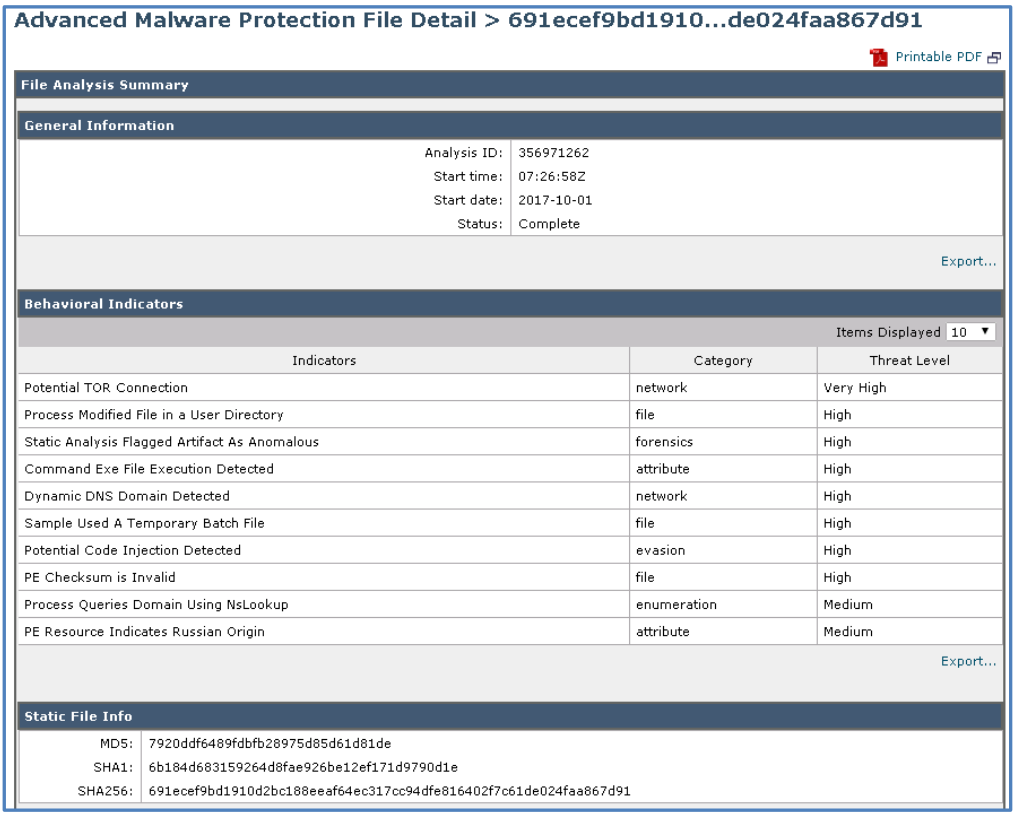
8. Navigate back to the CLI session, after several minutes a verdict will be returned. Note the time between when the file was sent for analysis and when the verdict was returned and finally the final action.



9. Navigate back to the GUI and select **Monitor > AMP File analysis** the verdict will now be presented here too.



10. Click on the **SHA** to get more details of the perceived threat and the various threat levels assigned to the file.



Advanced Malware Protection File Detail > 691ecef9bd1910...de024faa867d91

Printable PDF

File Analysis Summary

General Information

Analysis ID:	356971262
Start time:	07:26:58Z
Start date:	2017-10-01
Status:	Complete

Export...

Behavioral Indicators

Items Displayed 10

Indicators	Category	Threat Level
Potential TOR Connection	network	Very High
Process Modified File in a User Directory	file	High
Static Analysis Flagged Artifact As Anomalous	forensics	High
Command Exe File Execution Detected	attribute	High
Dynamic DNS Domain Detected	network	High
Sample Used A Temporary Batch File	file	High
Potential Code Injection Detected	evasion	High
PE Checksum is Invalid	file	High
Process Queries Domain Using NsLookup	enumeration	Medium
PE Resource Indicates Russian Origin	attribute	Medium

Export...

Static File Info

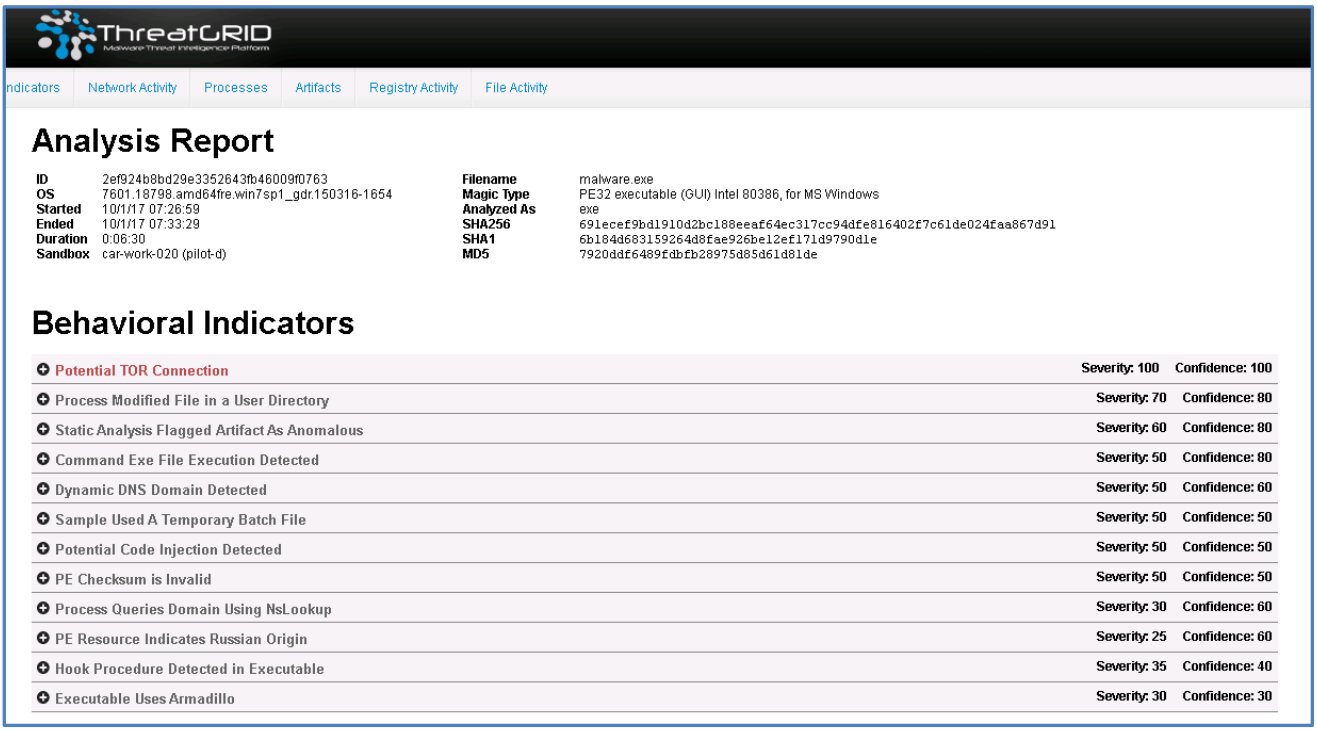
MD5:	7920ddf6489fdbfb28975d85d61d81de
SHA1:	6b184d683159264d8fae926be12ef171d9790d1e
SHA256:	691ecef9bd1910d2bc188eeaf64ec317cc94dfe816402f7c61de024faa867d91

11. Finally, click the link to the **Cisco AMP Threat Grid** to get details of the full analysis.

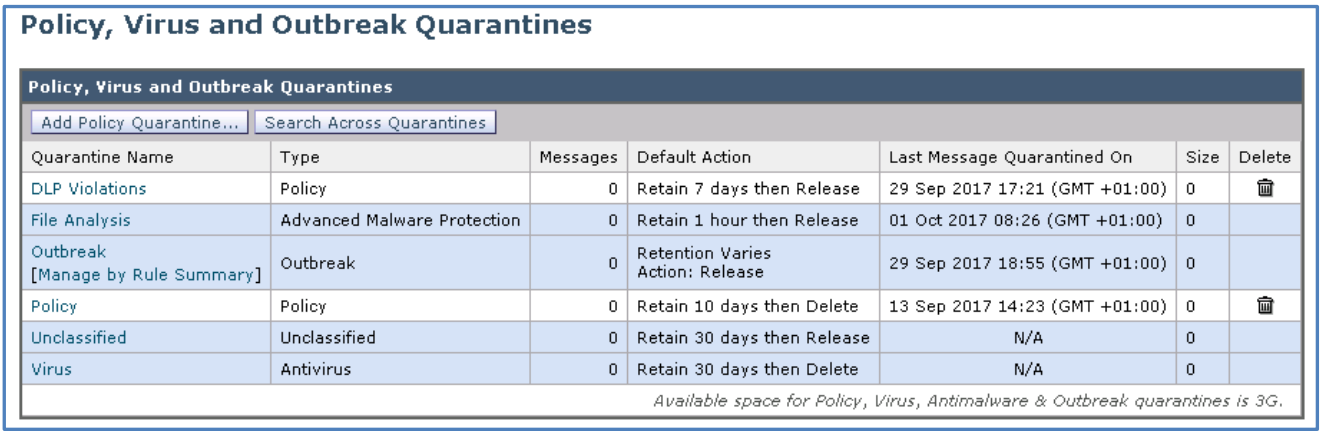
More Details

To view all messages for this threat, see: Message Tracking for SHA256 691ecef9bd1910d2bc188eeaf64ec317cc94dfe816402f7c61de024faa867d91
To view full analysis details, see: Cisco AMP Threat Grid

12. This will redirect to the Cisco AMP ThreatGrid portal to get a detailed analysis of what caused this file to be malicious.



13. Close the ThreatGrid window and navigate to **Monitor > Policy, Virus and Outbreak Quarantines**, and note the queue is now empty, this is because the verdict for the file returned was malicious and it was deleted from the quarantine.



Scenario 8. Graymail Detection

Use Case

Since the investment in the Cisco Email Security Solution by Voyage Corp the volume of messages classified as SPAM have decreased markedly with most users reporting a high level of satisfaction in a recent user satisfaction survey. The control of threat within email messages has also improved significantly with a sharp drop in reported incidents following the implementation of multiple security engines.

A handful of users however have complained that they receive messages from company websites that they once signed up for, an example being the manager of enterprise accounts who regular receives email from Netflix, this was initially a service that he had subscribed to, however is now looking to remove himself from that particular mailing list or at least have the message classified appropriately making it easy to identify within his busy mailbox.

Security Control

Graymail messages are messages that do not fit the definition of spam, for example, newsletters, mailing list subscriptions, social media notifications, and so on. These messages were of use at some point in time, but have subsequently diminished in value to the point where the end user no longer wants to receive them.

The difference between graymail and spam is that the end user intentionally provided an email address at some point (for example, the end user subscribed to a newsletter on an e-commerce website or provided contact details to an organization during a conference) as opposed to spam, messages that the end user did not sign up for.

Objective

This scenario will demonstrate, through simulation, how Graymail messages are classified and processed by the Cisco Email Security Solution.

NOTE: The graymail management solution in the Email Security appliance comprises of two components: an integrated graymail scanning engine and a cloud-based Unsubscribe Service. The graymail scanning engine is part of the base operating system, and additional license is required to use the unsubscribe service.

Steps

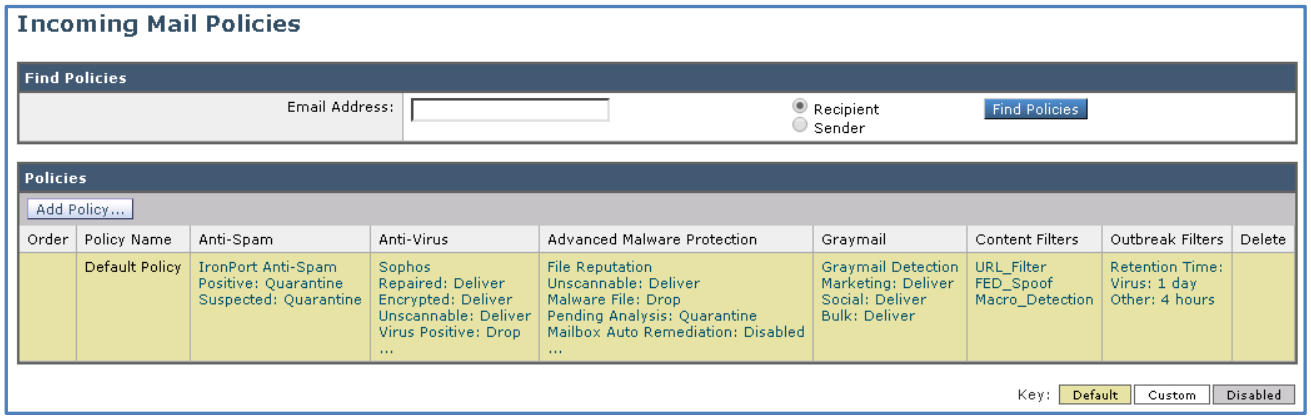
Task - Customise Graymail Classification (Estimated time to complete: 2 min)

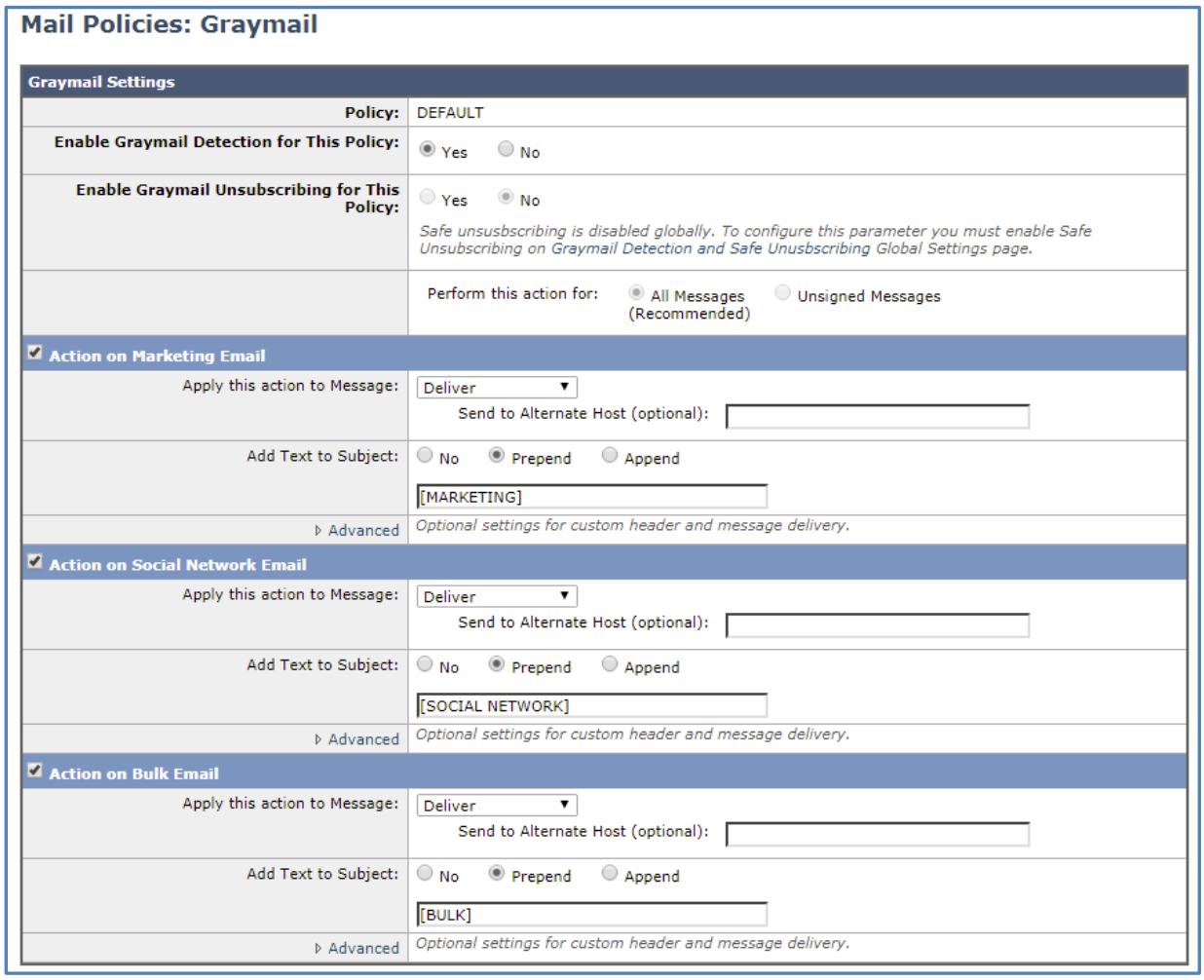
The graymail engine classifies each graymail into one of the following categories:

- **Marketing Email**. Advertising messages sent by professional marketing groups.
- **Social Network Email.** Notification messages from social networks, dating websites, forums, and so on
- **Bulk Email.** Advertising messages sent by unrecognized marketing groups, for example, newsletters from TechTarget, a technology media company.

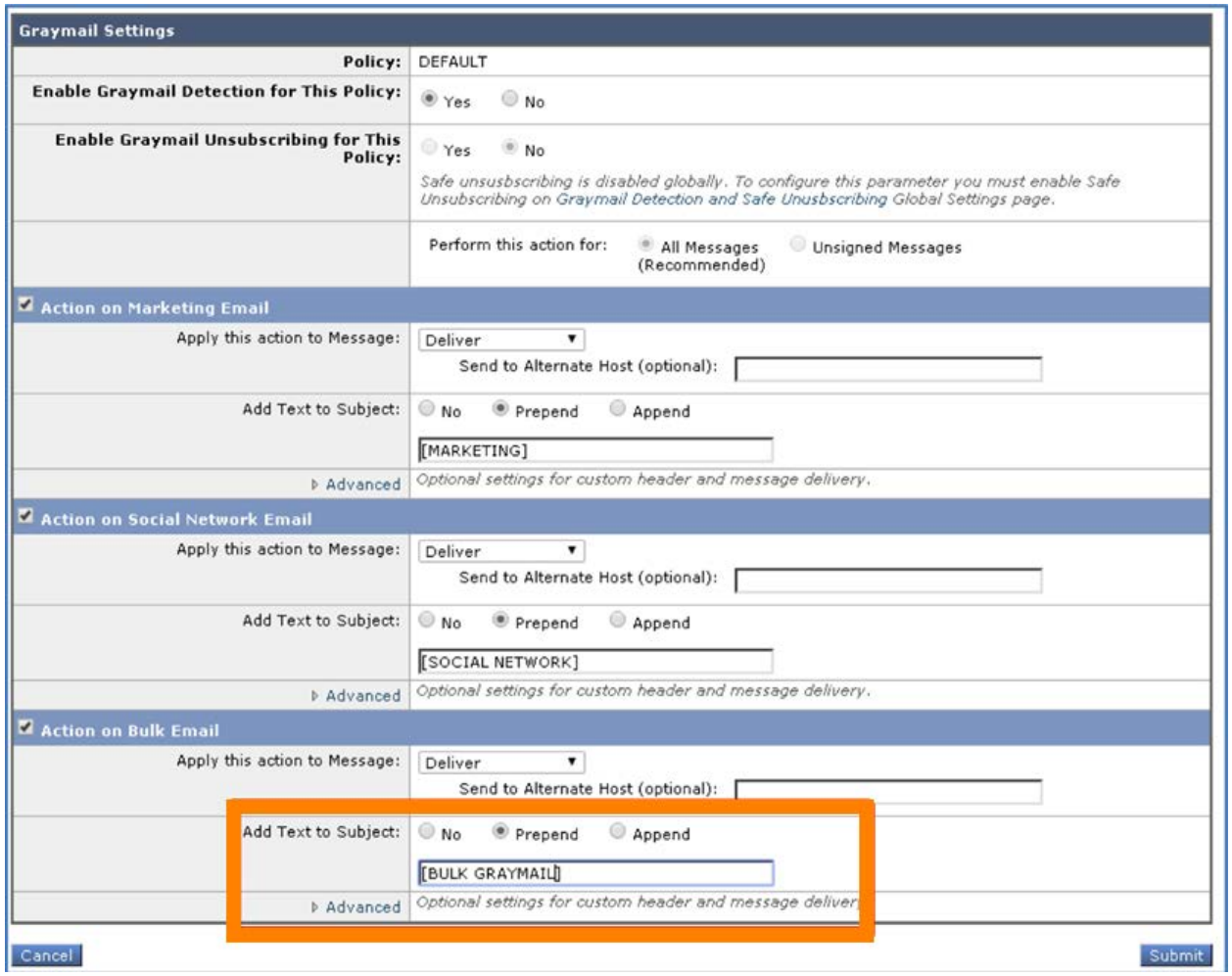
This task will review these and make a subtle change to one.

1. From the workstation access the GUI and navigate to **Mail Policy > Incoming Mail Policies** and click within the Graymail box of the Default Policy to launch the Graymail settings

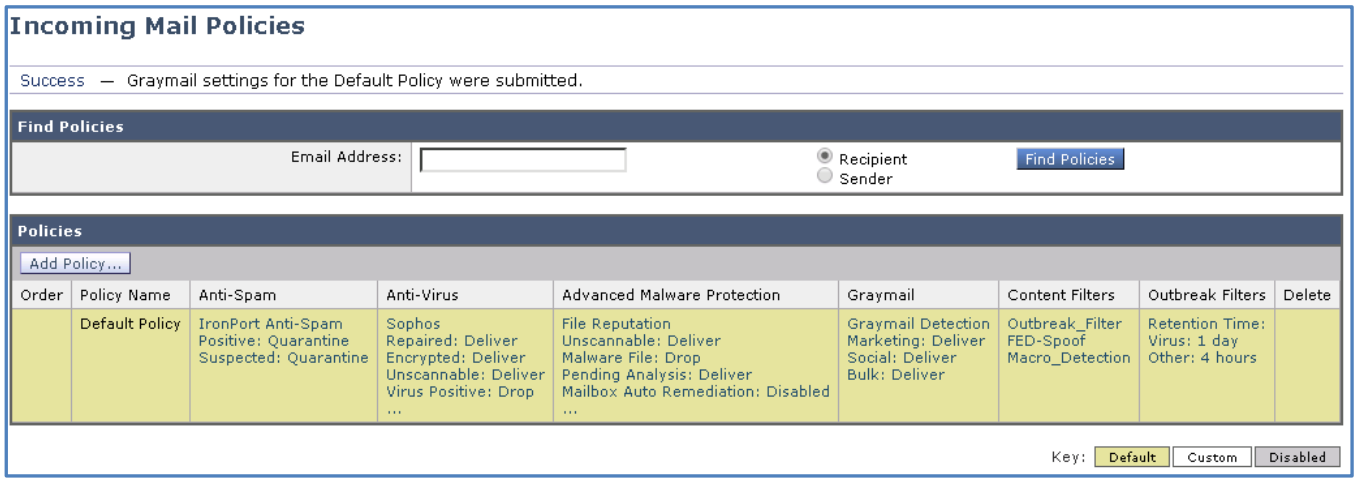




2. For the *Action for Bulk Email* edit default Add Text to Subject so alternate text is displayed.
3. Change the default to **BULK GRAYMAIL**.



4. Click **Submit** to apply the changes.



5. Once complete, ensure the change is applied by clicking the **Commit Changes** button, adding optional comments if desired.

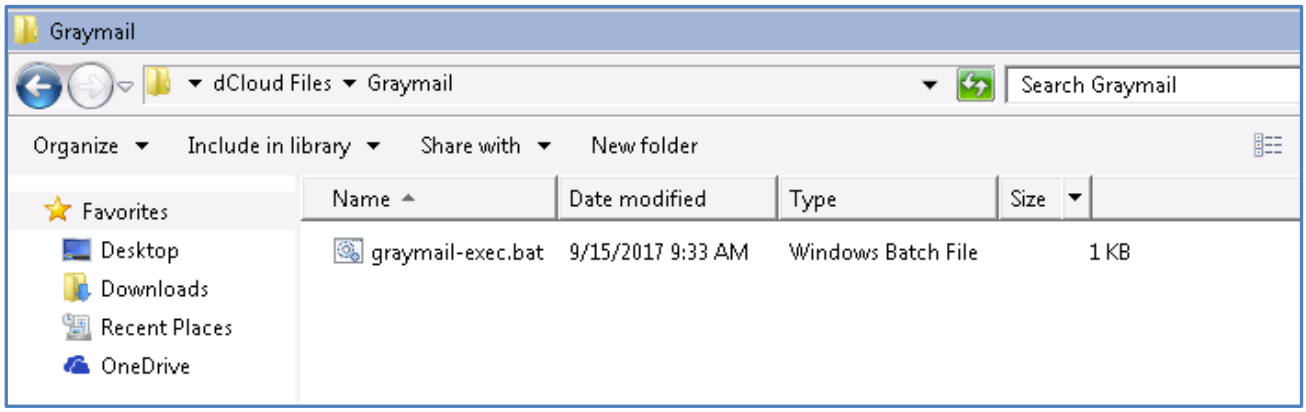
Task - Simulate Graymail (Estimated time to complete: 5 min)

In order to see the effect of the Graymail engine this task will simulate the sending and processing of a Netflix message that would be categorised by the engine as Bulk.

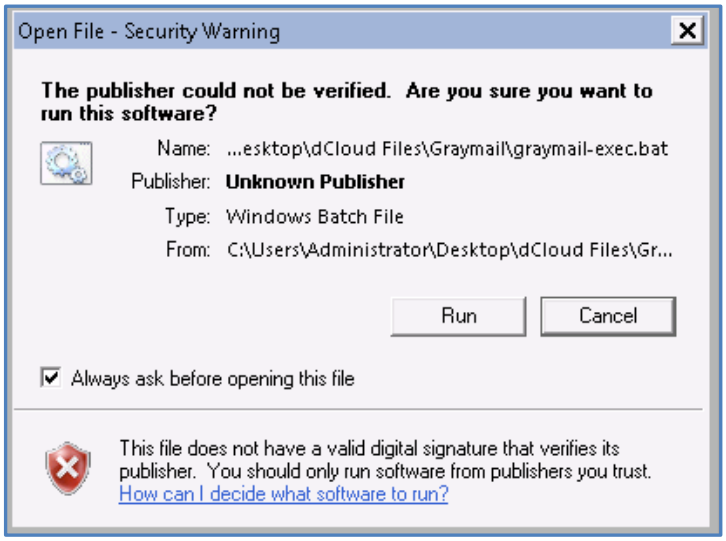
Initiate a CLI session

Prior to preparing the message, initiate a connection to the Cisco Email Security solution from the CLI in order to view, using the tail command, the mail logs to see the message being processed and the actions being applied as it works its way through the pipeline, repeat the same steps to initiate this from the previous scenario.

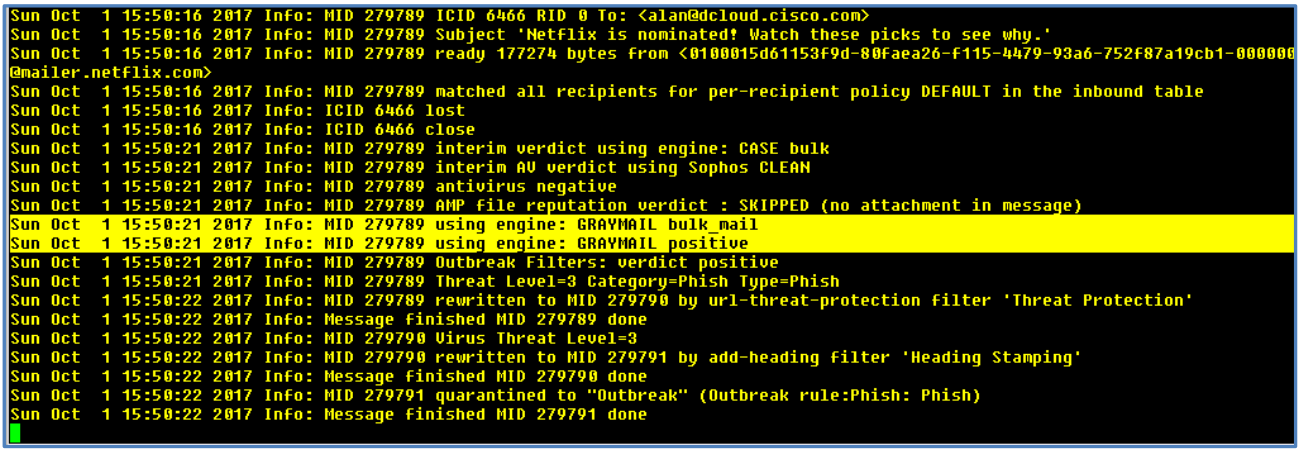
1. From the desktop, navigate to the folder dCloud File>Graymail and verify the presence of graymail-exec.bat file.



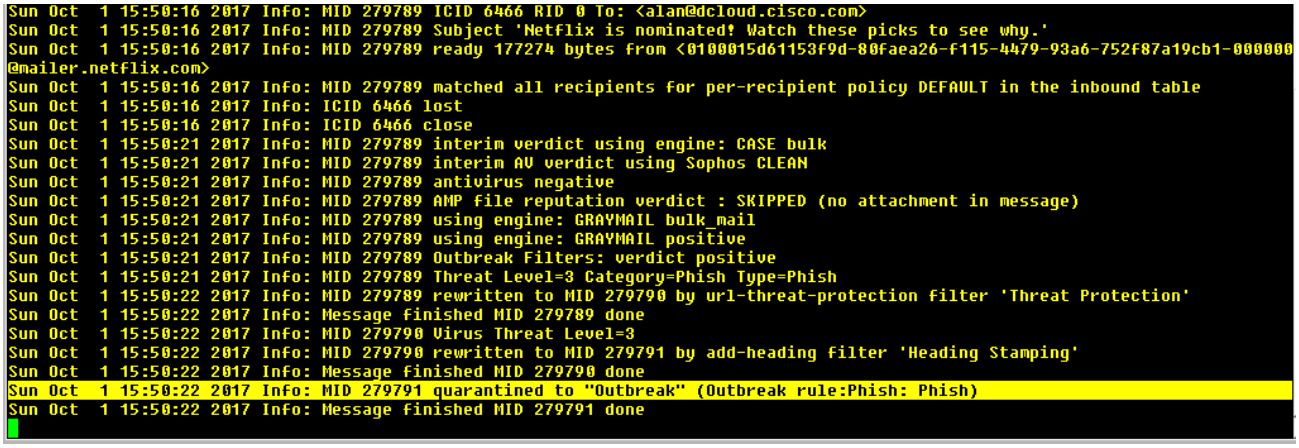
2. Execute the file by double clicking it - acknowledging any security warning message as this is safe for this environment.



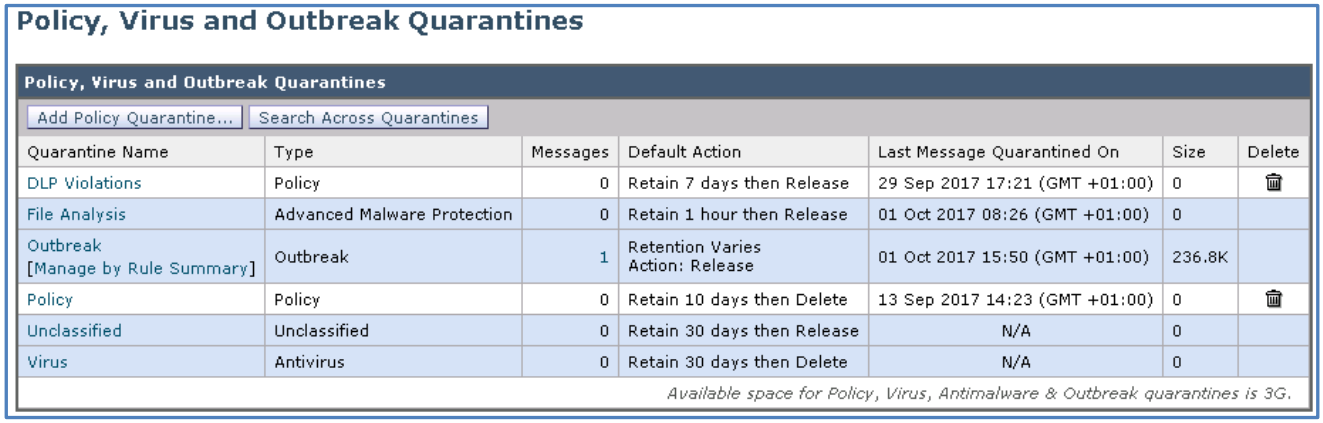
3. Navigate to the CLI and note how the graymail engine classifies this type of message.



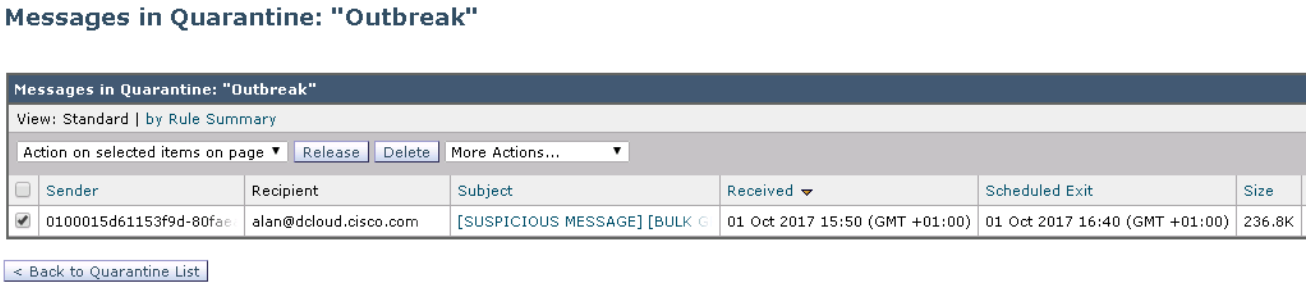
4. Also notice the outbreak filters engine delivered a verdict, and took action on the message by sending it the quarantine.



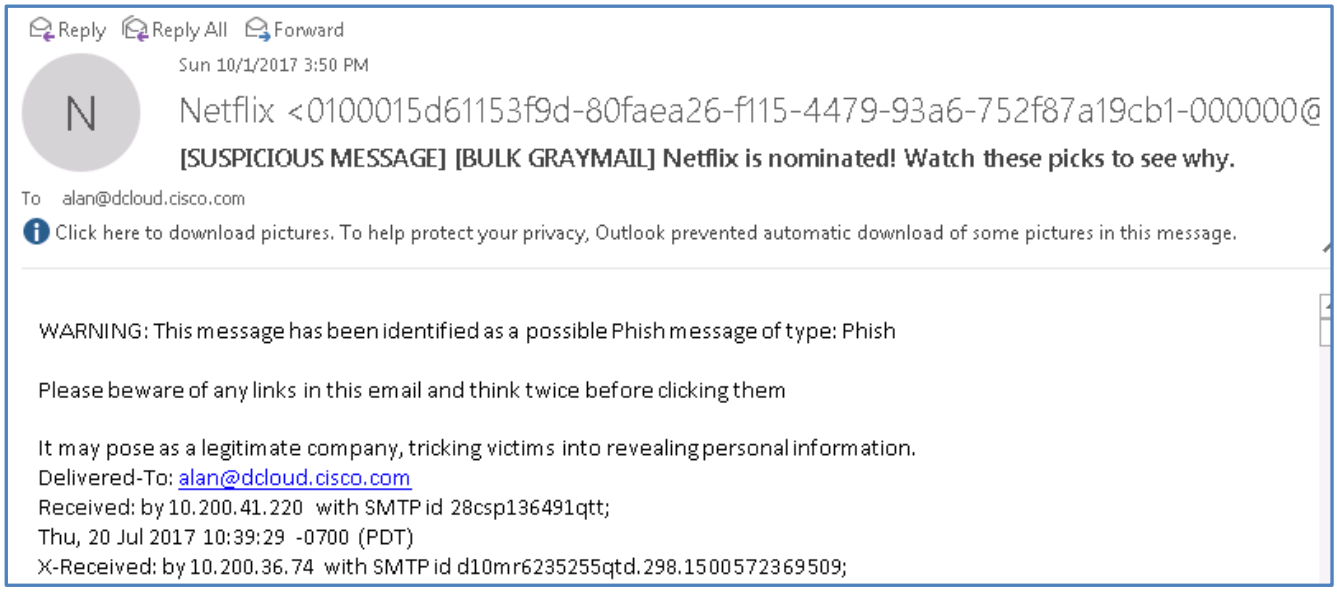
5. Navigate to **Monitor > Policy, Virus and Outbreak Quarantines,** and note the queue is now empty, this is because the verdict for the file returned was malicious and it was deleted from the quarantine.



6. Click the number under the Messages column to view the message, place a check next the message and press the **Release** button to send the file onwards.



7. From the desktop navigate back the outlook client and synchronize the mailboxes. The message from Netflix will now appear in Alan's inbox, note the subject header, this has now been modified as per the previous task.



NOTE: The second part of this feature is Unsubscribe, which provides an easy mechanism for end users to unsubscribe from unwanted messages using Unsubscribe Service.

Scenario 9. Image Analysis

Use Case

Voyage Corp regularly takes on office interns from the local college to help students gain valuable work experience prior to their graduation; in return they get additional resources temporarily without having to go through the process of applying for headcount. The offer can range from range from 1-4 weeks depending on the agreement between HR and the college.

Recently a new intern was inducted and the offer would last for one week only, leaving little time for formal company training on acceptable use and how to exercise caution when dealing with email and web systems, this unfortunately lead to an intern receiving an attachment via email, that had, what was seen as inappropriate content for a professional working environment, this caused unnecessary embarrassment to the intern and their peers at the time.

Security Control

Some messages contain images that you may wish to scan for inappropriate content. The image analysis engine can be leveraged to search for inappropriate content in email. Image analysis is not designed to supplement or replace your anti-virus and anti-spam scanning engines; instead, its purpose is to enforce acceptable use by identifying inappropriate content in email. The image analysis scanning engine can be used to quarantine and analyses mail and to detect trends allowing for better policy enforcement and end user education.

Objective

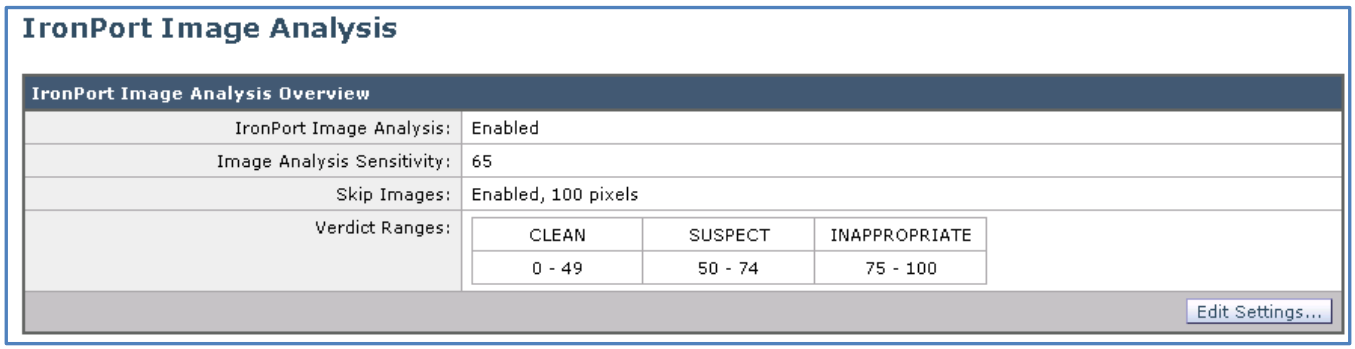
This scenario will demonstrate how the Image Analysis engine in the Cisco Email Security Solution can identify inappropriate content in an email message and take necessary actions as required by company policy.

Steps

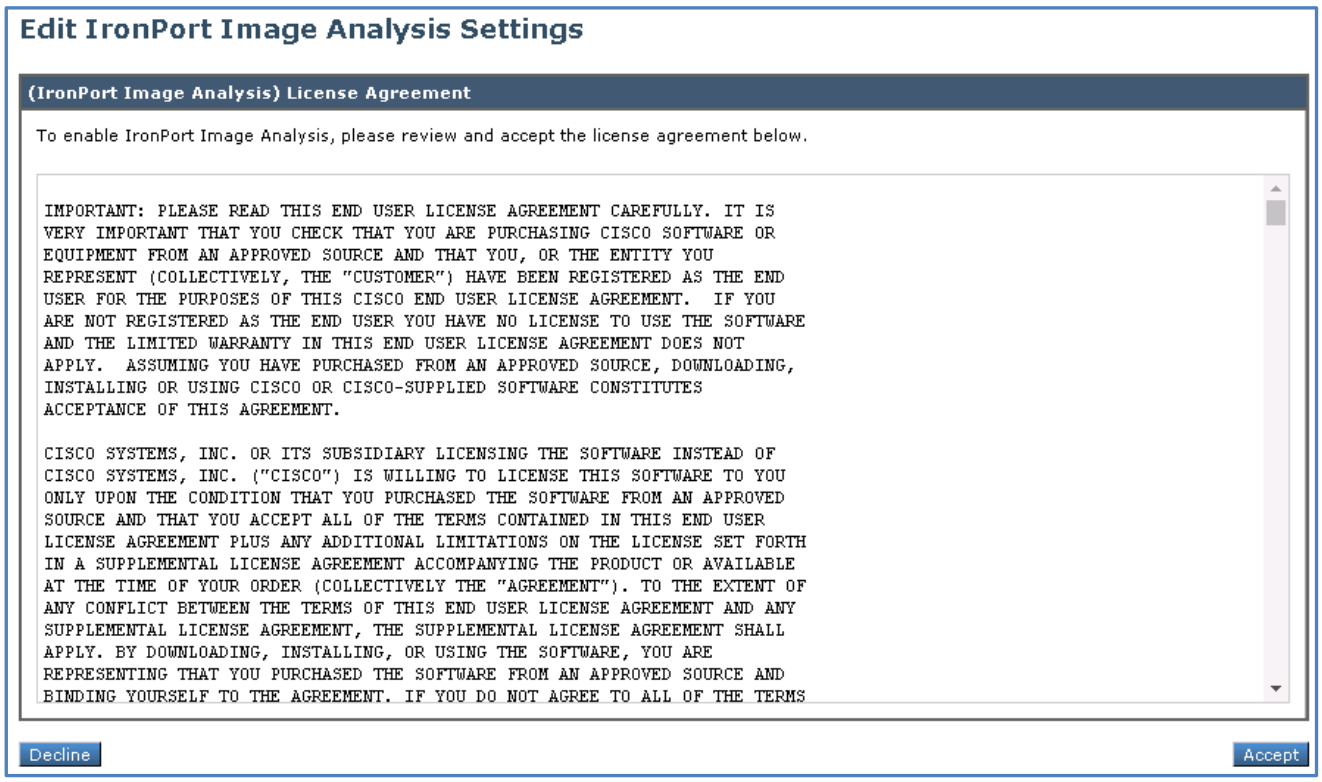
Task - Enabling the Image Analyser Feature (Estimated time to complete: 5 min)

The image analyser is an additional feature license that once installed can be tuned to suit the requirements of the environment in which it operates.

1. Navigate to **Security Services > IronPort Image Analysis** and from the resulting screen click Edit Settings



2. View the license agreement and click **Accept**.

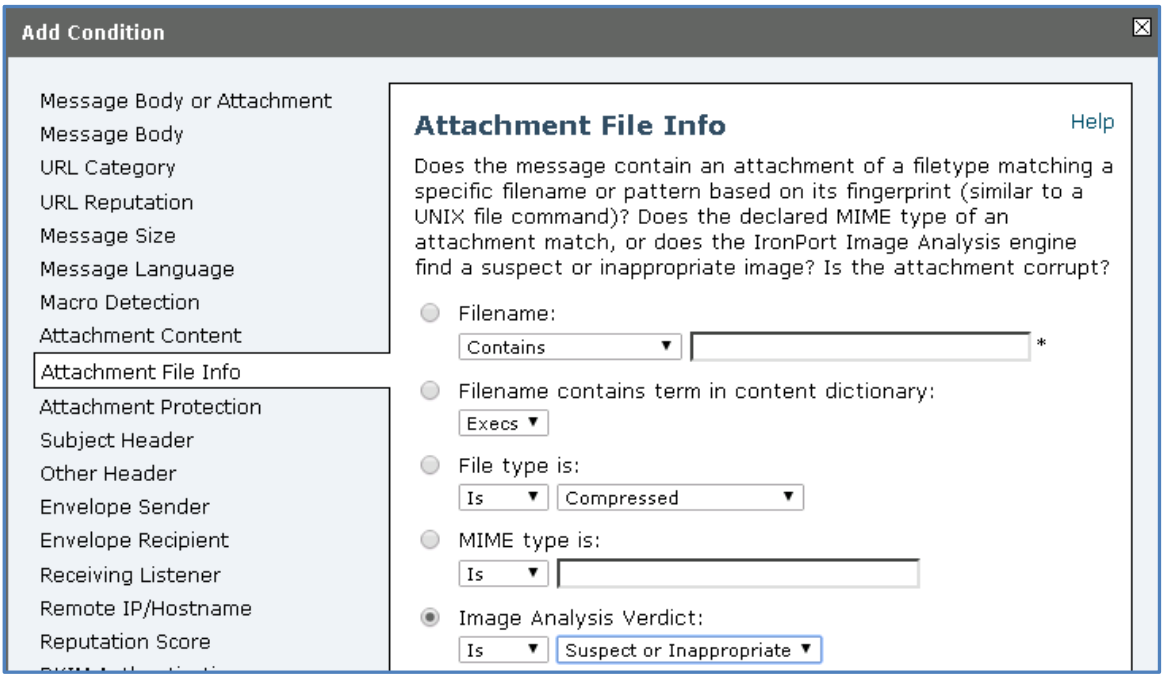


3. Once accepted the confirmation message is displayed, advising this feature can now be use with either Content Filters or Message Filters.

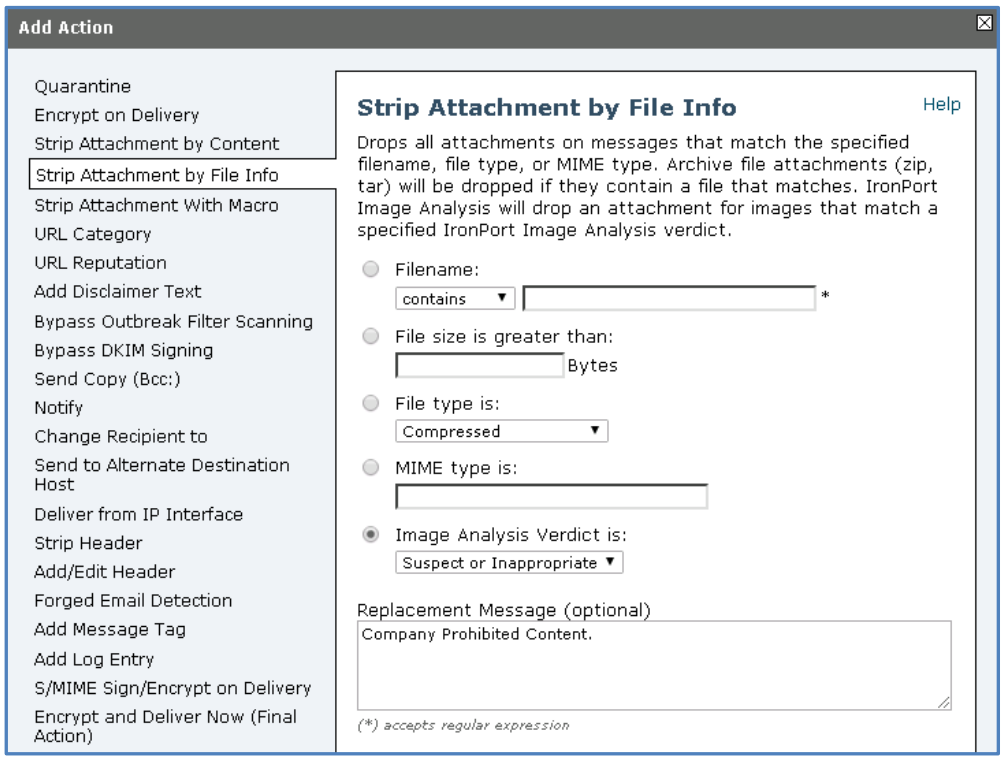
Task - Configuring a Content Filter (Estimated time to complete: 3 min)

This task will create a new content filter to identify inappropriate content with in an email message and apply an action of stripping the attachment before advising the recipient the reason this action was taken.

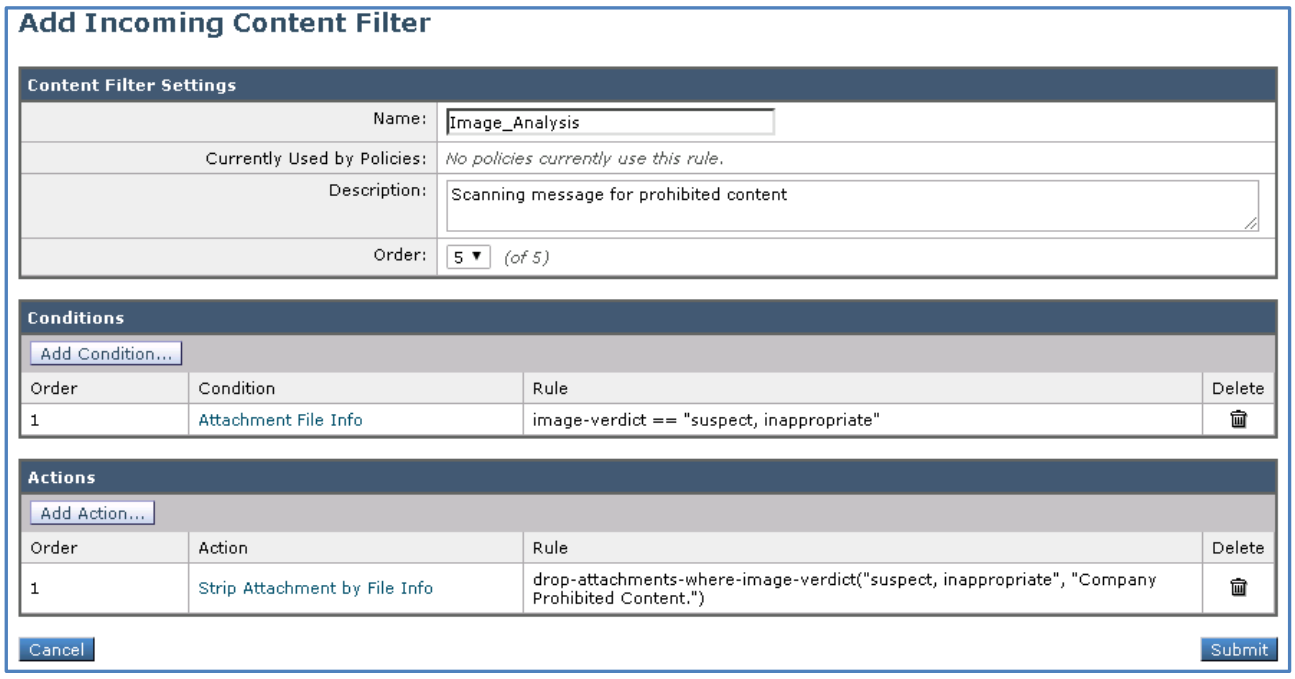
1. From the workstation access the GUI and navigate to **Mail Policy > Incoming Content Filters** and click **Add Filter**.
2. Using the following settings configure the Conditions and Actions.
   - Name: Image_Analysis
   - Description: Scanning message for prohibited content
   - Condition: Attachment File Info > Image Analysis Verdict: Is > Suspect or Inappropriate
   - Actions: Strip Attachment by File Info > Image Analysis Verdict is: Suspect or Inappropriate
   - Replacement Message (optional) > Company prohibited content.



3. Click **OK.**
4. Click **Add Action.**



5. Click **OK.**

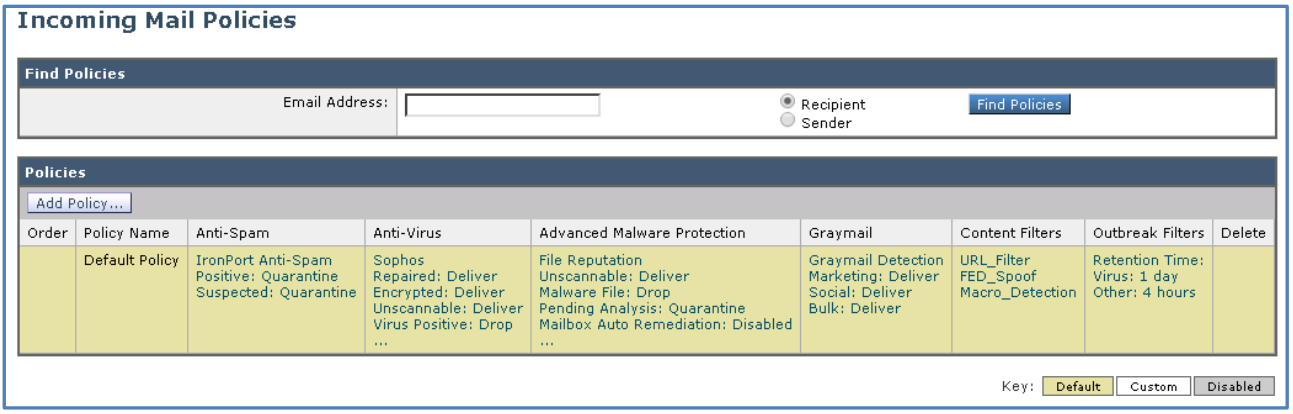


6. Click **Submit** to apply the actions and commit changes.

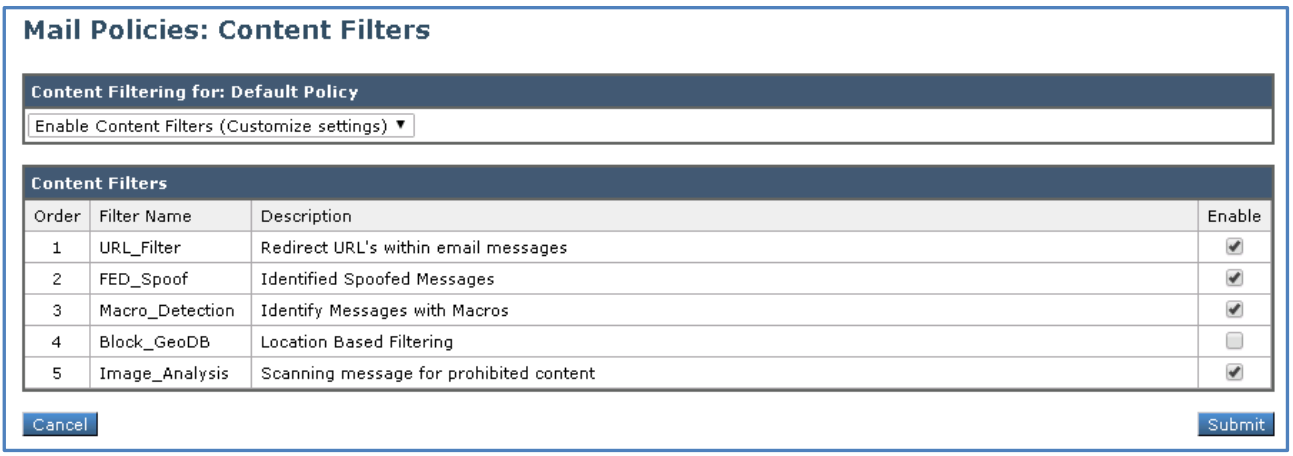
Task - Edit Incoming Mail Policy (Estimated time to complete: 1 min)

With the required Content Filter in place, the final task is to create an incoming mail policy to implement the conditions specified in the previous step and take the necessary actions.

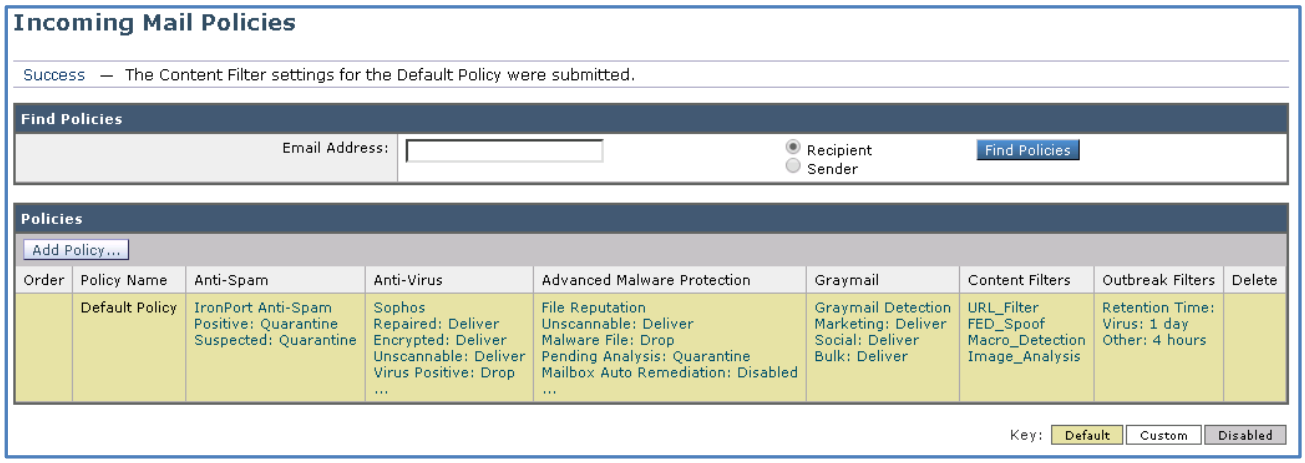
1. From the workstation access the GUI and navigate to **Mail Policy > Incoming Mail Policies** and click within the Content Filters box of the Default Policy.



2. Place a checkmark against the content filter Image_Analysis created in the previous step to enable it.



3. Click **Submit** to create the content Filter and verify the policy.



4. Once complete, ensure the change is applied by clicking the **Commit Changes** button, adding optional comments if desired.

Task - Testing Image Analysis (Estimated time to complete: 5 min)

With the entire configuration in place, the Image Analysis feature can be tested by sending an email to Alan from external user Adam with an inappropriate image attached to the message.

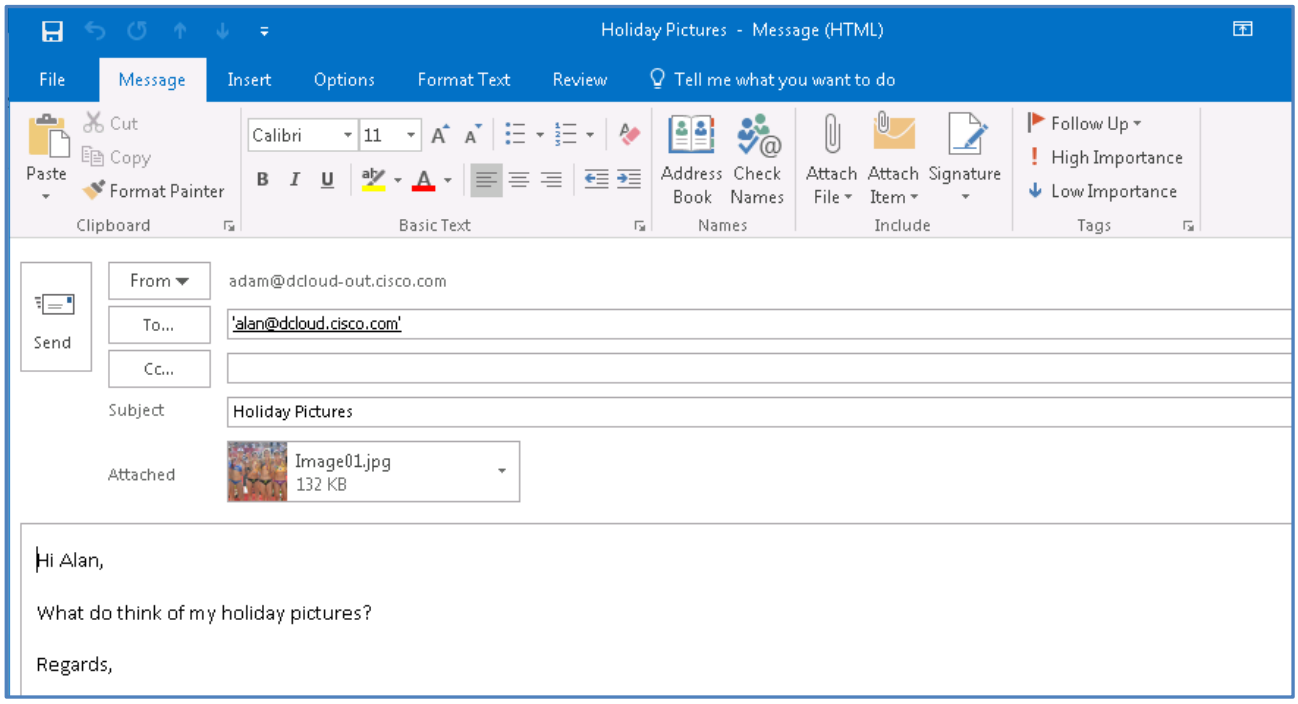
Initiate a CLI session

Prior to preparing the message, initiate a connection to the Cisco Email Security solution from the CLI in order to view, using the tail command, the mail logs to see the message being processed and the actions being applied as it works its way through the pipeline, repeat the same steps to initiate this from the previous scenario.

1. From the workstation launch Microsoft Outlook and from Adams inbox, prepare a new message with the following parameters.
   - To: alan@dcloud.cisco.com
   - Subject: Holiday Pictures
   - Body: Hi Alan,

     What do you think of my Holiday pictures?

     Regards,
   - Attach: Image01.jpg - located on the desktop under the Images sub folder.



2. Send the email - Force the synchronization process by clicking **Send/Receive Folder** or by pressing the **F9** key.

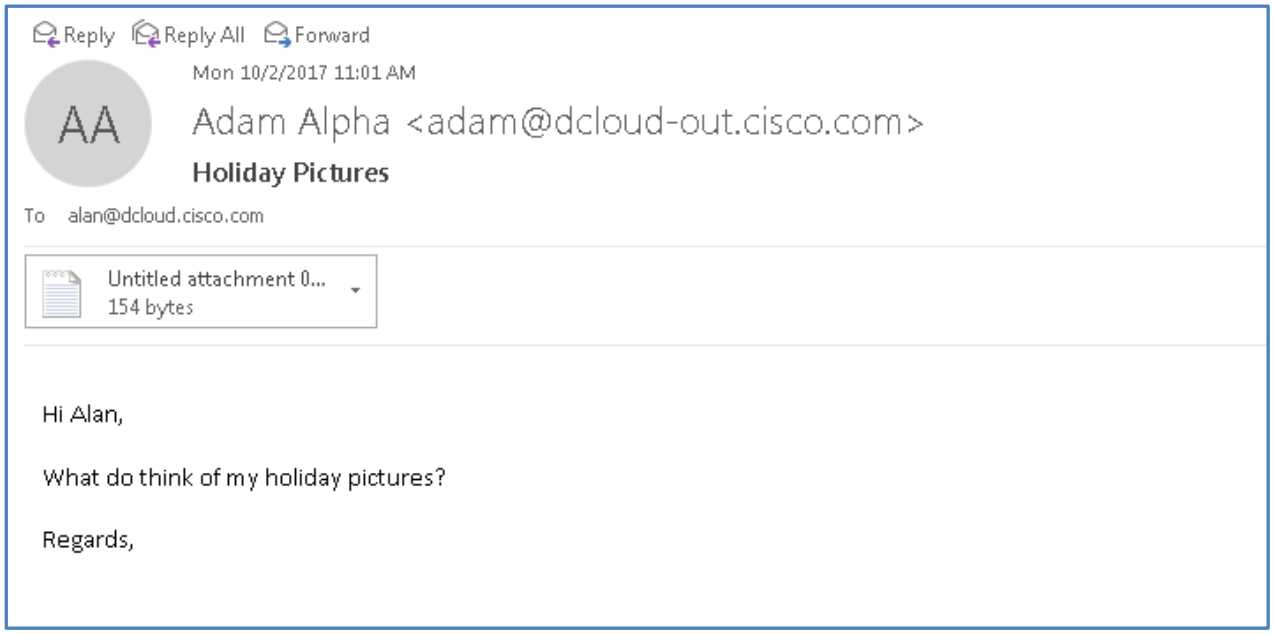
3. Switch back to the CLI and notice how the content filter handled the message, the attachment was assigned a score of 87 which falls under the category of Inappropriate

```
Mon Oct  2 11:00:40 2017 Info: MID 279808 ICID 6480 From: <adam@dcloud-out.cisco.com>
Mon Oct  2 11:00:40 2017 Info: MID 279808 ICID 6480 RID 0 To: <alan@dcloud.cisco.com>
Mon Oct  2 11:00:40 2017 Info: MID 279808 Message-ID '<00ad01d33b65$4fbbcdc0$ef336940$@dcloud-out.cisco.com>'
Mon Oct  2 11:00:40 2017 Info: MID 279808 Subject 'Holiday Pictures'
Mon Oct  2 11:00:40 2017 Info: MID 279808 ready 183198 bytes from <adam@dcloud-out.cisco.com>
Mon Oct  2 11:00:40 2017 Info: MID 279808 attachment 'Image01.jpg'
Mon Oct  2 11:00:41 2017 Info: MID 279808 IronPort Image Analysis: attachment 'Image01.jpg' score 87
Mon Oct  2 11:00:41 2017 Info: MID 279808 matched all recipients for per-recipient policy DEFAULT in the inbound table
Mon Oct  2 11:00:43 2017 Info: ICID 6480 close
Mon Oct  2 11:00:46 2017 Info: MID 279808 interim verdict using engine: CASE spam negative
Mon Oct  2 11:00:46 2017 Info: MID 279808 using engine: CASE spam negative
Mon Oct  2 11:00:46 2017 Info: MID 279808 interim AV verdict using Sophos CLEAN
Mon Oct  2 11:00:46 2017 Info: MID 279808 antivirus negative
Mon Oct  2 11:00:46 2017 Info: MID 279808 AMP file reputation verdict : UNKNOWN
Mon Oct  2 11:00:46 2017 Info: MID 279808 using engine: GRAYMAIL negative
Mon Oct  2 11:00:46 2017 Info: MID 279808 rewritten to MID 279809 by drop-attachments-where-image-verdict filter 'Image_Analysi
s'
Mon Oct  2 11:00:46 2017 Info: Message finished MID 279808 done
Mon Oct  2 11:00:46 2017 Info: MID 279809 using engine: CASE using cached verdict
Mon Oct  2 11:00:46 2017 Info: CASE cache status: hits = 3, misses = 24, expires = 0, adds = 24, seconds saved = 13.51, total s
econds = 123.23
Mon Oct  2 11:00:46 2017 Info: MID 279809 Outbreak Filters: verdict negative
Mon Oct  2 11:00:46 2017 Info: MID 279809 queued for delivery
Mon Oct  2 11:00:46 2017 Info: New SMTP DCID 2580 interface 198.18.133.146 address 198.18.133.2 port 25
Mon Oct  2 11:00:46 2017 Info: Delivery start DCID 2580 MID 279809 to RID [0]
Mon Oct  2 11:00:46 2017 Info: Message done DCID 2580 MID 279809 to RID [0]
Mon Oct  2 11:00:46 2017 Info: MID 279809 RID [0] Response '2.6.0 <00ad01d33b65$4fbbcdc0$ef336940$@dcloud-out.cisco.com> [Inter
nalId=32] Queued mail for delivery'
```

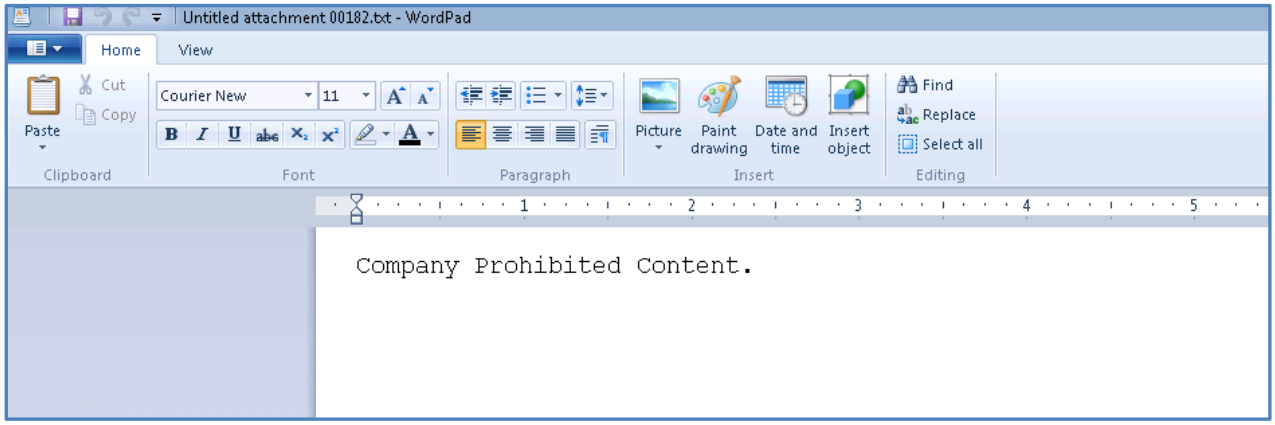
4. The attachment is subsequently dropped from the message.

```
Mon Oct  2 11:00:40 2017 Info: MID 279808 Subject 'Holiday Pictures'
Mon Oct  2 11:00:40 2017 Info: MID 279808 ready 183198 bytes from <adam@dcloud-out.cisco.com>
Mon Oct  2 11:00:40 2017 Info: MID 279808 attachment 'Image01.jpg'
Mon Oct  2 11:00:41 2017 Info: MID 279808 IronPort Image Analysis: attachment 'Image01.jpg' score 87
Mon Oct  2 11:00:41 2017 Info: MID 279808 matched all recipients for per-recipient policy DEFAULT in the inbound table
Mon Oct  2 11:00:43 2017 Info: ICID 6480 close
Mon Oct  2 11:00:46 2017 Info: MID 279808 interim verdict using engine: CASE spam negative
Mon Oct  2 11:00:46 2017 Info: MID 279808 using engine: CASE spam negative
Mon Oct  2 11:00:46 2017 Info: MID 279808 interim AV verdict using Sophos CLEAN
Mon Oct  2 11:00:46 2017 Info: MID 279808 antivirus negative
Mon Oct  2 11:00:46 2017 Info: MID 279808 AMP file reputation verdict : UNKNOWN
Mon Oct  2 11:00:46 2017 Info: MID 279808 using engine: GRAYMAIL negative
Mon Oct  2 11:00:46 2017 Info: MID 279808 rewritten to MID 279809 by drop-attachments-where-image-verdict filter 'Image_Analys
s'
Mon Oct  2 11:00:46 2017 Info: Message finished MID 279808 done
Mon Oct  2 11:00:46 2017 Info: MID 279809 using engine: CASE using cached verdict
Mon Oct  2 11:00:46 2017 Info: CASE cache status: hits = 3, misses = 24, expires = 0, adds = 24, seconds saved = 13.51, total
econds = 123.23
Mon Oct  2 11:00:46 2017 Info: MID 279809 Outbreak Filters: verdict negative
Mon Oct  2 11:00:46 2017 Info: MID 279809 queued for delivery
Mon Oct  2 11:00:46 2017 Info: New SMTP DCID 2580 interface 198.18.133.146 address 198.18.133.2 port 25
Mon Oct  2 11:00:46 2017 Info: Delivery start DCID 2580 MID 279809 to RID [0]
Mon Oct  2 11:00:46 2017 Info: Message done DCID 2580 MID 279809 to RID [0]
Mon Oct  2 11:00:46 2017 Info: MID 279809 RID [0] Response '2.6.0 <00ad01d33b65$4fbbcdc0$ef336940$@dcloud-out.cisco.com> [Inte
nalId=32] Queued mail for delivery'
Mon Oct  2 11:00:46 2017 Info: Message finished MID 279809 done
Mon Oct  2 11:00:51 2017 Info: DCID 2580 close
Mon Oct  2 11:05:10 2017 Info: SLBL: Database watcher updated from snapshot 20171002T100509-slbl.db.
```

5. Navigate back to Alan's inbox, the message is delivered, however the inappropriate content was removed and a replacement inserted.



6. Open the attachment to verify the message presented the end user.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**