

## LTRSEC-2724

### Stopping the lastest attacks with Email Threat Defense

A hand on lab covering Protection of Mail Platforms,  
Best Practices, and API Automation

Greg Barnes - TME  
Alberto Torralba - TME

# Cisco Secure Email Threat Defense Lab

Last Updated: February - 2025

**IMPORTANT!** This content is community-developed and is not subject to standard Cisco verification or support.

## About This Lab

In this lab, you'll explore Cisco Secure Email Threat Defense (ETD), a powerful solution designed to safeguard email environments against advanced threats. Email remains one of the most common and high-risk channels for cyberattacks, with threats ranging from spam and phishing to sophisticated malware and Business Email Compromise (BEC) attacks. Cisco Secure Email Threat Defense integrates seamlessly with on-premises or cloud-based email systems, providing real-time protection through machine learning, threat intelligence, and advanced analytics.

## Objectives

This hands-on lab will guide you through key features of ETD:

**Setting up and Connection to MS365:** Learn the simple process of setting up ETD and connecting it to Microsoft 365 environments

**Policy Configuration:** Learn to set up policies for detecting and mitigating various threats, including phishing attempts, malware, and spam.

**Threat Intelligence:** Discover how Cisco leverages AI/ML/others, to identify and block new and emerging threats in real-time.

**Reporting and Analytics:** Use the ETD dashboard to view threat reports and analyze trends, giving you insights into email security within your organization.

**Integration and APIs:** Understand how to leverage REST APIs to build powerful integration between ETD and your Security applications and/or processes.

## Lab Structure

Throughout this lab, you'll configure security policies, test threat detection capabilities, and monitor and respond to malicious messages. By the end, you should have a robust understanding of how Cisco Secure Email Threat Defense can strengthen your organization's email security posture.

Let's get started on securing email communications and defending against today's most advanced email-based threats!



## Table of Contents

ABOUT THIS LAB .....	2
OBJECTIVES .....	2
REQUIREMENTS .....	4
ABOUT THIS SOLUTION .....	4
TOPOLOGY .....	5
SCENARIO – INTEGRATION WITH EMAIL THREAT DEFENSE .....	6
<i>Use Case</i> .....	6
<i>Objective</i> .....	6
TASK – ACTIVATE CISCO SECURE EMAIL THREAT DEFENSE ACCOUNT .....	7
<i>Lesson learned</i> .....	14
TASK – CONFIGURE EMAIL THREAT DEFENSE ACCOUNT .....	15
<i>Lesson learned</i> .....	18
<i>Configure Cisco Secure Email Threat Defense Policy</i> .....	19
<i>Lesson learned</i> .....	21
TASK – CONFIGURE EXCHANGE ONLINE .....	22
<i>Connector in O365 for ETD traffic</i> .....	27
<i>Lesson learned</i> .....	32
TASK – REVIEW THE PERMISSIONS ASSIGNED IN MICROSOFT (OPTIONAL) .....	33
TASK – TEST THE SOLUTION .....	36
<i>Lesson learned</i> .....	39
TASK - HIGH IMPACT PERSONNEL .....	40
TASK – “ATTACK” YOUR ENVIRONMENT .....	46
<i>Send Email Threats</i> .....	46
TASK – DASHBOARD USE CASE .....	51
<i>Search Messages</i> .....	51
<i>Manual Remediation</i> .....	53
<i>Lesson learned</i> .....	57
TASK – API & POSTMAN .....	57
<i>Authentication API</i> .....	58
<i>Search API</i> .....	62
CONCLUSION .....	68
APPENDIX .....	69
<i>Postman Installation</i> .....	69



## Requirements

This lab will use cloud-based applications and solutions. It is not a requirement to install any application on your laptop, although you have the option to do so.

The requirements are:

- Laptop
- Internet connectivity
- Mobile phone to install the Cisco DUO mobile app

During this lab, we will create accounts on:

- Cisco Email Threat Defense
- Postman Cloud
- Cisco DUO
- Free Email Service (you can also use any other business email account)

## About This Solution

Email Threat Defense augments native Microsoft 365 security and provides complete visibility to inbound, outbound, and internal user-to-user messages.

With Email Threat Defense customers can:

- Detect and block threats with superior threat intelligence from Cisco Talos, one of the largest threat research and efficacy teams.
- Combat advanced threats using Secure Endpoint, and Secure Malware Analytics
- Get complete visibility to inbound, outbound, and internal messages.
- Leverage fast API-driven remediation of messages with malicious content.
- Use an integrated dashboard for search, reporting, and tracking, including conversation view and message trajectory.
- Enhance Microsoft 365 security in less than 5 minutes without changing the mail flow.

For additional information about Cisco Secure Email solutions, visit

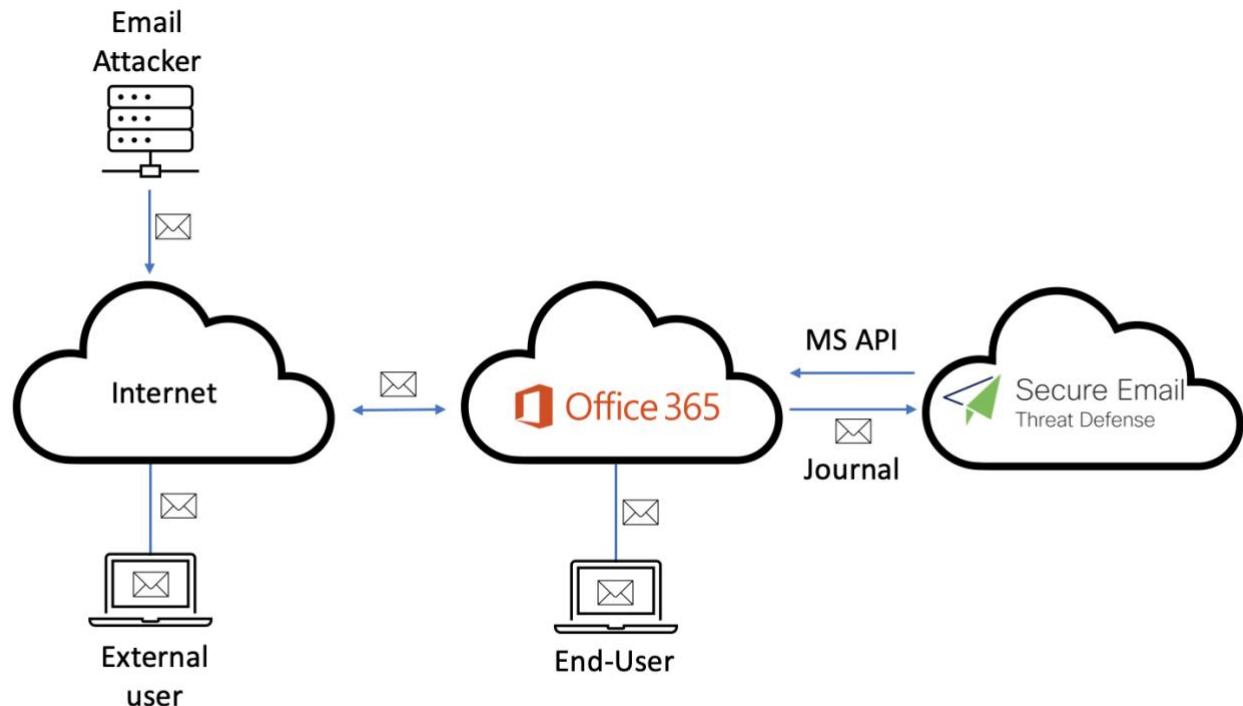
<https://www.cisco.com/site/us/en/products/security/secure-email/index.html>.



## Topology

In this diagram, we can see the different elements that we are going to use in our lab environment:

Figure 1. Lab Topology



### Item Description:

Workstation 1	A workstation that allows lab attendees to access other devices in the same topology
Attacker	A Linux machine that acts as the bad actor, which sends random email messages to other users.
Exchange Online	An Exchange Online mail server provided by the proctor.
Email Threat Defense	An email security cloud account provided by the trainer.

## Scenario – Integration with Email Threat Defense

### Use Case

Attackers are becoming increasingly creative. To detect and prevent the latest attacks, AI/ML should complement what customers currently use for email security, such as gateways or Microsoft 365.

### Objective

This lab goal is to deploy ETD in a Microsoft O365 environment.

For production environments, we may encounter scenarios and situations where some configurations may be different, but the chosen scenario is one of the most common for customers who want to increase security in their Microsoft O365 environment.



## Task – Activate Cisco Secure Email Threat Defense account.

In this lab, we are going to use the ETD beta portal. This means that some steps may be different from those in a production environment.

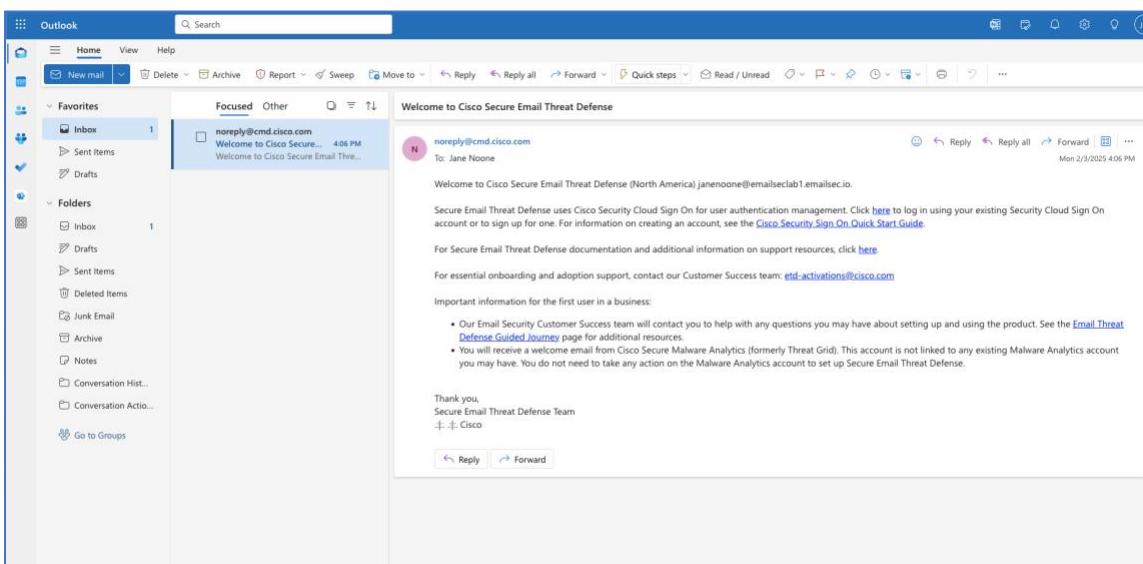
1. Please go to O365 portal <https://outlook.office.com/mail/>

For authentication credentials, please use the lab number assigned by the proctor.

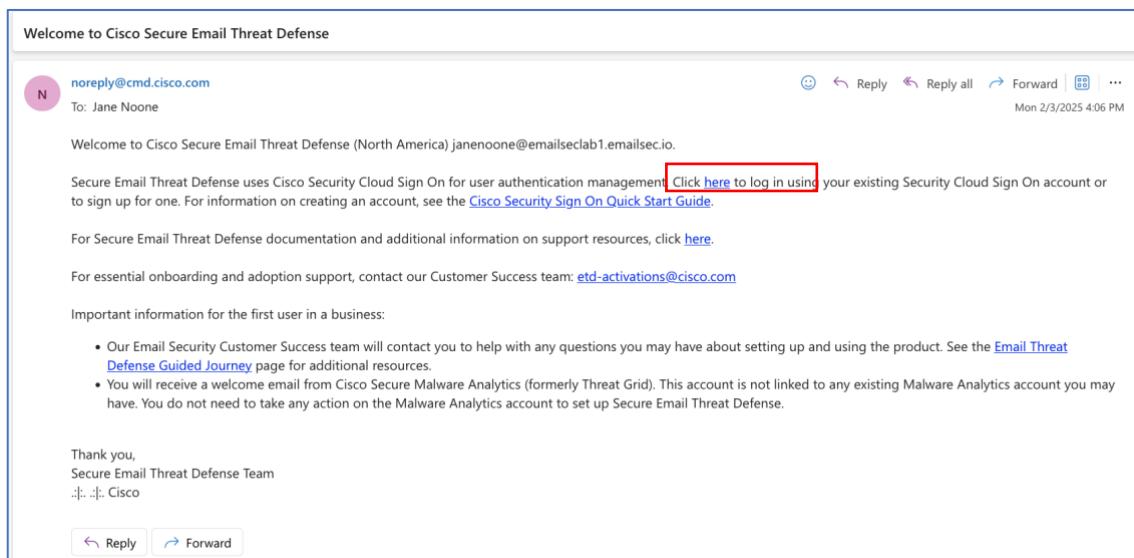
Administrator 1: [janenoone@emailseclabXX.emailsec.io](mailto:janenoone@emailseclabXX.emailsec.io)

User 2: [marcmarquez@emailseclabXX.emailsec.io](mailto:marcmarquez@emailseclabXX.emailsec.io)

2. Open the inbox, and you will see a “Welcome to Cisco Email Threat Defense” email.



3. Click on the link inside the email (see the picture)



4. For the email address, please use the one you used to log in to O365.  
 Click on [Sign up now](#).

5. For the email address, please use the one given to you by your proctor, choose the correct information, check the "[I agree...](#)" box, and click on "[Sign up](#)"

Email: <a href="mailto:janenoone@emailseclabXX.emailsec.io">janenoone@emailseclabXX.emailsec.io</a> First Name: Jane Last Name: Noone Country: United States Password:	Email: <a href="mailto:marcmarquez@emailseclabXX.emailsec.io">marcmarquez@emailseclabXX.emailsec.io</a> First Name: Marc Last Name: Marquez Country: United States Password:
--	--

## Account Sign Up

Provide following information to create enterprise account.

[Back to login page](#)

Email *	<input type="text" value="janenoone@emailseclab1.emailsec.io"/>
First name *	<input type="text" value="Jane"/>
Last name *	<input type="text" value="Noone"/>
Country *	<input type="text" value="United States"/>
Password *	<input type="password" value="*****"/> <a href="#">Show</a>
Confirm Password *	<input type="password" value="*****"/> <a href="#">Show</a>
<input checked="" type="checkbox"/> I agree to the <a href="#">End user license agreement</a> and <a href="#">Privacy statement</a> .	
<input type="button" value="Sign up"/>	
<a href="#">Cancel</a>	

**Password Requirements**

- ✓ At least 8 character(s)
- ✓ At least 1 number(s)
- ✓ At least 1 symbol(s)
- ✓ At least 1 lowercase letter(s)
- ✓ At least 1 uppercase letter(s)
- ✓ Does not contain part of username
- ✓ Does not contain 'First name'
- ✓ Does not contain 'Last name'



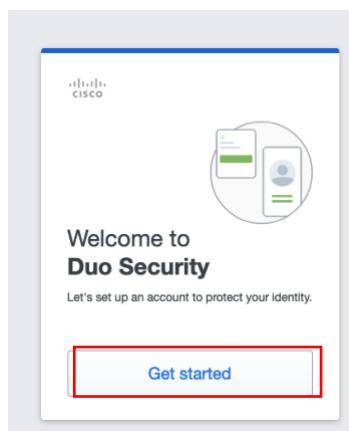
6. You should expect this screen:



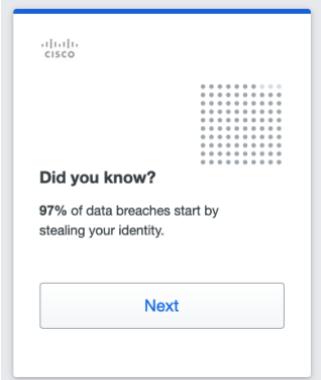
7. Go back to your administrator mailbox in O365: <https://outlook.office.com/mail/>  
8. Open the new message and press "Activate Account."



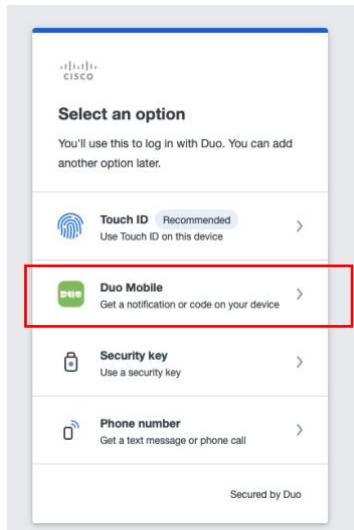
9. By default, you need to set up MFA when creating an ETD account. Press the "**Get started**" button:



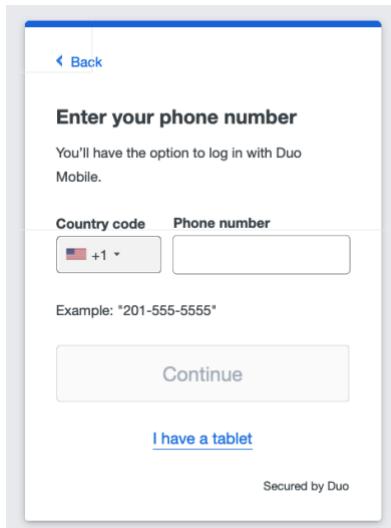
10. Click on **Next**.



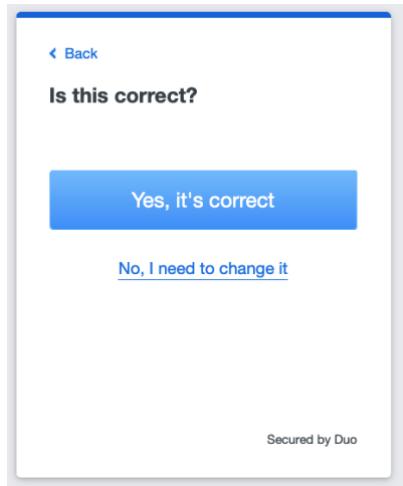
11. Press the "**Duo Mobile**" button.



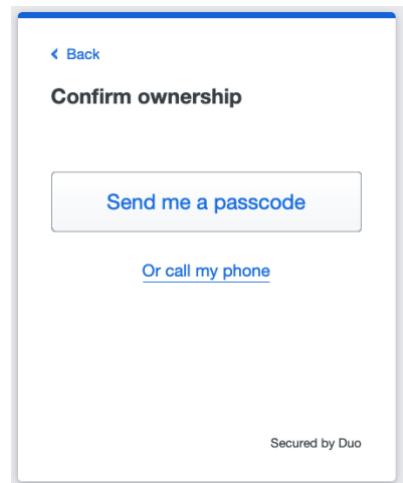
12. Introduce your phone number and press **Continue**.



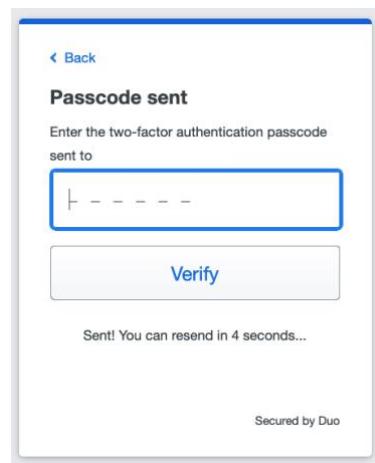
13. Verify the number and press ***Yes, it's correct.***



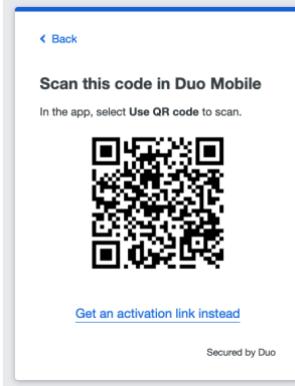
14. Now, click on "Send me a passcode" to confirm that you are the owner.



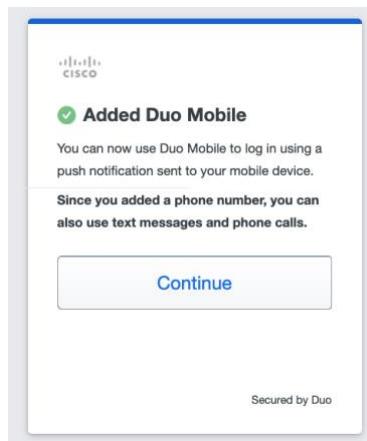
15. Introduce the code and press ***Verify***.



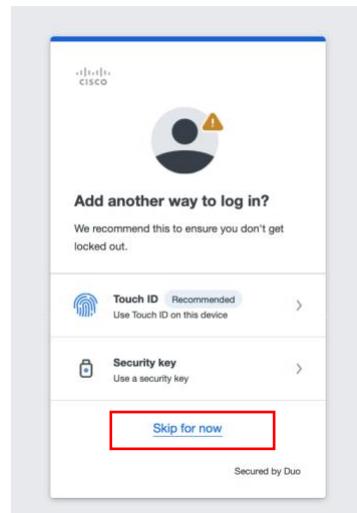
16. Open DUO or the camera to scan the QR code presented on the web page.



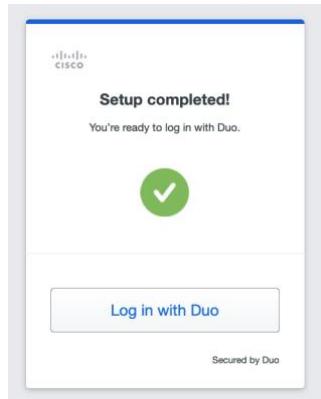
17. If you have DUO installed, you will see this image. For the ones that need to be installed, follow the steps presented in the browser.



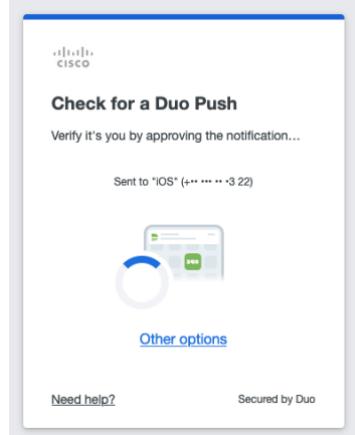
18. Press **Continue**  
19. Click on **Skip for now**.



20. Now, you can log in with Duo MFA. Click on [Log in with Duo](#)



21. Approved the push in your phone and click on [Finish](#)

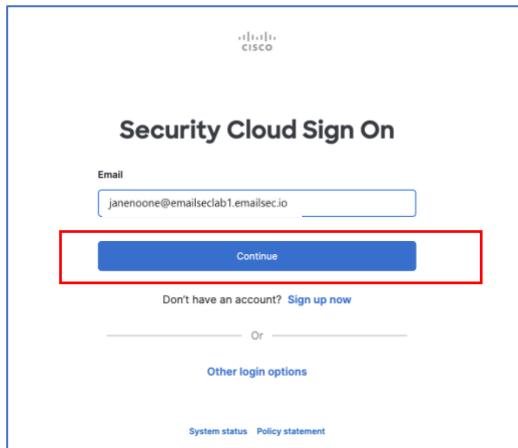


22. Please close the current window, open a new tab, and connect directly with <https://beta-ui.cmd.cisco.com/login>

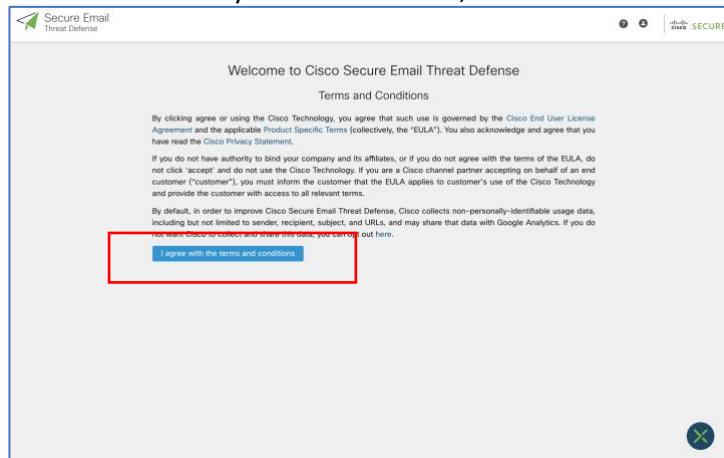
This step is required because we are using the beta environment.

This step needs to be done by one Administrator only

23. Introduce the email address provided by the proctor and used to activate the service.  
Click on [Continue](#).



24. You should now be at the ETD interface. If you see this screen, click on the button with "I agree.."



### Lesson learned.

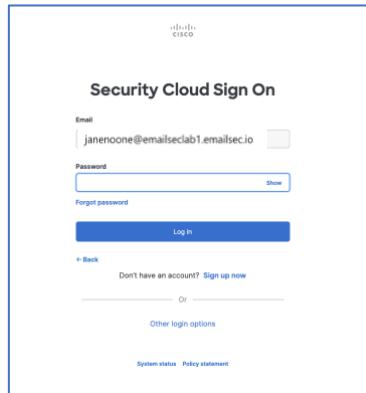
In this task, we have seen how to activate an Email Threat Defense account. This will be common for all types of deployments, although in today's lab, we will integrate it with O365.

The steps are simple and will always be executed with our client's account.

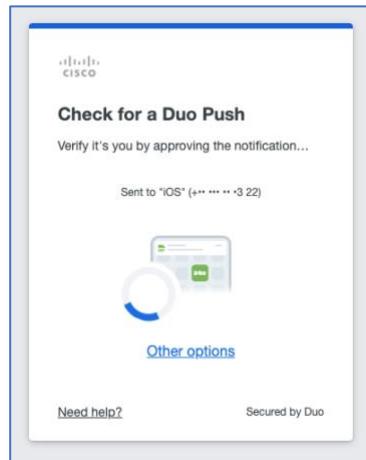
## Task – Configure Email Threat Defense account.

The steps we are going to see below are not the usual steps when deploying ETD.  
This is because we are using an already partially configured BETA environment.

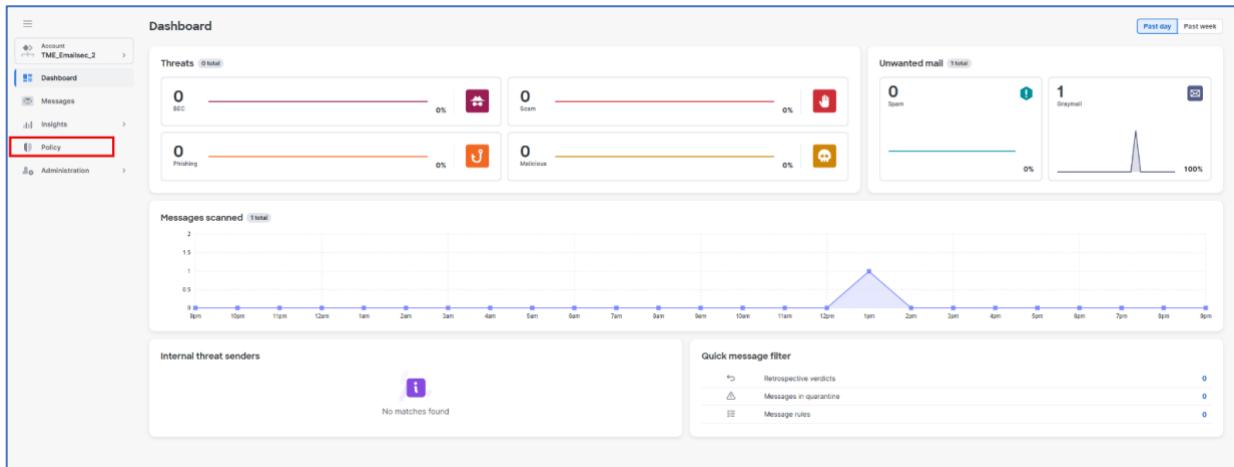
1. Log in again to the beta portal: <https://beta-ui.cmd.cisco.com/login>



2. Accept the push from DUO on your mobile.



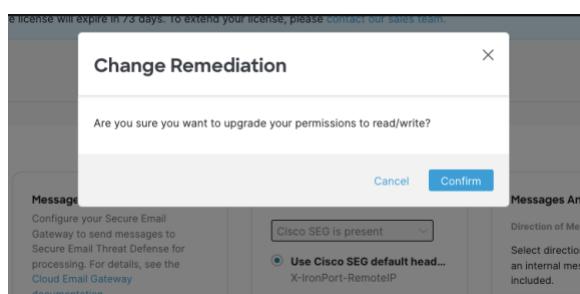
3. As we mentioned at the beginning, these are not the usual steps.  
Click on **Policy**



4. The Email Threat Defense account you have access to is already activated to work with a gateway with no integration with O365. We need to connect with O365 and to do this, we need to move from Gateway/No auth to Microsoft 365/Read-Write.

Click on **Read/Write** and after click on **Microsoft 365**

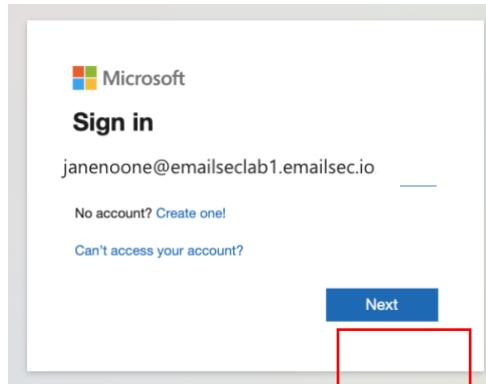
5. Click on **Confirm**.



6. Let's start the integration with MS365. We need to use the MS365 account provided:

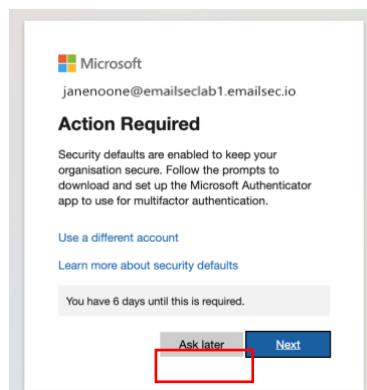
[janenoone@emailseclabXX.emailsec.io](mailto:janenoone@emailseclabXX.emailsec.io)

Click on **Next**

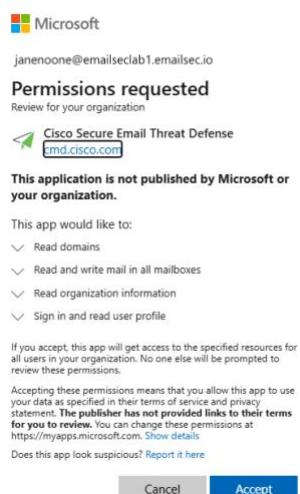


7. After the password, a new window will appear, asking to move to enable MFA.

Click on **Ask Later**.



8. Click on **Accept**.



## Lesson learned.

After activating Email Threat Defense, as in the first task, we made the first connection between Cisco Email Threat Defense and MS365.

This connection will still need to analyze the mail. We have activated the ability of Cisco Email Threat Defense to clean the mailboxes, in addition to having decided how we wanted to integrate it.



## Configure Cisco Secure Email Threat Defense Policy

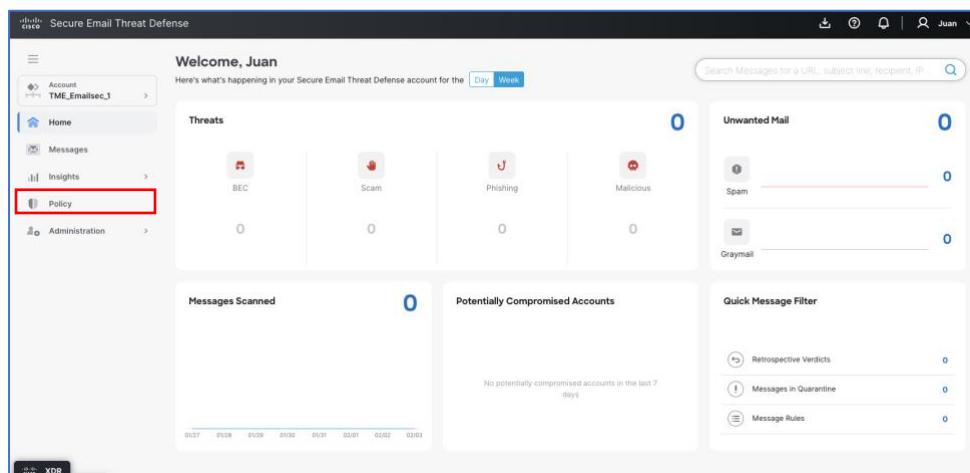
Depending on the customer scenario, we may need to adjust which features are enabled.

If the customer has a Cisco Secure Gateway (on-prem or cloud), we should leave SPAM and Graymail disabled. In this case, we will enable all the analysis modules.

If you want to learn more:

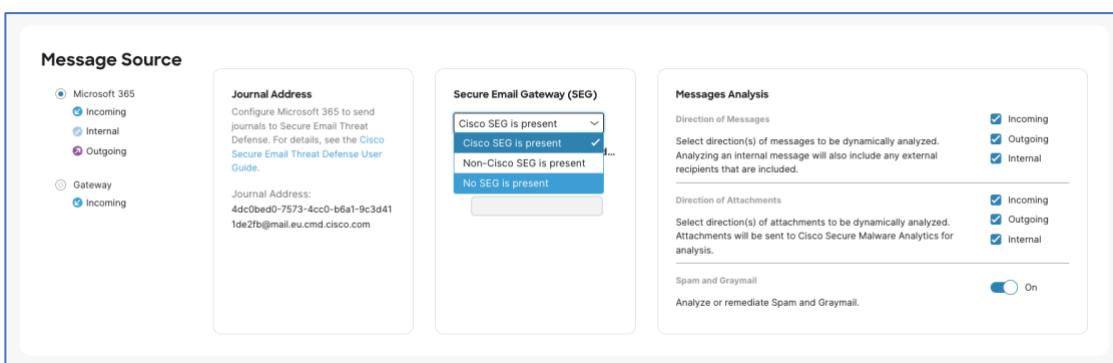
<https://www.cisco.com/c/en/us/td/docs/security/email-threat-defense/user-guide/secure-email-threat-defense-user-guide/policy.html>

1. On the Cisco Secure Email Threat Defense console, click on **Policy**:



2. Select “**No SEG is present**”

In this lab we don't have any security gateway in front of O365.



**Message Source**

Microsoft 365  
 Incoming  
 Internal  
 Outgoing

Gateway  
 Incoming

**Journal Address**  
Configure Microsoft 365 to send journals to Secure Email Threat Defense. For details, see the [Cisco Secure Email Threat Defense User Guide](#).  
Journal Address:  
4dc0bed0-7573-4cc0-b6a1-9c3d41  
1de2fb@mail.eu.cmd.cisco.com

**Secure Email Gateway (SEG)**

Cisco SEG is present  
Cisco SEG is present  
Non-Cisco SEG is present  
No SEG is present

**Messages Analysis**

**Direction of Messages**  
Select direction(s) of messages to be dynamically analyzed. Analyzing an internal message will also include any external recipients that are included.  
 Incoming  
 Outgoing  
 Internal

**Direction of Attachments**  
Select direction(s) of attachments to be dynamically analyzed. Attachments will be sent to Cisco Secure Malware Analytics for analysis.  
 Incoming  
 Outgoing  
 Internal

**Spam and Graymail**  
Analyze or remediate Spam and Graymail.  
 On

3. Enable “**Spam and Graymail**” and all the options.

**Messages Analysis**

**Direction of Messages**

Select direction(s) of messages to be dynamically analyzed. Analyzing an internal message will also include any external recipients that are included.

**Direction of Attachments**

Select direction(s) of attachments to be dynamically analyzed. Attachments will be sent to Cisco Secure Malware Analytics for analysis.

**Spam and Graymail**

Analyze or remediate Spam and Graymail.

Incoming  
 Outgoing  
 Internal

Incoming  
 Outgoing  
 Internal

On

- We will keep all the Automated Remediation actions disabled. For POV/POC scenarios, you should enable this feature after a couple of weeks, because the AI/ML engines already learned from the customer mail flow.

**Automated Remediation Policy**  Off

These actions apply to all selected domains.

Threat Category	Description	Action
Threats	Threats include messages flagged as Business Email Compromise (BEC), Scam, Malicious, or Phishing.	Move to Quarantine
Spam	Spam includes messages with unwanted content, including undesirable URLs.	Move to Junk
Graymail	Graymail is mail that has been determined to be marketing, social, or junk.	No Action

Do not remediate Microsoft Safe Sender messages with Spam or Graymail verdicts.

- Click on **Save and Apply**.

**Secure Email Threat Defense**

**Policy: TME\_Emailsec\_2**

**Message Source**

- Microsoft 365
  - Incoming
  - Outgoing
  - Internal
- Custom Journal
  - Incoming
  - Outgoing
  - Internal
- Custom
  - Incoming
  - Outgoing
  - Internal

**Secure Email Gateway (SEG)**

- No SEG is present
- Use Cisco 360 default header
- Use Custom SEG header

**Messages Analysis**

**Direction of Messages**

Select direction(s) of messages to be dynamically analyzed. Analyzing an internal message will also include any external recipients that are included.

**Direction of Attachments**

Select direction(s) of attachments to be dynamically analyzed. Attachments will be sent to Cisco Secure Malware Analytics for analysis.

**Spam and Graymail**

Analyze or remediate Spam and Graymail.

Incoming  
 Outgoing  
 Internal

Incoming  
 Outgoing  
 Internal

On

**Automated Remediation Policy**  Off

These actions apply to all selected domains.

Threat Category	Description	Action
Threats	Threats include messages flagged as Business Email Compromise (BEC), Scam, Malicious, or Phishing.	Move to Quarantine
Spam	Spam includes messages with unwanted content, including undesirable URLs.	Move to Junk
Graymail	Graymail is mail that has been determined to be marketing, social, or junk.	No Action

Do not remediate Microsoft Safe Sender messages with Spam or Graymail verdicts.

**Visibility & Remediation**

**Microsoft 365 Authentication**

- Assess
  - Identity
  - Delivery
  - Auto-remediation
  - Delivery
  - File Download
- Read
  - Identity
  - Delivery
  - File Download
  - CMS Download

**Imported domains** (0 auto-enrolled, 9 total)

Apply Auto-remediation to all domains

**Automated Remediation Policy**  Off

These actions apply to all selected domains.

Threat Category	Description	Action
Threats	Threats include messages flagged as Business Email Compromise (BEC), Scam, Malicious, or Phishing.	Move to Quarantine
Spam	Spam includes messages with unwanted content, including undesirable URLs.	Move to Junk
Graymail	Graymail is mail that has been determined to be marketing, social, or junk.	No Action

Do not remediate Microsoft Safe Sender messages with Spam or Graymail verdicts.

## Lesson learned.

It is essential to understand this task that we have done now.

Before managing traffic, we must configure a policy in our Email Threat Defense account. If we do not do this, we may have unexpected behavior since it could be deleting emails we do not want to delete.

Therefore, before carrying out the next task, we must have the policy we want to implement configured. In most cases, this will have a monitor mode configuration.



## Task – Configure Exchange Online.

In this task, we will configure Exchange Online and review the permissions automatically configured in the previous step.

- Now we need to go to the Purview Microsoft Admin center and configure the journaling rule.

<https://purview.microsoft.com/>

Microsoft updates the console from time to time. In this case, you can see either the legacy portal or the new Purview portal.

The configuration presented here is for the new Purview console.

Click on **Solutions** and then in **Data Lifecycle Management**.

The screenshot shows the Microsoft Purview Admin Center interface. On the left, there is a sidebar with the following navigation options:

- Home
- Solutions** (highlighted with a red box)
- Learn
- Settings
- Data Lifecycle Management... (highlighted with a red box)

The main content area is titled "Account overview". It displays the tenant name "emailseclab4". Below this, there is a list of solutions:

- Audit
- Communication Compliance
- Compliance Manager
- Data Lifecycle Management** (highlighted with a red box)
- eDiscovery
- Information Barriers
- Information Protection
- Insider Risk Management
- Records Management

At the bottom of the sidebar, there is a section titled "Related portals" with links to:

- Microsoft Defender
- Microsoft Entra
- Microsoft Fabric
- Microsoft Priva
- Microsoft Service Trust

- Click in **Settings** and **Data Lifecycle management** and then **Exchange (legacy)**.

The screenshot shows the Microsoft Purview interface. On the left, there's a sidebar with various options like Home, Settings, Solutions, Learn, Roles and scopes, Data connectors, Device onboarding, Optical character recognition (OCR), and several compliance-related items. A red box highlights the 'Settings' icon. Below it, under 'Solution settings', another red box highlights 'Data Lifecycle Management'. On the right, the main content area is titled 'Data Lifecycle Manager' and shows 'Adaptive protection' with a sub-section for 'Exchange (legacy)', which is also highlighted with a red box.

- Click on **Replace**. Before configuring the Journaling rule, you must indicate an email address to receive Undeliverable Reports. Please note that in a production environment, this step may already have been completed by the client.

This screenshot shows the 'Data Lifecycle Management settings' page. It has a tab for 'Adaptive protection' where 'Exchange (legacy)' is selected. In the 'Undeliverable reports' section, it says: 'Specify an email address to receive journal reports when they are not deliverable to the address specified in the journal rule. This email address can't correspond with an Exchange Online mailbox.' Below that, it says 'Send undeliverable journal reports to:' followed by the email address 'admin@inline.emailseclab20.emailsec.io'. At the bottom of this section is a red-bordered 'Replace' button.

In the new Microsoft Purview console verify the email address, if the email address is not present, please add it.  
[admin@inline.emailseclab20.emailsec.io](mailto:admin@inline.emailseclab20.emailsec.io)

4. Click on “[Data Lifecycle management](#)”:

5. Click on “[Exchange Legacy](#)” and on “[journal Rules](#)”.

If you see a rule created, please select and remove it.



6. Click on “**New Rule**”

The screenshot shows the Microsoft Purview Data Lifecycle Management interface. On the left, there's a navigation sidebar with options like Home, Data Lifecycle Management (which is selected), Overview, Retention labels, Policies, Import, Exchange (legacy), Journal rules (which is also selected), and Classifiers. The main area is titled "Journal rules". It contains a message about journaling content outside Microsoft 365. Below that, it says "Use journal rules to record all communications in support of your organization's email retention or archival strategy. Learn about journaling in Exchange Online". There's a button labeled "+ New rule" with a red box around it. A "refresh" button is next to it. To the right, there's a search bar, a status filter, and a "Send journal reports to" button. The table below shows one row with "No data available".

7. Before to fill the rule information, we need to get the journaling email address. Go back to Cisco Secure Email Threat Defense. Open **Settings → Administration**  
Copy the **Journal Address**.

The screenshot shows the Cisco Secure Email Threat Defense administration interface. The left sidebar includes Account (Motofan100), Home, Messages, Insights, Policy, and Administration (which is selected). The main area has tabs for Business, Users, and API Clients. Under Business, there are sections for Users, API Clients, Message Rules, and High Impact Personnel. The "High Impact Personnel" section shows a table with three rows. The first row has the value "37@beta.cmd.cisco.com" in the "Journal Address" column. To the right, there's a "License" section with fields for Type (standard), Seat Count (16), Start Date (Sep 27 2023), and End Date (Jul 27 2024). The "Journal Address" field is highlighted with a red box.

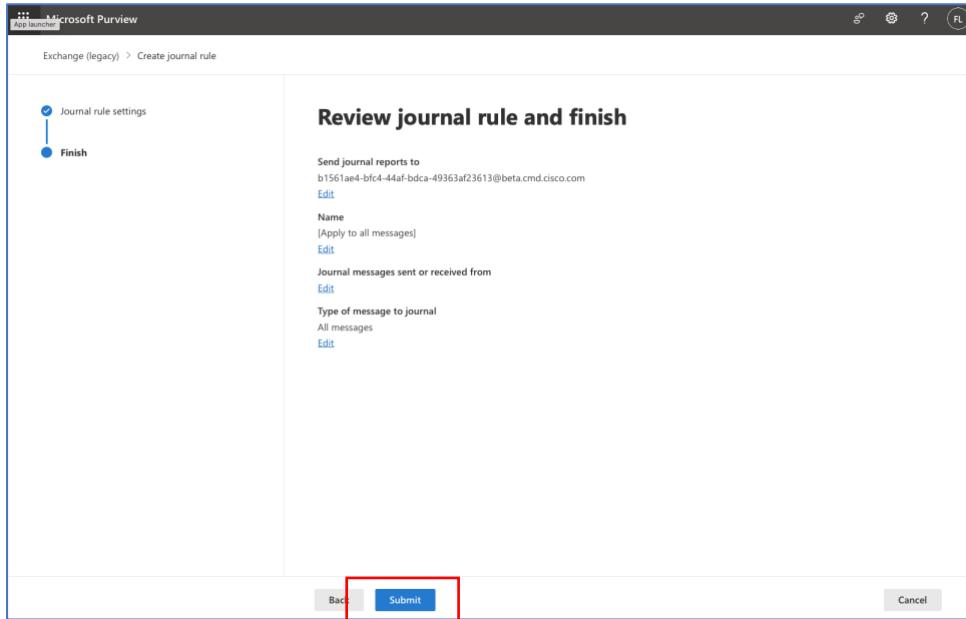


8. Now in the O365 window, fill all the data. Add a rule name, copy the journal address, and choose **Everyone** and **"All Messages"**. (Name should be the last box to fill).

Click on "**Next**":

9. Click on "**Submit**"

This is the most crucial step. All traffic will be sent to Email Threat Defense when you press the submit button. Since we are in a lab, we will not see anything. In a production environment, messages will be sent to ETD immediately, so we must ensure we have the correct policy settings before clicking the Submit button.



10. You should see this screen:



This concludes the ETD and Microsoft integration scenario.

#### Connector in O365 for ETD traffic.

In some environments, with secure gateways, Exchange on-premises devices, etc., more connectors will be configured. If this happens, it's important that the traffic delivered to ETD goes through one of these platforms without being stopped or delayed. Creating a connector for this traffic will force O365 to send this traffic directly to ETD.

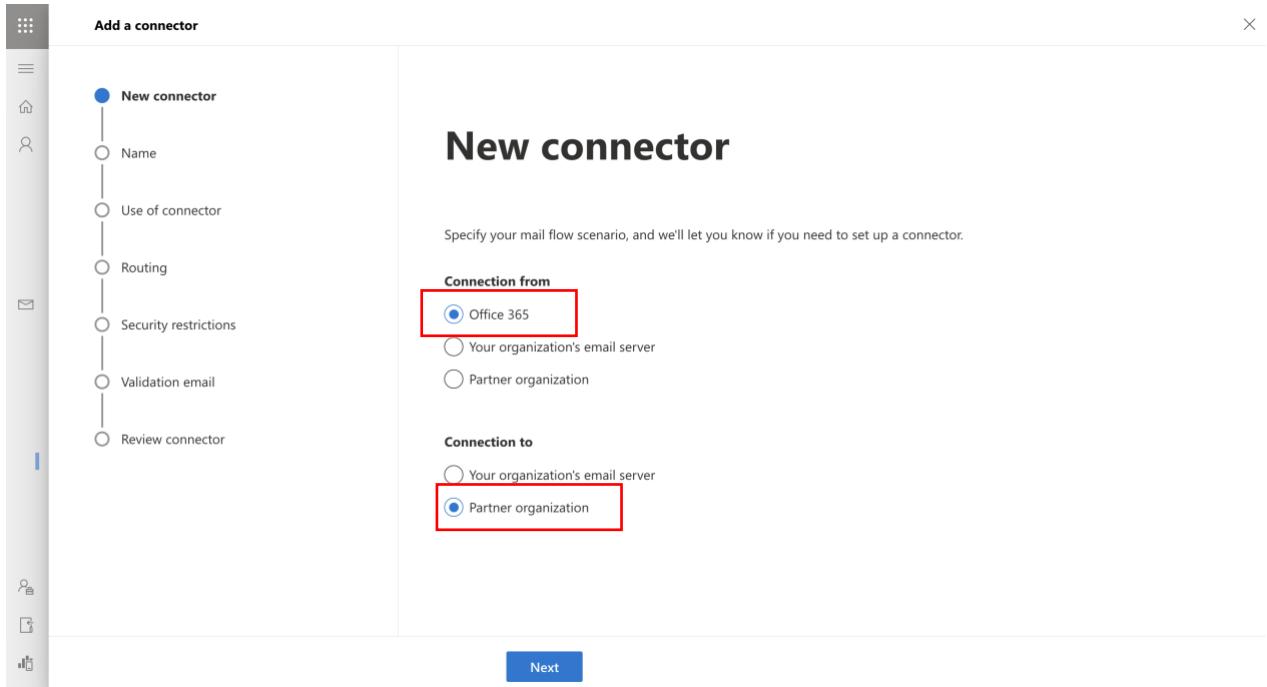
1. Open Exchange Online administration console at <https://admin.exchange.microsoft.com/>
2. Click on “**Mail Flow**” and “**Connectors**”.

The screenshot shows the Exchange admin center interface. The left sidebar is collapsed. The main area displays a "Mail flow" card titled "0 auto-forwarded messages". Below the title, it says "Shows messages that were automatically forwarded from your Microsoft cloud org to recipients in external domains. Last 7 days, updated 12:44 pm today." To the right of the card is a "Training & guides" section with two items: "Training for admins" (Exchange admin center video tutorial) and "Documentation" (Learn to use the Exchange admin center). At the bottom of the page, there are links for "Mail flow" and "Mailboxes", and a "Manage email forwarding" button.

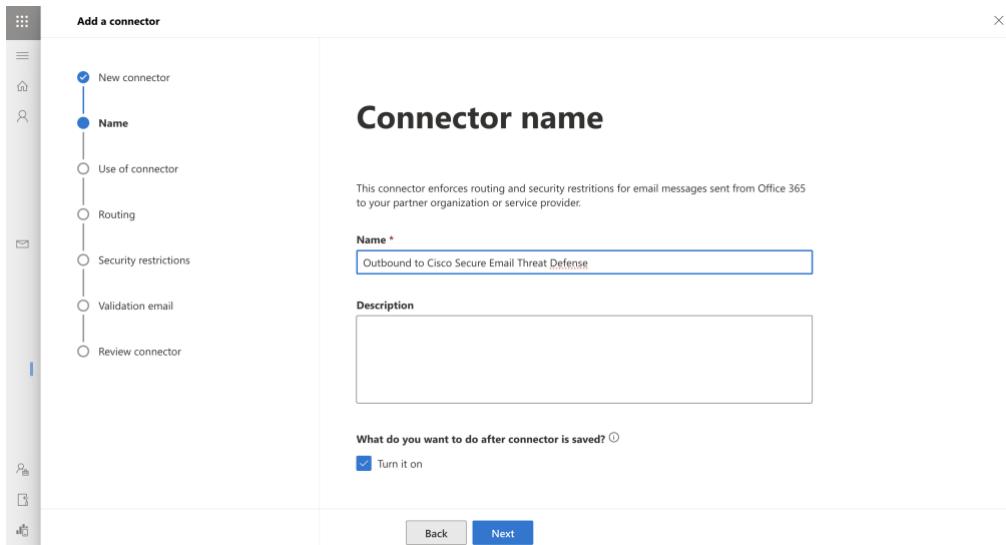
3. Click on “[Add a connector](#)”.

The screenshot shows the Exchange admin center interface. The left sidebar is collapsed. The main area displays a "Connectors" card with the heading "Connectors". Below the heading, it says "Connectors help control the flow of email messages to and from your Office 365 organization. We recommend that you [check to see if you should create a connector](#), since most organizations don't need to use them." At the top of the connector list, there is a red box around the "+ Add a connector" button. The connector list table has columns for Status, Name, From, and To. A message at the bottom of the list says "No data available". On the far right, there is a search bar and a filter icon.

4. Select Connection From “[Office 365](#)” and Connection to “[Partner Organization](#)” and click [Next](#)



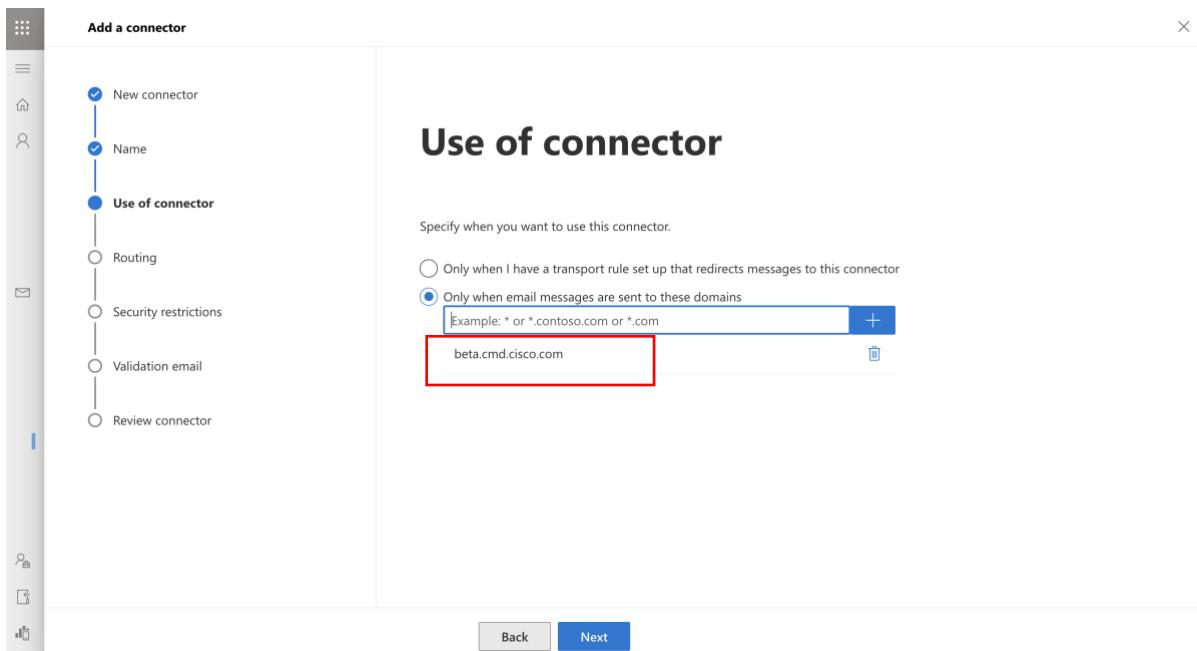
5. Write a name, in our case we can use "***Outbound to Cisco Secure Email Threat Defense***" and click **Next**.



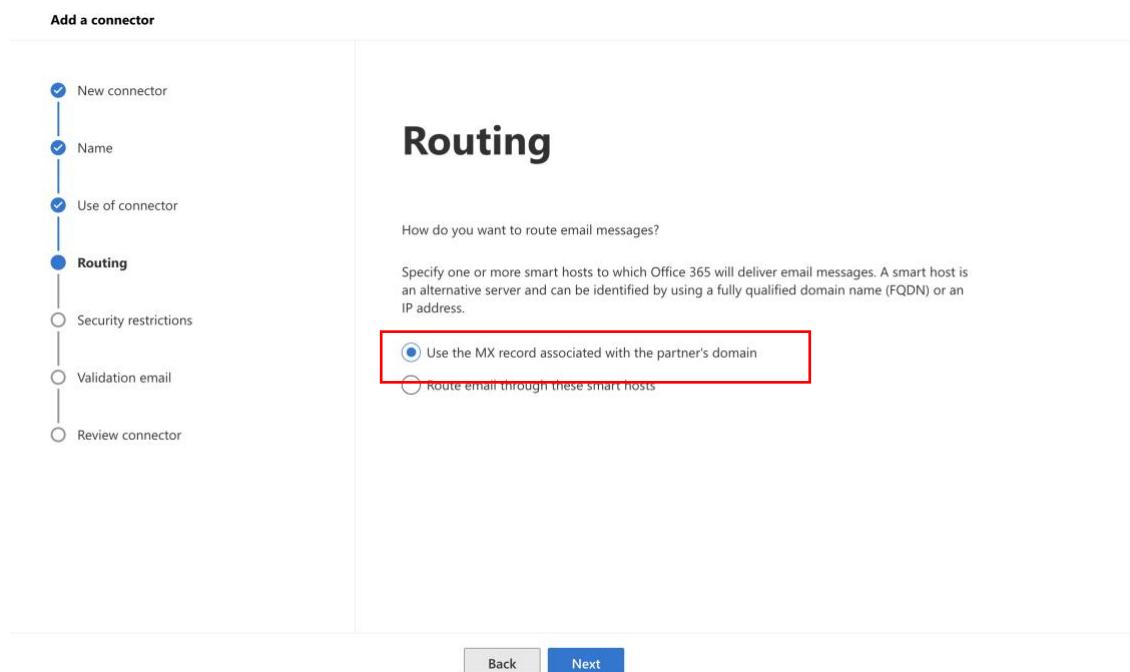
6. Write the domain that is in your journaling email address. In this lab the domain is "***beta.cmd.cisco.com***"

Click on **+**





7. Click on **Next**
8. Select "**Use the MX record associated with the partner's domain**" and click on **Next**



9. Select "**Always use Transport Layer Security (TLS) to secure the connection (recommended); Issued by a trusted certificate authority (CA)**" and Click on **Next**

10. Copy the journaling address to validate the connector. Click on “[Validate](#)”

**Note:** The connector validation may fail if your O365 tenant is already configured with conditional mail routing using an Exchange transport rule to route outbound mail to an existing connector. While journal messages are system-privileged and are not affected by transport rules, the connector validation test email is not privileged and is affected by transport rules.

Validation process takes some time to perform and not always is successful. If everything works you will see something like the picture below.



The screenshot shows a validation message in a web-based interface. At the top, there is a header with the email address "a24t1c54-c154-4uc4-9a30-deab0852ze20@beta.cmd.cisco.com" and a small icon. Below the header is a button labeled "Validate". A green success message box contains the text "Validation successful" with a checkmark icon. Underneath the message is a table with two columns: "Task" and "Status". The table has two rows: "Send test email" with status "Succeed".

Task	Status
Send test email	Succeed

11. Click on “[Create Connector](#)”

The screenshot shows the "Review connector" page. On the left, a vertical navigation bar lists steps: "New connector", "Name", "Use of connector", "Routing", "Security restrictions", "Validation email", and "Review connector". The "Review connector" step is highlighted with a blue circle. The main content area is titled "Review connector". It includes sections for "Mail flow scenario" (From: Office 365, To: Partner organization), "Name" (Outbound to Cisco Secure Email Threat Defense), "Status" (Turn it on after saving, with a "Edit name" link), "Use of connector" (Use only for email sent to these domains: beta.cmd.cisco.com, with a "Edit use" link), "Routing" (Use the MX record associated with the partner's domain, with a "Edit routing" link), and "Security restrictions". At the bottom right, there are "Back" and "Create connector" buttons, with "Create connector" being highlighted by a red box.

### Lesson learned.

We have already finished the integration between ETD and O365 in both directions.  
The next step is to verify the operation and carry out tests.



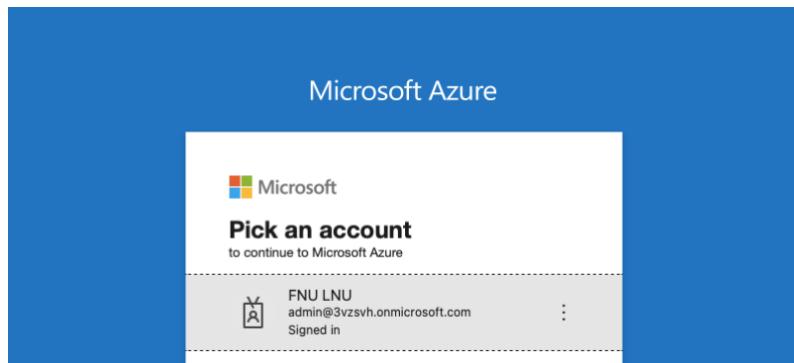
## Task –Review the permissions assigned in Microsoft (optional)

Frequently, customers ask about the permissions required to integrate ETD with Microsoft to be able to use the Read-Write mode on ETD.

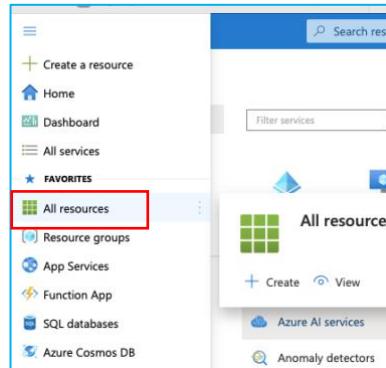
Let's see what Microsoft permissions are assigned to Cisco ETD.

1. Open the Azure portal with the O365 account provided for this lab:

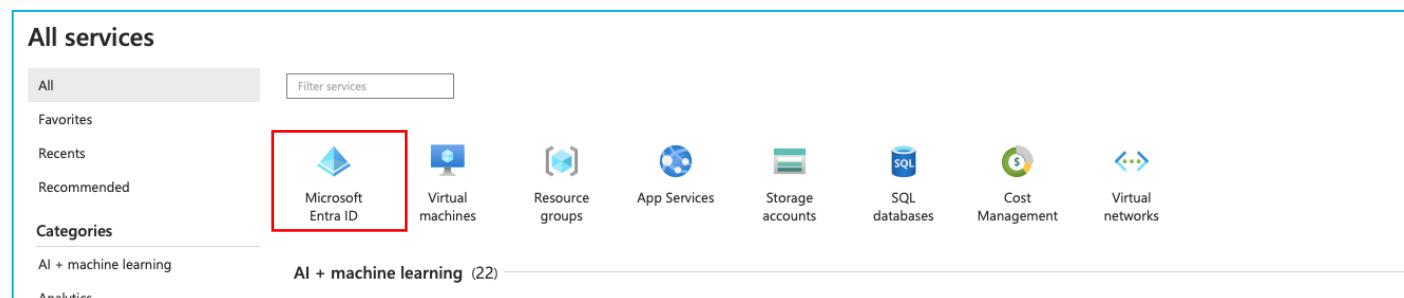
<https://azure.microsoft.com/en-us/get-started/azure-portal/>



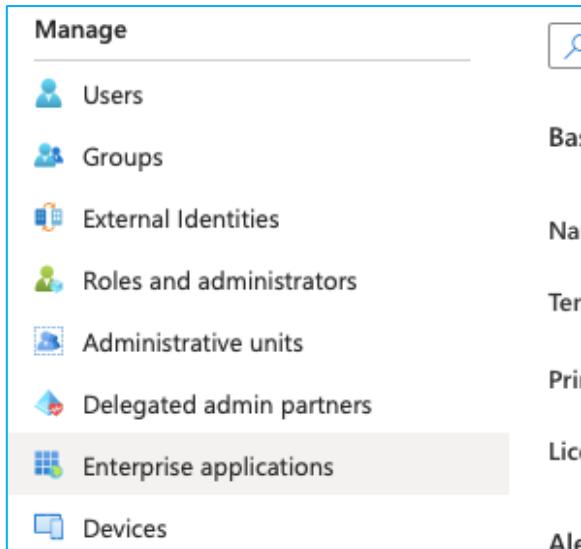
2. Click on "**All resources**"



3. Click on "**Microsoft Entra ID**".



4. Click on “Enterprise Applications”.



5. If the integration is correct, you will see an entry with the name “Cisco Secure Email...”

The screenshot shows the 'Enterprise applications | All applications' page. The left sidebar includes sections for 'Overview', 'Manage' (with 'All applications' selected), and 'Security'. The main area displays a table with one application entry:

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry St...	Active Certificate Ex...	Identifier URI (Entity...
Cisco Secure Email...	f657ceea-48f8-47df-aae...	23b06408-7389-43a1-a9...	https://portal.cmd.cisco....	20/09/2023	-	-	23b06408-7389-43a1-a9...

A red box highlights the 'Cisco Secure Email...' entry in the table.

6. Click on Permissions

- If you open the application, you can see the permissions assigned.

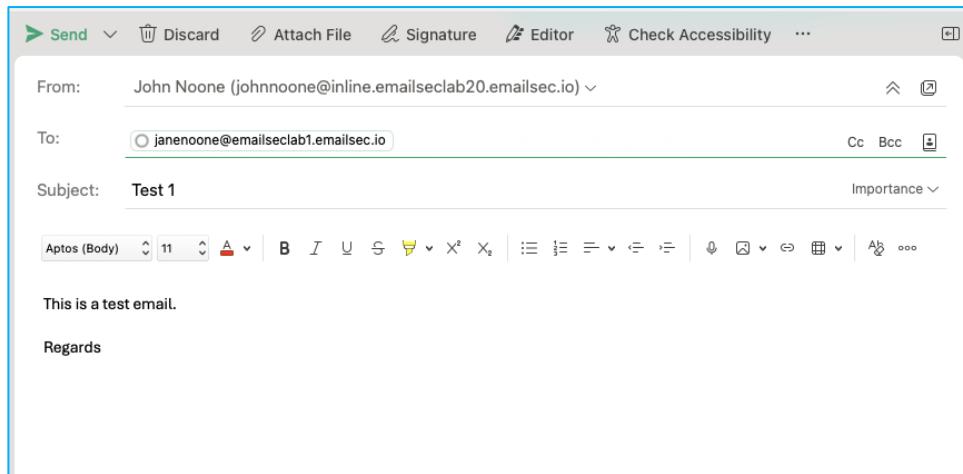
API name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph (3)					
Microsoft Graph	Mail.ReadWrite	Read and write mail in all mailboxes	Application	Admin consent	An administrator
Microsoft Graph	Domain.Read.All	Read domains	Application	Admin consent	An administrator
Microsoft Graph	Organization.Read.All	Read organization information	Application	Admin consent	An administrator



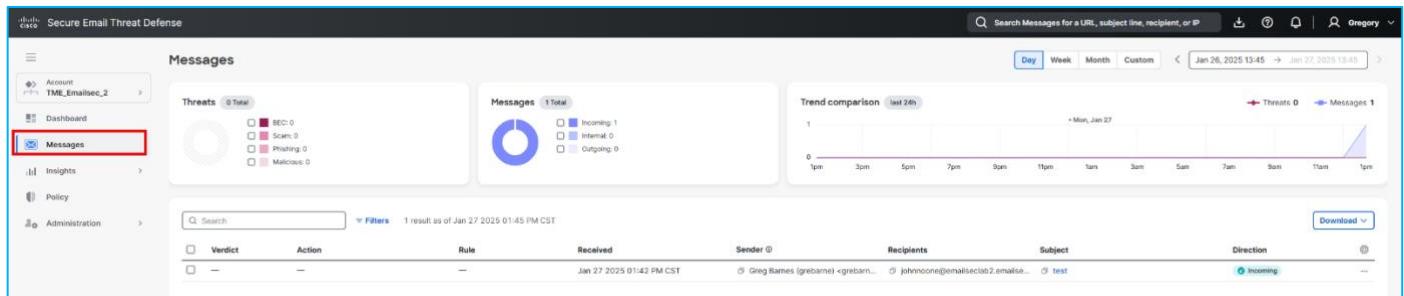
## Task – Test the solution.

To continue this lab, you are going to generate email traffic. Since the account is valid, you can send emails from your own business or personal account, and you see how it appears in the ETD admin interface. You will test all the options to verify that everything is working as expected.

1. Open your Email client and send an email to the account created in Exchange Online. Something like [janenoone@emailseclabXX.emailsec.io](mailto:janenoone@emailseclabXX.emailsec.io) (Please use your admin user and pod number)

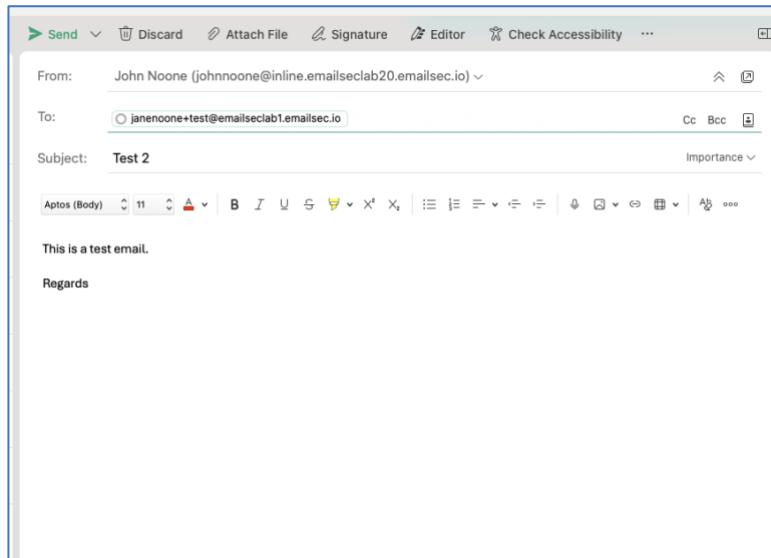


2. In the Email Threat Defense dashboard, on the **Messages tab**, you will see information about the email you just sent:



Verdict	Action	Rule	Received	Sender	Recipients	Subject	Direction
—	—	—	Jan 27 2025 01:42 PM CST	Greg Barnes (ggregb...)	janenoone@emailseclab20.emailsec...	test	Incoming

3. Using your business or any other email account, send an email to [janenoone+test@emailseclabXX.emailsec.io](mailto:janenoone+test@emailseclabXX.emailsec.io) or "[marcmarquez+test@emailseclabXX.emailsec.io](mailto:marcmarquez+test@emailseclabXX.emailsec.io)". (Please use your pod number)



4. You should see something like this in your ETD console.

5. Open both messages and compare the “Delivered To” field.

As you can see, both messages arrived in the same mailbox. “Delivered To” means who is the destination (final Mailbox). Many times, we will see “To”, “Envelope To” and “Delivered To” totally different. This happens when email is going to a Distribution List, Alias, BCC, etc.

ETD allows you to understand exactly where the email was sent to and who received it.

- If you want to confirm that both messages were delivered to the same destination, please open Outlook for your O365 admin user by clicking on <https://outlook.office.com/mail/>

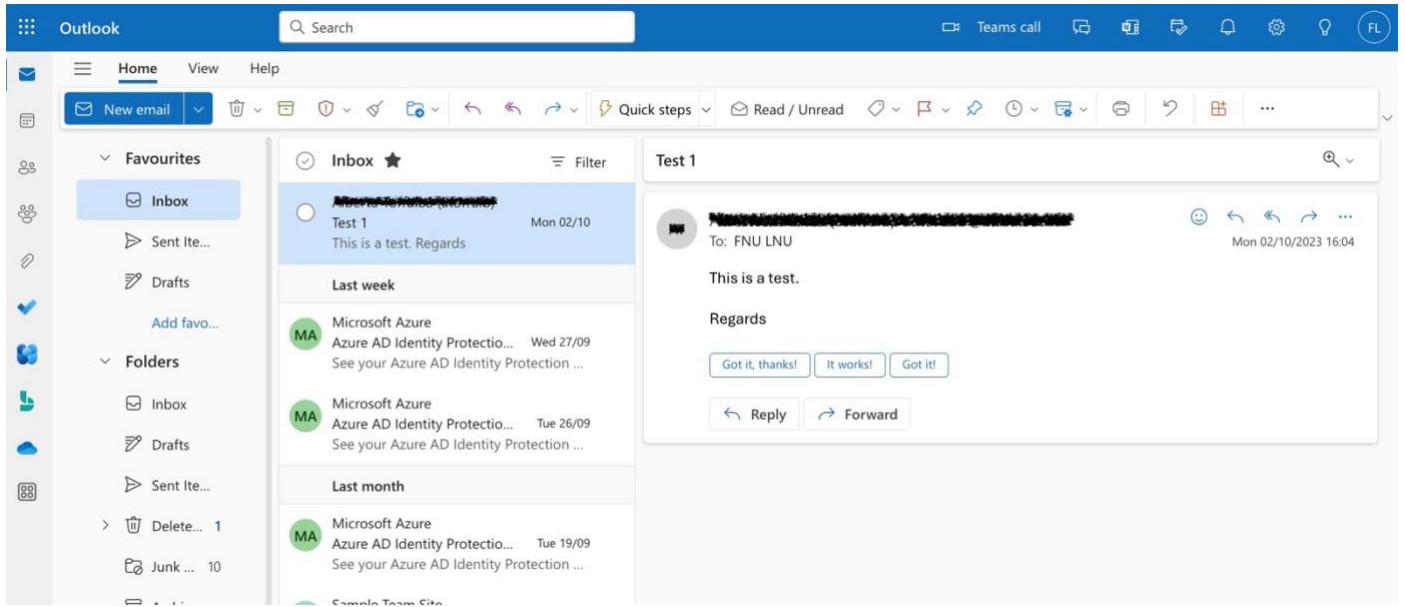
You should have these two emails.

The screenshot shows the Microsoft Outlook inbox interface. On the left, there's a sidebar with 'Favourites' (Inbox, Sent Items, Drafts) and 'Folders' (Inbox, Drafts, Sent Items, Junk E..., Archive, Notes, Conversations, Create new...). The main pane displays the 'Inbox' folder with two messages. The top message is from 'TEST 2' with subject 'this is a test.' and body 'This is a test.' The bottom message is from 'Test 1' with subject 'This is a test. Regards' and body 'This is a test. Regards'. To the right of the inbox, a preview pane shows the details of the selected message ('Test 1'). Below the inbox, sections for 'Last week' and 'Last month' show other messages from Microsoft Azure and a sample team site.

- Go back to the ETD dashboard, and on the Messages tab, please select one of the messages and remove the email. Select “Keep Verdict” and “Move to Junk”. Then click “Update”.

The screenshot shows the ETD (Email Threat Defense) dashboard. At the top, there's a search bar, a filters section, and a download button. Below that, a toolbar has 'Message selected' and 'Reclassify' buttons, with dropdown menus for 'Keep verdict' (highlighted with a red box) and 'Request action' (highlighted with a red box), both set to 'Move to Junk'. A 'Cancel' and 'Update' button are also present. The main area is a table listing messages. The first message in the list has its 'Verdict' and 'Action' columns checked, while the others are empty. The table includes columns for Verdict, Action, Rule, Received, Sender, Recipients, Subject, Direction, and a more options icon. The first message was received on Jan 27 2025 at 02:13 PM CST from Greg Barnes (grebarn...) to johnnoone+test@emailsec... with subject 'test 3'. The second message was received at 02:03 PM CST with subject 'Test 2'. The third message was received at 01:42 PM CST with subject 'test'.

- Automatically the email should disappear from the user's inbox and appear in the junk folder. Please go back to Outlook and confirm that the message is now in the Junk folder:



This concludes this task, and you may continue to the next one.

### Lesson learned.

In this task, we have carried out several tests and seen how Email Threat Defense displays the information in the console.

We have also conducted a test with an alias to understand what some of the parameters appearing in the console mean.

## Task - High Impact Personnel

Important personnel, such as members of executive leadership teams, are at risk of being impersonated in an attempt to compromise other targets. The high-impact personnel list helps Secure Email Threat Defense defend your organization from impersonation attacks.

Admins can create a list of up to 100 people that is sent to Cisco Talos for higher scrutiny on Display Name and Sender Email Address. Deviations from the configured information for an individual will be identified as a Technique in the Verdict Details panel of convicted messages.

1. Open the Cisco Email Threat Defense console.
2. Click on Administration → High Impact Personnel.

The screenshot shows the Cisco Email Threat Defense interface. On the left, there's a navigation sidebar with 'Administration' selected. Under 'Administration', 'High Impact Personnel' is highlighted with a red box. The main dashboard area has sections for 'Unwanted mail' (0 total), 'Scam' (0, 0%), 'Malicious' (0, 0%), 'Spam' (0, 0%), and 'Graymail' (0, 0%). Below these are two charts: one for 'Unwanted mail' over time and another for 'Quick message filter' with options for Retrospective verdicts, Messages in quarantine, and Message rules. At the bottom, it says 'No matches found'.

3. Click on “**Add New Personnel**”
4. We can add some names. In the list below we have the list of users created by Microsoft by default. Then you can add some of them manually in your environment. Add the users that you have in your environment. (You can see a list below)



**Add New Personnel**

First Name	Last Name	
<input type="text"/>	<input type="text"/>	
Title	Business Phone	Mobile Phone
<input type="text"/>	<input type="text"/>	<input type="text"/>
Email Address <span style="float: right;">0 of 5 max email addresses entered</span>		
Enter multiple email addresses separated by comma  <input type="text"/>		
<input type="button" value="Cancel"/> <input type="button" value="Submit"/>		

First Name	Last Name	Title	Email Address
Jane	Noone	SE Manager	janenoone@emailseclabXX.emailsec.io
Marc	Marquez	SE Director	MarcMarquez@emailseclabXX.emailsec.io

**Exchange admin center**

Home > Mailboxes

## Manage mailboxes

Create and manage settings for shared mailboxes. You can also manage settings for user mailboxes, but to add or delete them you must go to the [Microsoft 365 admin center](#) and do this on the [active users](#) page. [Learn more about mailboxes](#)

[Add a shared mailbox](#) [Mailflow setting](#) [Refresh](#) [Export mailboxes](#)

Display name ↑	Email address	Recipient type
Jane Noone	janenoone@emailseclab2.emailsec.io	UserMailbox
Marc Marquez	marcmarquez@emailseclab2.emailsec.io	UserMailbox

The screenshot shows the 'High Impact Personnel' section of the Cisco Secure Email Threat Defense web interface. The table lists personnel information with the following details:

Impersonations Last 30 Days	First Name	Last Name	Title	Business Phone	Mobile Phone	Email Address	Created By	Date Created	Last Updated By	Date Last Updated	Actions
0	Jane	Noone	SE Manager			janoone@email...	Juan Torralba	Feb 04 2025 10:14 AM GMT+1	Juan Torralba	Feb 04 2025 10:14 AM GMT+1	
0	Marc	Marquez	SE Director			marcmarquez@email...	John Noone	Nov 06 2024 11:46 AM GMT+1	John Noone	Nov 06 2024 11:46 AM GMT+1	

5. Open the web site: <https://emkei.cz/>

The screenshot shows the Emkei's Mailer interface. The form fields include:

- From Name: [Input field]
- From E-mail: [Input field]
- To: [Input field]
- Subject: [Input field]
- Attachment: [Choose file] Choose file No file chosen  
[Attach another file]  
[Advanced Settings]
- Content-Type:  text/plain  text/html  Editor
- Text: [Large text area]
- Captcha: I am human [Privacy + Terms](#)
- Buttons: Send, Clear

At the bottom, it says: © 2009–2023 Emkei • info@emkei.cz

6. Fill the form with this information. (the name must be one of the ones from your list).

From Name: Veronica Stroll

From Email: [Jane@pepe.com](mailto:Jane@pepe.com)

To: [janenoone@emailseclabXX.emailsec.io](mailto:janenoone@emailseclabXX.emailsec.io) or [MarcMarquez@emailseclabXX.emailsec.io](mailto:MarcMarquez@emailseclabXX.emailsec.io) (You must put your O365 email domain).

Content Type: text/html

Subject: This is a test

Body: Hello

# EwE's MAILER

Free online fake mailer with attachments, encryption,  
HTML editor and advanced settings...

**From Name:** Veronica Stroll  
**From E-mail:** veronica@pepe.com  
**To:** johnnoone@pod100.bce-demo.com  
**Subject:** This is a test  
**Attachment:** Choose file No file chosen  
Attach another file  
[Advanced Settings](#)

**Content-Type:**  text/plain  text/html  Editor  
**Text:** This is a test  
Finance  
Veronica

**Captcha:**  
 I am human   
[Privacy - Terms](#)

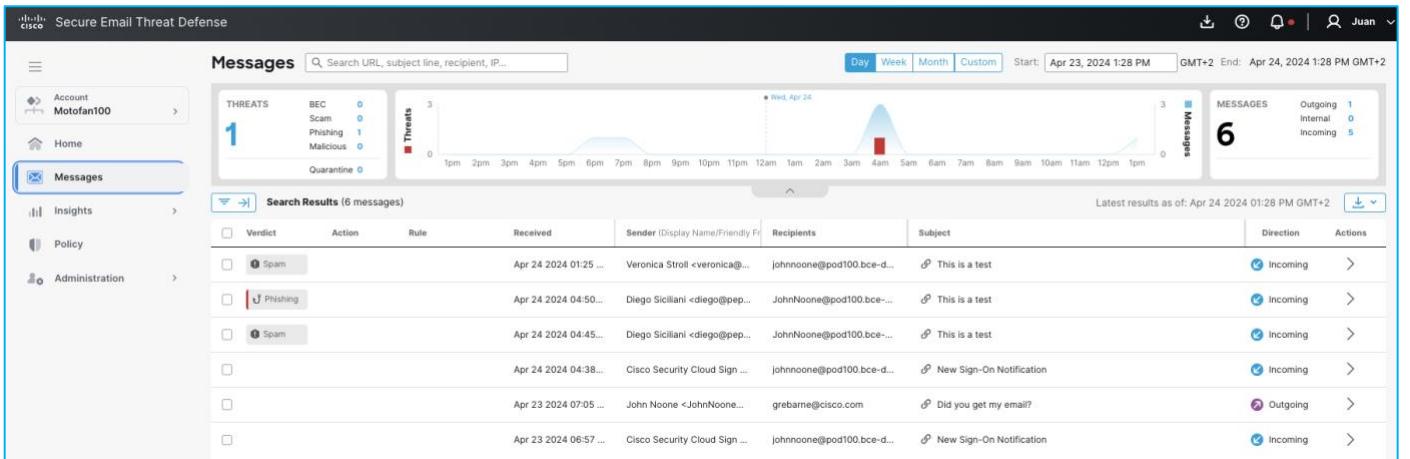
**Send** **Clear**

7. Repeat the same as before but change the body content adding [http://ihaveabadreputation\[.\]com](http://ihaveabadreputation[.]com)

**Content-Type:**  text/plain  text/html  Editor  
**Text:** Hello  
Bla bla bla  
<http://ihaveabadreputation.com>

**Captcha:**  
 I am human 

8. Review If both messages were processed by Cisco Secure Email Threat Defense.



- If you don't see a message processed by Email Threat Defense, then maybe O365 detected as malicious and quarantined it. In this case, open the O365 quarantine and release the email.

Remember that Microsoft will process all the emails before Cisco Secure Email Threat Defense.

<https://security.microsoft.com/quarantine?viewid=Email>

The screenshot shows the Microsoft Defender Quarantine interface. It has a left sidebar with 'Investigation & response', 'Threat intelligence', 'Microsoft Sentinel', 'Email & collaboration', 'Reports', 'Trials', and 'More resources'. The main area is titled 'Quarantine' and shows a list of emails. At the top, there are buttons for 'Refresh', 'Release', 'Approve release', 'Deny', 'Delete messages', 'Preview message', and 'More'. Below that is a filter 'Time received: Last 30 days'. The list contains two entries:

- Apr 24, 2024 1:26:03 PM: This is a test 2 (Sender: veronica@pepe.com, Reason: Malware, Status: Needs review, Policy type: Anti-malware policy, Expires: May 24, 2024 1:26:03 PM, Recipient: johnnoone@pod100.bce-d...)
- Apr 24, 2024 4:47:19 AM: This is a test (Sender: diego@pepe.com, Reason: Malware, Status: Released, Policy type: Anti-malware policy, Expires: May 24, 2024 4:47:19 AM, Recipient: johnnoone@pod100.bce-d...)

To the right of the list, there's a modal window titled 'Release email to recipients inboxes' with options: 'Release to all recipients' (radio button selected), 'Release to one or more of the original recipients of the email', 'Send a copy of this message to other recipients', and 'Submit the message to Microsoft to improve detection (false positive)'. At the bottom of the modal are 'Release message' and 'Cancel' buttons.

- Go back to Cisco Secure Email Threat Defense and Open "**High Impact Personnel**".

The screenshot shows the 'Administration' section of the Cisco Secure Email Threat Defense interface. On the left, there's a navigation sidebar with links for Home, Messages, Insights, Policy, and Administration. The 'Administration' link is currently selected and highlighted in blue. In the main content area, there's a table titled 'Business' under the 'Users' category. A red box highlights the 'High Impact Personnel' dropdown menu, which is currently set to 'High Impact Personnel'. The table lists several personnel entries with columns for First Name, Last Name, Title, Business Phone, Mobile Phone, Email Address, Created By, Date Created, Last Updated By, Date Last Updated, and Actions.

11. You should see a number next to the name, this indicates how many HIP detections have occurred.

The screenshot shows the 'High Impact Personnel' page. The navigation sidebar is identical to the previous one. The main content area has a title 'High Impact Personnel' and a sub-instruction '(2 personnel) - Correct personnel information helps protect against user impersonation attacks. Add up to 100 personnel.' Below this is a table with a red box highlighting the 'Impersonations Last 30 Days' column header. The table lists two personnel entries: Jane Noone (SE Manager) and Marc Marquez (SE Director). Each entry includes columns for First Name, Last Name, Title, Business Phone, Mobile Phone, Email Address, Created By, Date Created, Last Updated By, Date Last Updated, and Actions.

12. Click on Messages and expand the message detected as phishing. You should see a "User Impersonation" technique.

The screenshot shows a detailed view of a message. At the top, it says 'Timeline' and shows a timestamp 'Apr 24 2024 02:16:02 PM'. Below this is a 'Received Incoming' section. The main body is titled 'Verdict & Techniques'. It shows a 'Spam' icon and a 'Remediate & Reclassify' button. A red box highlights a yellow box containing the text 'USER IMPERSONATION'. Below this, another yellow box contains the text 'Detected a possible impersonation for high impact user Veronica Stroll'.



## Task – “Attack” your environment.

### Send Email Threats.

To be able to see ETD detection capabilities, threat messages must be sent to users. For this lab, we have prepared a group of threat messages (around 60) to be sent to users created within the Microsoft E5 dev account.

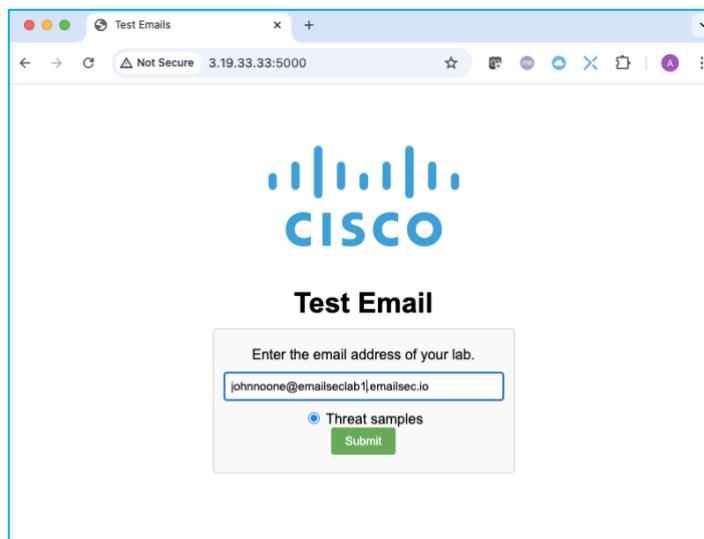
Use this email tool just for lab purposes. Actions are being logged.

Microsoft can block the traffic coming from these IPs, if this happens you can create traffic manually from a free account or from <https://emkei.cz/>.

As a malicious IOC you can use [http://ihaveabadreputation\[.\]com](http://ihaveabadreputation[.]com)

1. Connect to any of the sites below, insert your email domain, and press **Submit**.

<http://3.19.33.33:5000/>



2. Wait for the “Thank you for submitting your domain:” message to be displayed on the screen. **This message may take up to 3min to show.**



3. Go back to your ETD dashboard. On the Home tab or at the Messages tab, you should be able to see threat messages in the 6 categories: BEC, Scam, Phishing, Malicious, Spam, and Graymail

Verdict	Action	Rule	Received	Sender	Recipients	Subject	Direction
BEC	—	—	Jan 27 2025 02:43 PM CST	Veronica Stroll <john...	johnnoone@emailseci...	test	Incoming
Malicious	—	—	Jan 27 2025 02:38 PM CST	Veronica Stroll <john...	johnnoone@emailseci...	This is a test	Incoming
BEC	—	—	Jan 27 2025 02:36 PM CST	Veronica Stroll <john...	johnnoone@emailseci...	This is a test	Incoming
Malicious	—	—	Jan 27 2025 02:32 PM CST	Greg Barnes (grebarn...	johnnoone@emailseci...	test rep	Incoming
—	—	—	Jan 27 2025 02:13 PM CST	Greg Barnes (grebarn...	johnnoone+test@em...	test 3	Incoming
—	—	—	Jan 27 2025 02:03 PM CST	Greg Barnes (grebarn...	johnnoone@emailseci...	Test 2	Incoming
—	—	—	Jan 27 2025 01:42 PM CST	Greg Barnes (grebarn...	johnnoone@emailseci...	test	Incoming

4. Open one of the messages and check the information. In the picture we are opening a phishing email.

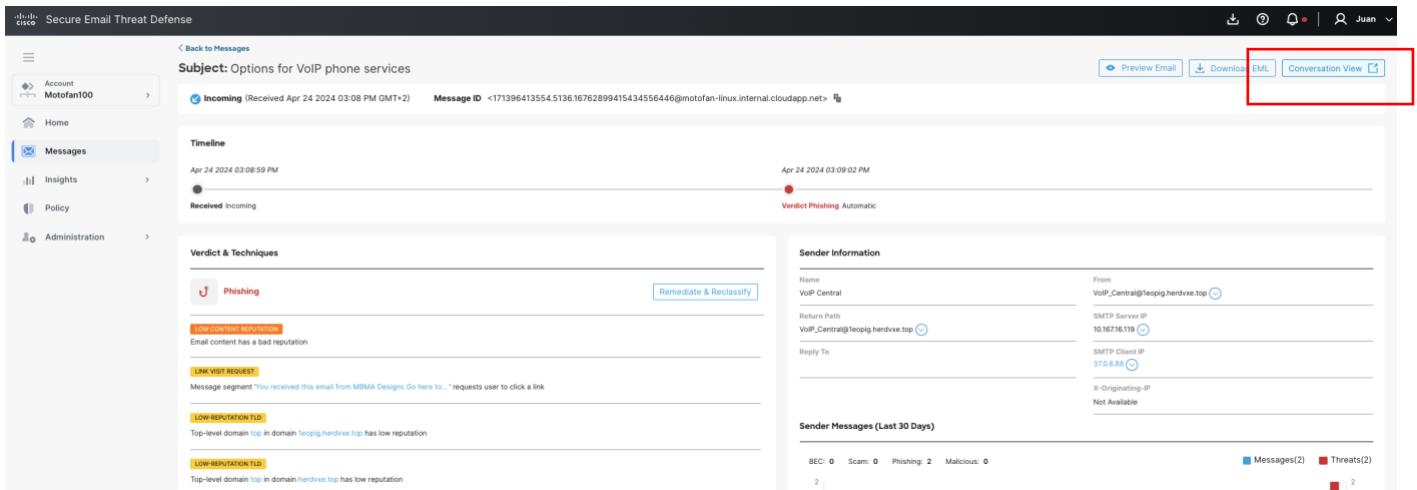
5. You should see emails have come in. In some cases, O365 will stop some emails. These will remain in the Microsoft quarantine and will not be analyzed by ETD. If, for some reason, this email is released from quarantine, that email will be scanned by ETD.



Open the Microsoft Quarantine <https://security.microsoft.com/quarantine?viewid=Email> and review if there is any email. You can release them.

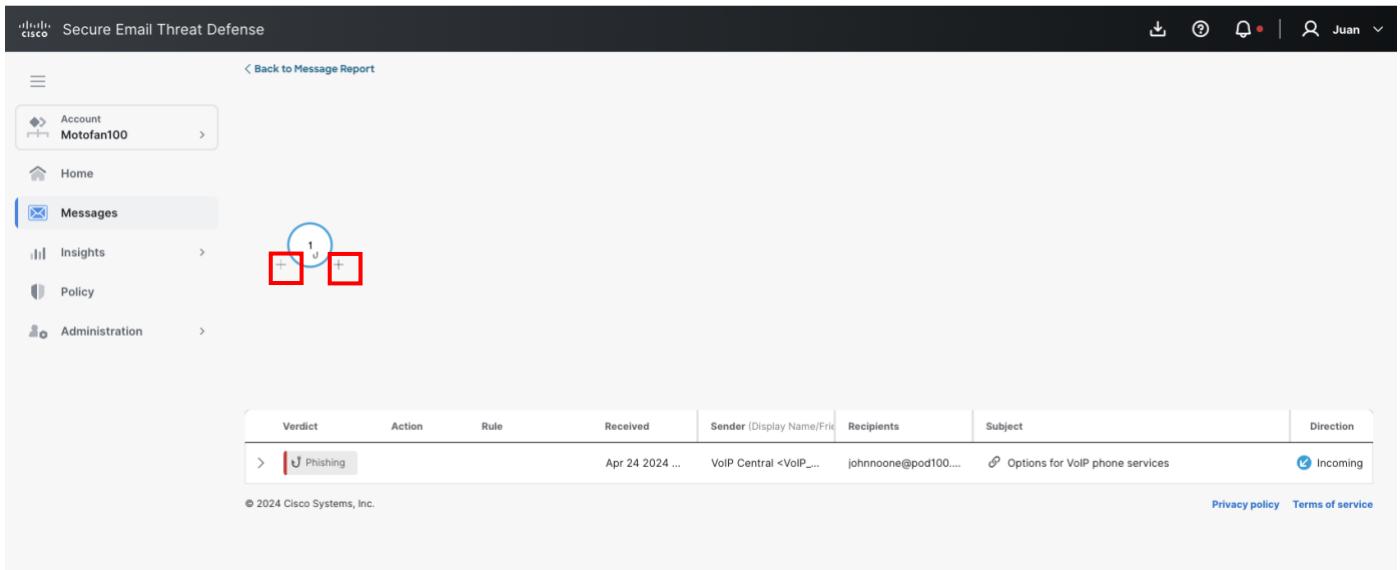
Remember that Microsoft may display the emails after some minutes.

6. Open one message and click on “**Conversation view**”.



The screenshot shows the Cisco Secure Email Threat Defense interface. On the left, a sidebar navigation includes Account (Motofan100), Home, Messages (selected), Insights, Policy, and Administration. The main content area displays a message from 'Motofan100' to 'johnnoone@pod100...'. The subject is 'Options for VoIP phone services'. The message was received on April 24, 2024, at 03:08:59 PM. The verdict is 'Phishing'. The timeline shows the message was received and flagged as phishing. The 'Verdict & Techniques' section lists 'Phishing' and other reputation issues like 'LOW CONTENT REPUTATION' and 'LINK VISIT REQUEST'. The 'Sender Information' section shows the sender is 'VoIP Central' with an SPF record and MX record. The 'Sender Messages (Last 30 Days)' section shows two messages and two threats. The top right corner has buttons for Preview Email, Download EML, and Conversation View, with the latter being the one highlighted by a red box.

7. In the screen you will see one circle with two + symbols, click on both + symbols. Nothing must change.



The screenshot shows the Cisco Secure Email Threat Defense interface. The sidebar navigation is identical to the previous screen. The main content area shows a message report for the same email. The 'Recipient' field contains 'johnnoone@pod100...' with a circular icon containing two '+' symbols next to it, which is highlighted by a red box. Below the recipient field, the message details are shown: Verdict (Phishing), Action (Auto-Block), Rule (None), Received (Apr 24 2024 ...), Sender (VoIP Central <VoIP\_Central@10.10.10.119>), Recipients (johnnoone@pod100...), Subject (Options for VoIP phone services), and Direction (Incoming). The bottom of the screen includes a copyright notice for Cisco Systems, Inc. and links for Privacy policy and Terms of service.

8. Open Your Administrator mailbox and forward the same message to another internal user. In the screen the message that we are using is "Search results For: Solar-Power In Homes" <https://outlook.office.com/mail/>

The screenshot shows the Microsoft Outlook inbox interface. On the left, there's a sidebar with 'Favourites' (Inbox 4, Sent Itms., Drafts 1, Add favo...), 'Folders' (Inbox 4, Drafts 1, Sent Itms., Delete 4, Junk Em..., Archive, Notes), and a 'This week' section with an email from Alberto Torralba. The main pane displays search results for 'Solar-Power In Homes'. The first result is from 'Solar Energy Systems' with the subject 'Search results For: Solar-P...'. The second result is from 'Premium Pure Forskolin' with the subject 'Want to get a Business Degr...'. Below the results, there's a note about blocked content and a link to learn more about sender identity. The message list includes a header for 'Search results For: Solar-Power In Homes'.

9. We will forward to [veronicastroll@pvtlabXXXX.bce-demo.com](mailto:veronicastroll@pvtlabXXXX.bce-demo.com). (Use your pod number)  
 (Microsoft creates around 16 accounts in the dev environments, always the same. You can verify this in the O365 dashboard).

The screenshot shows an Outlook compose email window. The 'To' field contains 'Joni Sherman'. The subject line is 'Fw: " Search results For: Solar-Power In Homes "' and the body text is 'Type / to insert files and more'. Below the body, there are two sets of email headers. The first set is for the forwarded message: From: FNU LNU <admin@3vzsvh.onmicrosoft.com>, Sent: 06 October 2023 13:14, To: Joni Sherman <JoniS@3vzsvh.onmicrosoft.com>, Subject: Fw: " Search results For: Solar-Power In Homes ". The second set is for the original message: From: Solar Energy Systems <SolarEnergySystems@sniffishic.download>, Sent: 30 August 2023 13:18, To: FNU LNU <admin@3vzsvh.onmicrosoft.com>, Subject: " Search results For: Solar-Power In Homes ". A note at the bottom of the body text says 'If your display can't survey the COMMERCIAL-Advertisement at all? You will need to tap [here](#)'.

10. Now, go back to Email Threat Defense dashboard and click on messages. Search for the internal email you sent to Veronica Stroll.



Verdict	Action	Rule	Received	Sender (Display Name)	Recipients	Subject	Direction	Actions
			Apr 24 202...	John Noone <Jo...	veronicastr...@p...	⌚ Fw: " Search results For: Solar-Power In Hom...	Internal	>

11. You can see an internal email. Open the message and click on “**Conversation View**”

Secure Email Threat Defense

Subject: Fw: " Search results For: Solar-Power In Homes "

Internal (Received Apr 24 2024 03:14 PM GMT+2) Message ID <AS8P193MB1544E5E90DE651BB3CCF1E77FD102@AS8P193MB1544.EURP193.PROD.OUTLOOK.COM>

Timeline

Received Internal

Verdict & Techniques

No Details Available

Conversation View

12. Your output should be as the next picture.

Secure Email Threat Defense

Back to Message Report

Account Motofan100

Messages

Verdict Action Rule Received Sender (Display Name/Friend) Recipients Subject Direction

> ⚡ Graymail			Apr 24 2024 ...	Solar Energy Syste...	johnnoone@pod100...	⌚ " Search results For: Solar-Power In Homes "	Incoming
>			Apr 24 2024 ...	John Noone <JohnN...	veronicastr...@p...	⌚ Fw: " Search results For: Solar-Power In Homes "	Internal

© 2024 Cisco Systems, Inc. Privacy policy Terms of service

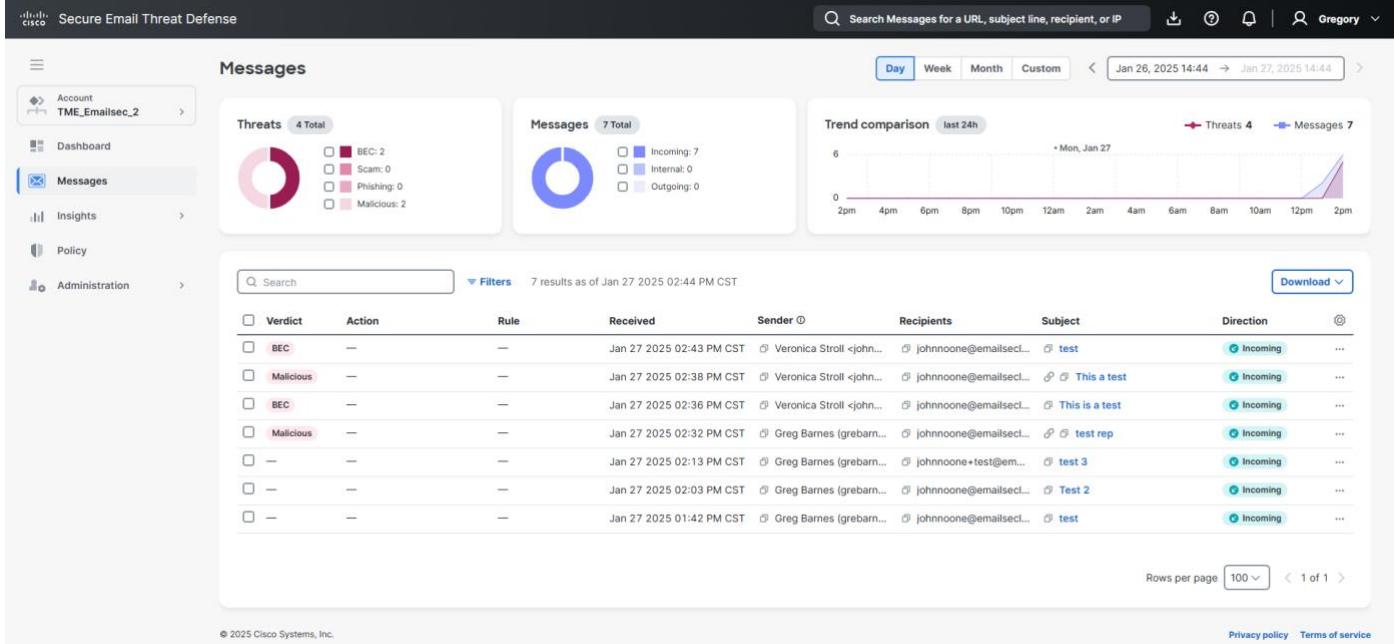


## Task – Dashboard use case

### Search Messages

This task will allow us to learn how to use searches from the Cisco Email Threat Defense console. We cannot see all the options in this lab, but it is essential that you perform searches so you can see how it works.

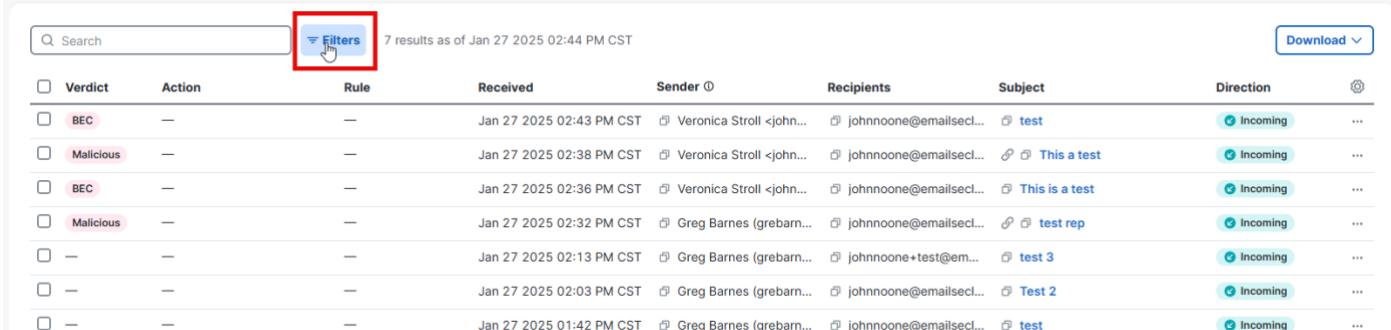
#### 1. Click on Messages



The screenshot shows the Cisco Secure Email Threat Defense interface. On the left, there's a navigation sidebar with 'Account TME\_Emailsec\_2' selected. The main area is titled 'Messages'. It features three cards: 'Threats' (4 Total), 'Messages' (7 Total), and 'Trend comparison' (last 24h). Below these is a search bar with 'Search' and a 'Filters' button. The table below lists 7 results as of Jan 27 2025 02:44 PM CST. The columns include Verdict, Action, Rule, Received, Sender, Recipients, Subject, Direction, and a more options icon. The 'Direction' column shows 'Incoming' for all entries. The 'Recipients' column shows various email addresses, some with attachments. The 'Subject' column contains test-related messages like 'test', 'This a test', 'test rep', and 'Test 3'. The 'Direction' column has a 'Download' button at the top right. At the bottom, there are links for 'Privacy policy' and 'Terms of service'.

Verdict	Action	Rule	Received	Sender	Recipients	Subject	Direction	...
BEC	—	—	Jan 27 2025 02:43 PM CST	Veronica Stroll <john...	johnnoone@emailsec...	test	Incoming	...
Malicious	—	—	Jan 27 2025 02:38 PM CST	Veronica Stroll <john...	johnnoone@emailsec...	This a test	Incoming	...
BEC	—	—	Jan 27 2025 02:36 PM CST	Veronica Stroll <john...	johnnoone@emailsec...	This is a test	Incoming	...
Malicious	—	—	Jan 27 2025 02:32 PM CST	Greg Barnes (grebarn...	johnnoone@emailsec...	test rep	Incoming	...
—	—	—	Jan 27 2025 02:13 PM CST	Greg Barnes (grebarn...	johnnoone+test@em...	test 3	Incoming	...
—	—	—	Jan 27 2025 02:03 PM CST	Greg Barnes (grebarn...	johnnoone@emailsec...	Test 2	Incoming	...
—	—	—	Jan 27 2025 01:42 PM CST	Greg Barnes (grebarn...	johnnoone@emailsec...	test	Incoming	...

#### 2. Click on the “filters” text.



The screenshot shows the same 'Messages' table as above, but with a red box highlighting the 'Filters' button in the search bar. The table displays 7 results as of Jan 27 2025 02:44 PM CST. The columns and data are identical to the first screenshot.

#### 3. Using the options, search for all the emails detected as “**All Threats**” and click “**Apply**”.

Secure Email Threat Defense

Search Messages for a URL, subject line, recipient, or IP

Gregory

### Messages

Threats 4 Total

- BEC: 2
- Scam: 0
- Phishing: 0
- Malicious: 2

Messages 7 Total

- Incoming: 7
- Internal: 0
- Outgoing: 0

Trend comparison last 24h

Mon, Jan 27

Filters

Verdicts

- All Threats
- BEC
- Scam
- Phishing
- Malicious

Last action

- Move to Junk
- Move to Trash
- Move to Inbox
- Move to Quarantine
- Delete
- No Actions

Message rules

- Allow List
- Verdict Override
- Bypass Analysis
- No Rules

Reset all Cancel Apply

Verdict	Action	Rule	Received	Sender	Recipients	Subject
<input type="checkbox"/> BEC	—	—	Jan 27 2025 02:43 PM CST	Veronica Stroll <john...	johnnoone@emailsec...	<a href="#">test</a>
<input type="checkbox"/> Malicious	—	—	Jan 27 2025 02:38 PM CST	Veronica Stroll <john...	johnnoone@emailsec...	<a href="#">This is a t</a>
<input type="checkbox"/> BEC	—	—	Jan 27 2025 02:36 PM CST	Veronica Stroll <john...	johnnoone@emailsec...	<a href="#">This is a t</a>
<input type="checkbox"/> Malicious	—	—	Jan 27 2025 02:32 PM CST	Greg Barnes (grebam...	johnnoone@emailsec...	<a href="#">test re</a>
<input type="checkbox"/> —	—	—	Jan 27 2025 02:13 PM CST	Greg Barnes (grebam...	johnnoone+test@em...	<a href="#">test 3</a>
<input type="checkbox"/> —	—	—	Jan 27 2025 02:03 PM CST	Greg Barnes (grebam...	johnnoone@emailsec...	<a href="#">Test 2</a>
<input type="checkbox"/> —	—	—	Jan 27 2025 01:42 PM CST	Greg Barnes (grebam...	johnnoone@emailsec...	<a href="#">test</a>

© 2025 Cisco Systems, Inc.



## Manual Remediation.

We are going to manually remove/remediate some phishing emails discovered in the previous task.

1. Open the admin mailbox in another browser window. <https://outlook.office.com/mail/>

The screenshot shows the Microsoft Outlook inbox with 76 messages. Several messages are highlighted as potential threats:

- Dog Food Brands: Compare Top Dog Food... (3/16 PM)
- Breathaking Alaskan Cruises: You should consider g... (3/16 PM)
- Brain Disease: Ships fast - Feeling Tir... (3/16 PM)
- VOIP Plans: Find the Best VOIP pla... (3/16 PM)
- Used\_Car\_Dealers: Used Car Dealers Online... (3/16 PM)
- Important\_News: Make Money From Ho... (3/16 PM)
- Online\_Roofing\_Quotes: Upgrade Your Home w... (3/16 PM)
- Ella Wallace: Fix your power compa... (3/16 PM)
- Wireless\_Security\_Camera: Wireless security for T... (3/16 PM)
- Sarah Taylor: Your Monthly Lifemar... (3/16 PM)
- Defeating Diabetes: Mysterious "super star..." (3/16 PM)

2. You must have two windows, one with Cisco Email Threat Defense and other with the administrator Mailbox.
3. In Cisco Email Threat Defense console, select one email. A new menu will appear.

The screenshot shows the Cisco Secure Email Threat Defense interface. On the left, there's a navigation sidebar with options like Account, Dashboard, Messages, Insights, Policy, and Administration. The main area displays three donut charts: Threats (4 Total), Messages (4 Total), and Trend comparison (last 24h). Below these are search and filter fields, and a detailed view of selected messages.

**Message Selection Dialog:**

Verdict	Action	Rule	Received	Sender	Recipients	Subject	Direction
<input checked="" type="checkbox"/> BEC	—	—	Jan 27 2025 02:43 PM CST	Veronica Stroll <john...	johnnoone@emailsec...	test	Incoming
<input type="checkbox"/> Malicious	—	—	Jan 27 2025 02:38 PM CST	Veronica Stroll <john...	johnnoone@emailsec...	This is a test	Incoming
<input type="checkbox"/> BEC	—	—	Jan 27 2025 02:36 PM CST	Veronica Stroll <john...	johnnoone@emailsec...	This is a test	Incoming
<input type="checkbox"/> Malicious	—	—	Jan 27 2025 02:32 PM CST	Greg Barnes (grebarn...	johnnoone@emailsec...	test rep	Incoming



4. Click on the Reclassify dropdown menu.

The screenshot shows the 'Messages' section of the Cisco Secure Email Threat Defense interface. At the top, there are three donut charts: 'Threats' (4 Total), 'Messages' (4 Total), and 'Trend comparison (last 24h)'. Below these are search and filter fields, and a download button. The main area displays a table of messages with columns for 'Verdict', 'Action', 'Date', 'Sender', 'Recipients', 'Subject', and 'Direction'. A red box highlights the 'Reclassify' dropdown menu in the top right corner of the message list table. The table contains the following data:

Verdict	Action	Date	Sender	Recipients	Subject	Direction
BEC	—	7/2025 02:43 PM CST	Veronica Stroll <john...	johnnoone@emailsec...	test	Incoming
Malicious	—	7/2025 02:38 PM CST	Veronica Stroll <john...	johnnoone@emailsec...	This is a test	Incoming
BEC	—	7/2025 02:36 PM CST	Veronica Stroll <john...	johnnoone@emailsec...	This is a test	Incoming
Malicious	—	7/2025 02:32 PM CST	Greg Barnes (grebarn...	johnnoone@emailsec...	test rep	Incoming

5. Select “Keep verdict”.

If we change the verdict, the information will be sent automatically to Talos.  
As this is a lab, we don't want to send anything.

Secure Email Threat Defense

Messages

Threats 4 Total

Messages 4 Total

Trend comparison last 24h

Message selected | Reclassify [Keep verdict] Request action Select action

Verdict	Action	Received	Sender	Recipients	Subject	Direction
<input checked="" type="checkbox"/> BEC	—	2025 02:43 PM CST	Veronica Stroll <john...	johnnoone@emailsec...	test	Incoming
<input type="checkbox"/> Malicious	—	2025 02:38 PM CST	Veronica Stroll <john...	johnnoone@emailsec...	This is a test	Incoming
<input type="checkbox"/> BEC	—	2025 02:36 PM CST	Veronica Stroll <john...	johnnoone@emailsec...	This is a test	Incoming
<input type="checkbox"/> Malicious	—	2025 02:32 PM CST	Greg Barnes (grebarn...	johnnoone@emailsec...	test rep	Incoming

Rows per page 100 < 1 of 1 >

© 2025 Cisco Systems, Inc. Privacy policy Terms of service

6. Click on the “Request Action” dropdown menu and select “**Move to Junk**”

Secure Email Threat Defense

Messages

Threats 4 Total

Messages 4 Total

Trend comparison last 24h

Message selected | Reclassify [Keep verdict] Request action Select action

Verdict	Action	Rule	Received	Subject	Direction
<input checked="" type="checkbox"/> BEC	—	—	Jan 27 2025 02:43 PM CST	johnnoone@emailsec...	test
<input type="checkbox"/> Malicious	—	—	Jan 27 2025 02:38 PM CST	johnnoone@emailsec...	This is a test
<input type="checkbox"/> BEC	—	—	Jan 27 2025 02:36 PM CST	Veronica Stroll <john...	This is a test
<input type="checkbox"/> Malicious	—	—	Jan 27 2025 02:32 PM CST	Greg Barnes (grebarn...	test rep

Rows per page 100 < 1 of 1 >

© 2025 Cisco Systems, Inc. Privacy policy Terms of service

7. Click on **Update**



The screenshot shows the 'Messages' section of the Secure Email Threat Defense dashboard. It includes a sidebar with navigation links like Account, Dashboard, Messages, Insights, Policy, and Administration. The main area displays three donut charts: Threats (4 Total), Messages (4 Total), and Trend comparison (last 24h). Below these are search and filter options, and a table of messages. The table has columns for Verdict, Action, Rule, Received, Sender, Recipients, Subject, and Direction. One row in the table is selected, showing a 'Request action' dropdown set to 'Move to Junk'. A red box highlights the 'Update' button at the top right of the table. The bottom of the screen shows copyright information and links to Privacy policy and Terms of service.

8. You should see this information.

The screenshot shows a search results page with a search bar and a 'Filters' button indicating 4 results. Below is a table with columns for Verdict, Action, and Rule. One row is selected, showing a 'BEC' verdict, an 'Action' of 'Move Requested', and a 'Rule' of '—'. A red box highlights the 'Move Requested' button.

9. Open the window browser with the admin Mailbox. The email should be moved to the junk folder.

The screenshot shows the Microsoft Outlook inbox. The left sidebar shows Favorites (Inbox, Sent Items, Drafts) and Folders (Inbox, Drafts, Sent Items, Deleted Items, Junk Email). The 'Junk Email' folder is selected, showing one item. The item details show it's from 'Breathaking Alaskan Cruises' with the subject 'You should consider going...'. A red box highlights this item in the list.



10. On the Cisco Email Threat Defense console, open the message click in the arrow. In this window you can see the timeline, and last step is the remediation process.

The screenshot shows the Cisco Email Threat Defense interface. At the top, there's a header with a back button, subject information ('Subject: You should consider going on an Alaskan Cruise'), and download/preview buttons. Below the header is a timeline section with three events: 'Received Incoming' at 03:16:14 PM, 'Verdict Phishing Automatic' at 03:16:18 PM, and 'Junk Manual Remediated by Juan Torralba' at 03:24:04 PM. Underneath the timeline is a 'Verdict & Techniques' section, which includes a 'Phishing' icon and a 'LOW CONTENT REPUTATION' alert stating 'Email content has a bad reputation'. There's also a 'Remediate & Reclassify' button.

### Lesson learned.

In this task, we have seen how to perform searches, and we have seen the "Timeline" option. There are other options, such as "Download the EML", which you can try. This allows you to download a copy of the email in EML format.

### Task – API & Postman.

As you know, APIs are being promoted in all security platforms, and email platforms are no exception. Saying this, Cisco Secure Email Gateways and Cisco Email Threat Defense provide REST APIs to integrate with external tools and applications.

Cisco XDR is one of the applications that can use the APIs to improve the detection, analysis, and convictions of messages.

Today, you will see how the Message Search API in Email Threat Defense works.

In this lab, you will learn how to use Postman's as an API client.

Postman can be installed on our workstation or you can use their cloud application without installation.

If you want to use the cloud application, we need to create an account on the Postman portal. It is explained in [Appendix A](#).

To use the Message Search API there are 2 steps required:

1 – Use the client credentials to authenticate and to get an access token



2 – Use the access token from Step 1 and query the message information

If you want to learn more:

<https://developer.cisco.com/docs/message-search-api/>

## Authentication API

1. You must create API credentials in our Email Threat Defense account.  
Open the Email Threat Defense console. <https://beta-ui.cmd.cisco.com/>

2. Click on “*Administration*” -> “*API Clients*”.

The screenshot shows the Cisco Secure Email Threat Defense administration interface. The left sidebar has a red box around the 'Administration' tab. The main content area has a red box around the 'API Clients' link under the 'Business' category. Below it, there are two cards: one for 'Scam' (0) and one for 'Malicious' (2). To the right, there's a chart titled 'Unwanted mail' showing 0 total messages. At the bottom, a search bar says 'No matches found'.

3. Click on “*Add New Client*”.

- 4.

The screenshot shows the Cisco Secure Email Threat Defense administration interface for account 'TME\_Emailsec\_1'. The left sidebar has a red box around the 'Administration' tab. The main content area shows the 'API Key' section with a note about rate limiting and a 'Generate API Key' button. Below it is the 'API Clients' section with a table header: 'Client Name', 'ID', 'Description', 'Expiration Status', and 'Action'. A red box highlights the '+ Add New Client' button.

5. Fill in the “*Client Name*” box. We can name it “*Postman*”, and then click on “*Submit*”.



Add New API Client

---

Client Name  
Postman

Description  
Add description...

6. Copy the “*Client ID*” and “*Client Password*” in your text editor.

Please make sure you copy the Client Password. You will not be able to retrieve it later.

Add New API Client

**⚠** The Client Password cannot be recovered, once you close this window.  
Please store securely.

Client ID  
70edcdce-f51b-4f16-ae99-abd056d2d755

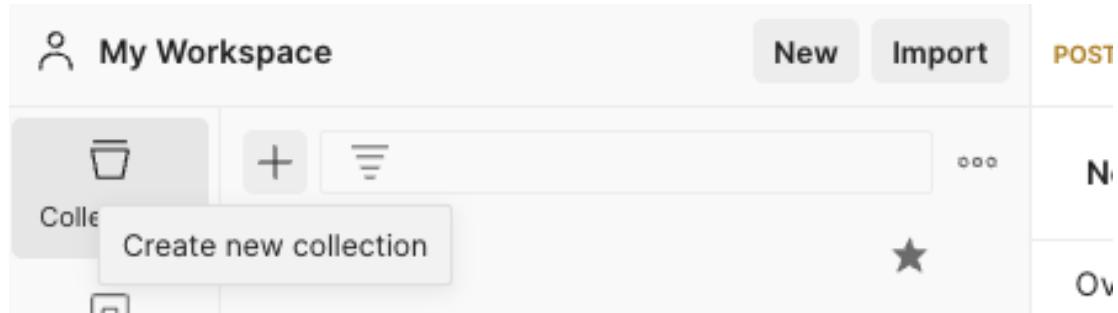
Client Password  
GVsLQIL22F7Qyc1waCKbgmef3DE8EtP8-gUzEWgmgOE

7. Click on “*Close*”
8. Open “*Postman*” application  
If you don't have the Postman application installed, you can go to Appendix A and check the steps to create an account or install the application on your desktop.

<https://www.postman.com/api-platform/api-client/>

9. Create a “*New collection*”.





10. You can use the name “*ETD LAB BETA*”.

11. Click on “*Add a request*” inside the “*New collection*” you created in the previous step.

12. You can name “*authentication*” as the new name.

Key	Value
Key	Value

13. Put the following link in the “*Enter URL..*” box: <https://api.beta.etd.cisco.com/v1/oauth/token>  
 14. Click on the “*Headers tab*” and add the API key to identify the ETD tenant.

Key	Value	Description
x-api-key	hGEaUD4Vyl3WLA5rHfjuA1ZRstqT7dgf7mDaxKTL	
Key	Value	Description

15. Select “*Authorization tab*” and select “*Basic Auth*”. In the Basic auth, you will use “Client ID” as username and “Client Password” as Password.

The method used in this query must be “**POST**”.

Type	Basic Auth
Username	1515c3bd-8e3a-4d30-9764-a3eeb42be700
Password	zNtdtYg4maJobRLA9eF-TPfzECU5xCuN

Body Cookies Headers (16) Test Results  
 Pretty Raw Preview Visualize JSON Status: 200 OK Time: 2.79 s Size: 1.03 KB Save as Example

```

1 "accessToken": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOiE2OTYzNDIzOTgsImlhCI6MTY5NjMzODc5OCwi3ViIjoiYXBpLWNsaWVudCIs
2   "tokenType": "access",
3   "expiresIn": 3600
4
5
  
```

You should see a message with the “*accessToken*” in the response. This will be the token you will query message information in the next task.



## Search API

Once we have completed the authentication process, we will use the token obtained for the search API. In the exercise, we will carry out several searches, but you can do more.

1. Click on “+” to create a new request.

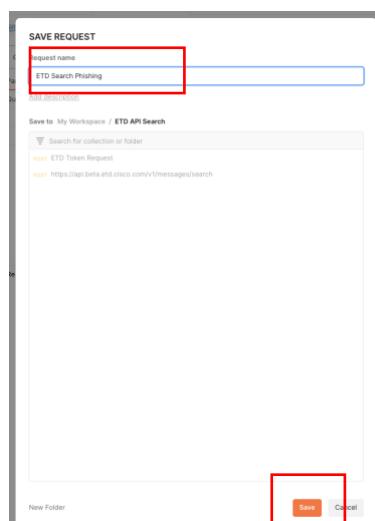
The screenshot shows the Postman interface. At the top, there is a search bar labeled "Search Postman". Below it, a list of requests includes "POST ETD Token Request" and a new request entry with a plus sign icon, which is highlighted with a red box. The URL field contains "v1/oauth/token". On the right side, there are buttons for "Save", "Send", and "Cookies". Below the URL field, there are tabs for "Pre-request Script", "Tests", and "Settings".

2. Click on **Save**.

The screenshot shows the Postman interface with an "Untitled Request" tab. The "Params" tab is selected. A "Save" button is highlighted with a red box. Below the "Params" tab, there is a "Query Params" table with one row. The "Send" button is also visible on the right.

3. Name the query "**ETD Search Phishing**".

You will create a query to search all the phishing emails during the last 2 hours.



4. Put the following link in the "**Enter URL..**" box: <https://api.beta.etd.cisco.com/v1/messages/search> And Select **Post**.



The screenshot shows the Postman application interface. At the top, there are tabs for 'Network' and 'Explore'. A search bar says 'Search Postman'. On the right, there are buttons for 'Invite', 'Upgrade', and other account settings. Below the header, there's a list of requests: 'POST https://api.beta.etd.ci' (status red), 'POST ETD Search Phishing' (status red), and 'POST ETD Token Request'. A '+' button and three dots are next to them. To the right, it says 'No Environment' with a dropdown arrow. On the far right, there are icons for file operations like 'Save', 'Edit', and 'Copy'. The main area shows an 'HTTP ETD API Search / ETD Search Phishing' request. The method is 'POST' and the URL is 'https://api.beta.etd.cisco.com/v1/messages/search'. Below the URL, there are tabs for 'Params', 'Authorization', 'Headers (7)', 'Body', 'Pre-request Script', 'Tests', and 'Settings'. The 'Params' tab is selected. Under 'Query Params', there's a table with one row: 'Key' (Value: 'Key') and 'Value' (Description: 'Value'). To the right, there are buttons for 'Save', 'Send', and 'Cookies'. On the left side of the main area, there's a vertical sidebar with sections like 'Response' and other collapsed sections.

5. Open **Authorization** tab and select **Bearer Token**.

This screenshot shows the same Postman interface as above, but with a different focus. The 'Authorization' tab is now selected, highlighted with a red box. The URL and method remain the same: 'POST https://api.beta.etd.cisco.com/v1/messages/search'. The other tabs ('Params', 'Headers (7)', 'Body', etc.) are visible but not selected. To the right, there are buttons for 'Save', 'Send', and 'Cookies'. On the left, there's a 'Type' dropdown set to 'Bearer Token' and a 'Token' input field containing 'Token'. A note below explains that the authorization header will be generated automatically when the request is sent.

6. Copy the Access Token from the previous task.



HTTP ETD API Search / ETD Search Phishing

POST <https://api.beta.etd.cisco.com/v1/messages/search>

Save Send

Params Authorization **8** Headers **8** Body Pre-request Script Tests Settings Cookies </> **?** **i**

Type	Bearer Token	Token
The authorization header will be automatically generated when you send the request. Learn more about <a href="#">authorization</a>		
<pre>eyJhbGciOiJIUzI1NiJnR5cCl6IkpxVCJ9eyJl eHAiOiE2OTY4NDU2MzgsImhdC16MTY5Njg 0MJaZOCwic3ViljojYXBpLWNsaWVudCislmF1 ZC16InB1YmxpYy1hcGkiLCJjbGlibnRJZC16ljE1 MTVjM2JKLThiM2EtNGQzMCO5NzY0LWEzZ WVINDJiZTcwMCIsInRlbmFudElkjjojYjE1NjFh ZTQtYmZjNC00NGFmLWJkY2EtNDkzNjNhZjI zNjEzln0.rSWTxelA2irgiqEab1RlmIT8He0PT ThyNxF7wGgLRc </pre>		

Response

7. Remember to add always the api key in all the API queries you use.

Params Authorization **8** Headers **10** Body Scripts Settings

Headers **9 hidden**

Key	Value	Description
<input checked="" type="checkbox"/> x-api-key	hGEaUD4Vyl3WLA5rHfjuA1ZRstqT7dgf7mDaxKTL	
Key	Value	Description

8. Now, click on the “**Body**” tab, and inside the Body tab select “**raw**”.

In the body, we will configure the search query. There are different attributes that we can use, the first task will be simple, and we will search all the Phishing emails in the last 24 hours.



POST ETD Search Phishing | POST ETD Token Request | + ⚙️ | No Environment | ⌂

HTTP ETD API Search / ETD Search Phishing

POST https://api.beta.etd.cisco.com/v1/messages/search

Params Authorization Headers (9) Body Pre-request Script Tests Settings Cookies

none form-data x-www-form-urlencoded raw binary GraphQL Text

```

1 {
2   "verdicts": [
3     "phishing"
4   ],
5   "timestamp": [
6     "2023-10-09T06:00:00Z",
7     "2023-10-09T08:00:00Z"
8   ]
9 }
10

```

9. Copy the JSON text into the **raw** section. (Review the timestamp and adapt this to your current date).

```
{
"timestamp":[
"2024-11-06T08:00:00.300Z", "2024-11-06T13:00:00.000Z"
],
"verdicts": [
"bec", "scam", "phishing", "malicious"
]
}
```

Adapting the timezone to UTC to use the search API query is essential.

**DateTimeRange** ▾ [  
example: List [ "2019-09-19T12:00:00Z", "2019-09-20T23:59:59Z" ]  
ISO 8601 formatted date time string range e.g ["2019-09-19T12:00:00Z", "2019-09-20T23:59:59Z"]. Beginning and end dates are inclusive. Timestamps should be in UTC timezone only. No other timezone is supported. First timestamp should be smaller than second.  
string]

10. Click on **Send**.



POST ETD Search Phishing

POST ETD Token Request

No Environment

HTTP ETD API Search / ETD Search Phishing

Save Send

Params Authorization Headers (9) Body Pre-request Script Tests Settings Cookies

Body Text

```

1 {
2   "verdicts": [
3     "phishing"
4   ],
5   "timestamp": [
6     "2023-10-09T06:00:00Z",
7     "2023-10-09T08:00:00Z"
8   ]
9 }
10

```

11. If everything is working, you will see something like this.

```

1 {
2   "data": {
3     "messages": [
4       {
5         "clientIP": "52.157.111.158",
6         "direction": "incoming",
7         "domain": "3vzvh.onmicrosoft.com",
8         "fromAddress": "office4@movenpick.ro",
9         "id": "155d4284-93d4-45cb-8d9e-390260099297",
10        "mailboxes": [
11          {
12            "joni@3vzvh.onmicrosoft.com"
13          }
14        ],
15        "internetMessageId": "<2937347ba5cc73f017a9939e7e9e059d@localhost.localdomain>",
16        "replyTo": [
17          {
18            "office4@movenpick.ro"
19          }
20        ],
21        "returnPath": "office4@movenpick.ro",
22        "serverIP": "10.13.183.106",
23        "subject": "Circuit Venetia Padova Verona Lacul di Garda",
24        "toAddresses": [
25          {
26            "joni@3vzvh.onmicrosoft.com"
27          }
28        ],
29        "timestamp": "2023-10-09T07:48:12Z",
30        "urls": [
31          "http://client_campaignsender.ro/u.php?g=304#",
32          "http://client_campaignsender.ro/to=%",
33          "https://online0.bisa01.repl.co/des/index.php",
34          "http://client_campaignsender.ro/u.php?g=skmr87w/1te/48b/rs",
35          "http://www.alexanderpalace.it/en",
36          "http://www.visti",
37          "http://www.movenpick.ro",
38          "http://www.movenpick.ro/",
39          "http://client_campaignsender.ro/tl.php?p=",
40          "http://www.vision-nl.biz/movenpick/images/2.jpg&quot"
41        ],
42        "verdict": {
43          "isManualVerdict": false,
44          "timestamp": "2023-10-09T07:48:15Z",
45          "category": "phishing"
46        }
47      }
48    ]
49  }
50

```

12. You can use this online tool to work with the JSON response.

<https://jsonpathfinder.com/>

13. Copy the output from Postman to the JsonPathFilder tool.



The screenshot shows the jsonpathfinder.com interface. On the left, a JSON document is displayed with line numbers from 1 to 40. The document contains nested objects for 'data' and 'messages'. The 'messages' object has properties like 'clientIP', 'direction', 'domain', 'fromAddress', 'id', 'mailboxes', 'toAddresses', and 'url'. On the right, a results panel shows the path 'x.data.messages[0]' and the expanded JSON object. The expanded object includes properties such as 'clientIP', 'direction', 'domain', 'fromAddress', 'id', 'mailboxes', 'internetMessageId', 'returnPath', 'serverIP', 'subject', 'toAddresses', 'timestamp', and 'urls'. The 'toAddresses' field is expanded to show two email addresses: 'admin@3zsvh.onmicrosoft.com' and 'admin@3zsvh.onmicrosoft.com'. The 'urls' field is expanded to show several URLs related to the message.

In this link, we can see all the options that we can use in the queries.

<https://developer.cisco.com/docs/message-search-api/#!message-search-api>

```
{
  "subject": "string",
  "from": "string",
  "recipient": "string",
  "filename": "string",
  "fileSHA256": "string",
  "verdicts": [
    "spam"
  ],
  "directions": [
    "incoming"
  ],
  "url": "string",
  "internetMessageId": "string",
  "pageSize": 100,
  "pageToken": "string",
  "timestamp": [
    "2023-10-01T12:00:00Z",
    "2023-10-02T23:59:59Z"
  ]
}
```



14. Change the verdict and test other from the list.

### **Verdict** ↘ `string`

Search for messages with specific verdicts.

Enum:

↙ [ `spam`, `malicious`, `phishing`, `neutral`, `graymail`, `bec`, `scam` ]

## Conclusion

If you have arrived here, you have reached the end of the laboratory. Congratulations.

You can repeat some of the exercises performed using different parameters, different emails, etc.

Remember that the deployment method and environment were simple.

Yes in. In our scenario, we find security gateways, local exchange, etc, and some configurations could change.

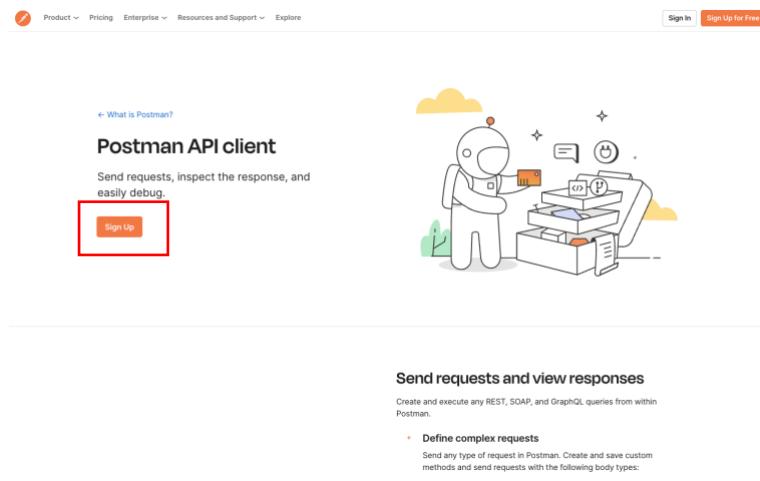


## APPENDIX

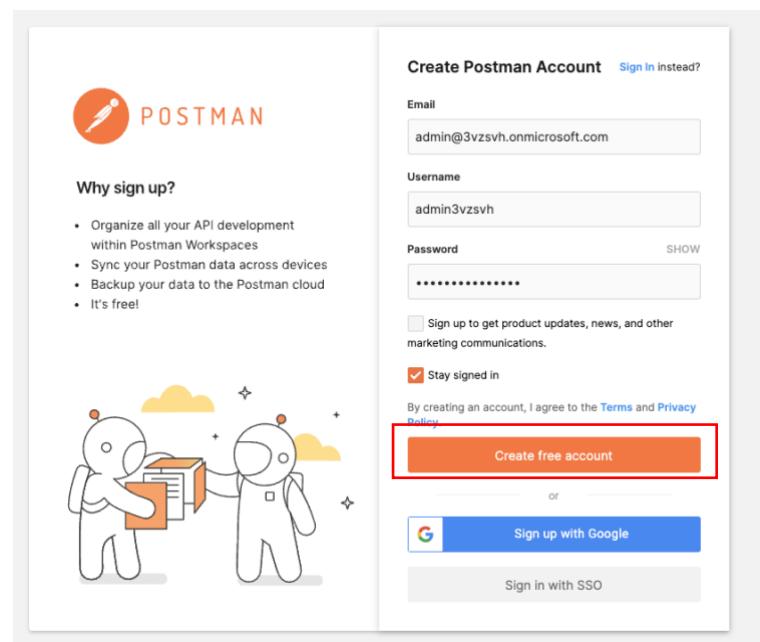
### Postman Installation

This is not intended to be a Postman manual, simply to highlight the steps to take to create a Postman account. As you can see they are very simple.

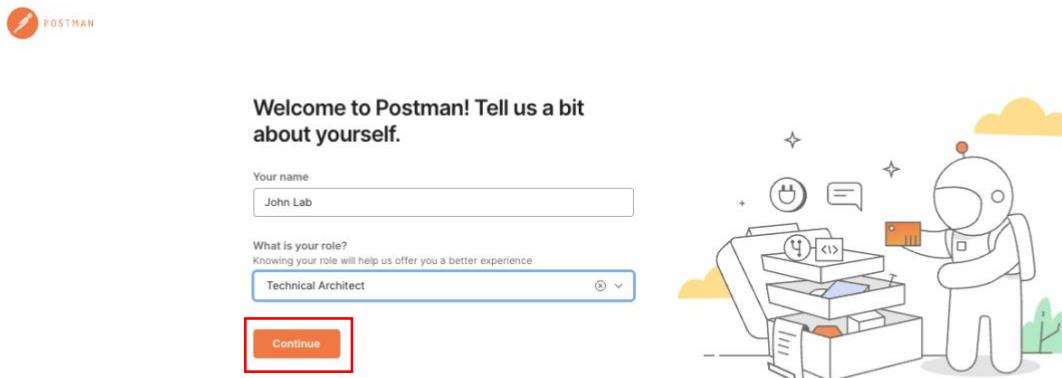
1. Open the link <https://www.postman.com/product/api-client/>
2. Click on “*Sign Up*”



3. Fill the form. You can use your cisco email, or whatever you want. And click on “*Create free account*”.



4. Fill the form and click on **Continue**



5. Now you are inside of Postman cloud service.

A screenshot of the Postman workspace interface. The top navigation bar includes "Home", "Workspaces", "API Network", "Explore", a search bar, and user account options. The main area is titled "My Workspace" and shows a collection named "My first collection" containing two folders: "First folder inside collection" and "Second folder inside collection". Each folder contains several requests. A modal window titled "Use a template to quickly set up your workspace" offers options like "API demos", "API development", "API testing", and "More templates". On the right side, there are sections for "About" (with a placeholder for a workspace summary), "Contributors" (listing "You"), and a link to "View workspace activity". A sidebar on the left provides links to "Collections", "Environments", "History", and "Create a collection for your requests" (with a "Create Collection" button).

6. Save and reserve the credentials for the lab.



7. If you want, you can download a local client. Click on [Home](#)

The screenshot shows the Postman interface. The top navigation bar includes 'Home' (highlighted with a red box), 'Workspaces', 'API Network', and 'Explore'. A search bar says 'Search Postman'. On the right, there are 'Invite', 'Settings', 'Bell', and 'Upgrade' buttons. The main area is titled 'My Workspace' with a 'Overview' tab selected. It displays a collection named 'My first collection' containing several requests. Below it is another collection named 'Second folder inside collection'. A sidebar on the left shows 'Collections', 'Environments', 'History', and a button to 'Create a collection for your requests'. A modal window titled 'Use a template to quickly set up your workspace' offers options like 'API demos', 'API development', 'API testing', and 'More templates'. To the right of the workspace overview, there are sections for 'About' (with a summary input field), 'Contributors' (listing 'You'), and a link to 'View workspace activity'.

8. Click on “[Download Desktop App](#)”

The screenshot shows the Postman homepage. The top navigation bar includes 'Home', 'Workspaces', 'API Network', and 'Explore'. A search bar says 'Search Postman'. On the right, there are 'Settings', 'Bell', and 'Upgrade' buttons. The main content area features a 'Recently visited workspaces' section with a link to 'My Workspace'. Below it is a 'Explore popular APIs' section with three items: 'Salesforce Platform APIs' (by Salesforce Developers, updated 29 Sep, 2023), 'Postman API' (by Postman, updated 6 Oct, 2023), and 'Day 05: Variables' (by Postman, updated 12 Jan, 2023). A sidebar on the left includes links for 'Postman works best with teams', 'Workspaces', 'Private API Network', 'Integrations', 'Reports', and sections for 'What is Postman', 'Learning Center', 'Support Center', 'Postman Enterprise', and 'Download Desktop App' (which is underlined).

9. Select your SO and install the application.



## Download Postman

Download the app to get started using the Postman API Platform today. Or, if you prefer a browser experience, you can try the web version of Postman.

### The Postman app

Download the app to get started with the Postman API Platform.

[Mac Intel Chip](#) [Mac Apple Chip](#)

By downloading and using Postman, I agree to the [Privacy Policy](#) and [Terms](#).

[Release Notes](#) · [Product Roadmap](#)

Not your OS? Download for Windows (x64) or Linux (x64, arm64)

### Postman on the web

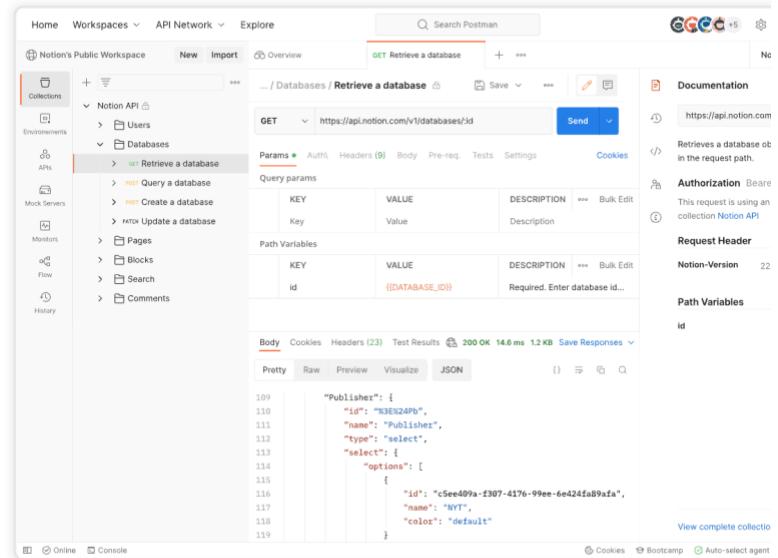
Access the Postman API Platform through your web browser. Create a free account, and you're in.

[Launch Postman](#)

### Postman Enterprise

Postman Enterprise is designed for organizations who need to deploy Postman at scale.

[Learn more →](#)



The screenshot shows the Postman web interface. On the left, there's a sidebar with sections like Home, Workspaces, API Network, and Explore. Under 'Workspaces', 'Notion's Public Workspace' is selected. In the main area, a request is being made to '... / Databases / Retrieve a database'. The method is 'GET' and the URL is 'https://api.notion.com/v1/databases/{id}'. The 'Params' tab shows a 'Query param' named 'Key' with 'Value' and 'Description' columns. The 'Path Variables' tab shows a 'Path Variable' named 'id' with a placeholder '(DATABASE\_ID)'. Below the request, the response status is '200 OK' with a duration of '14.6 ms' and a size of '1.2 KB'. The response body is displayed in JSON format:

```

109    "Publisher": {
110      "id": "8E3E24PB",
111      "name": "Publisher",
112      "type": "select",
113      "select": {
114        "options": [
115          {
116            "id": "c5ee409a-f307-4176-99ee-6e424fa89afa",
117            "name": "NYT",
118            "color": "default"
119          }
        ]
      }
    }
  
```



**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](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

