



## 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!



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

## 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> .....	28
<i>Lesson learned</i> .....	33
TASK – REVIEW THE PERMISSIONS ASSIGNED IN MICROSOFT (OPTIONAL) .....	34
TASK – TEST THE SOLUTION.....	37
<i>Lesson learned</i> .....	40
TASK - HIGH IMPACT PERSONNEL .....	41
TASK – “ATTACK” YOUR ENVIRONMENT.....	47
<i>Send Email Threats.</i> .....	47
TASK – DASHBOARD USE CASE .....	52
<i>Search Messages</i> .....	52
<i>Manual Remediation.</i> .....	54
<i>Lesson learned</i> .....	58
TASK – API & POSTMAN.....	59
<i>Authentication API</i> .....	59
<i>Search API</i> .....	65
CONCLUSION .....	71
APPENDIX .....	72
<i>Postman Installation</i> .....	72



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

## 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>.

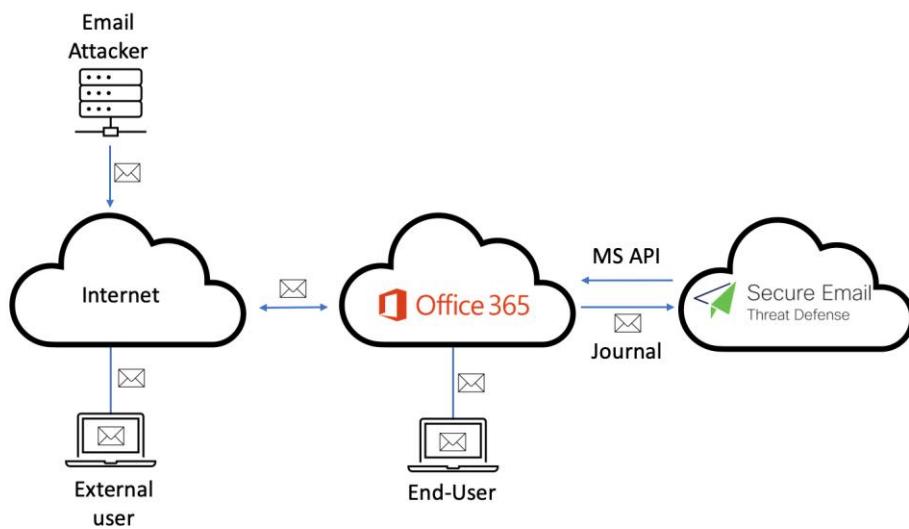


Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

## 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.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

## 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.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

## 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.

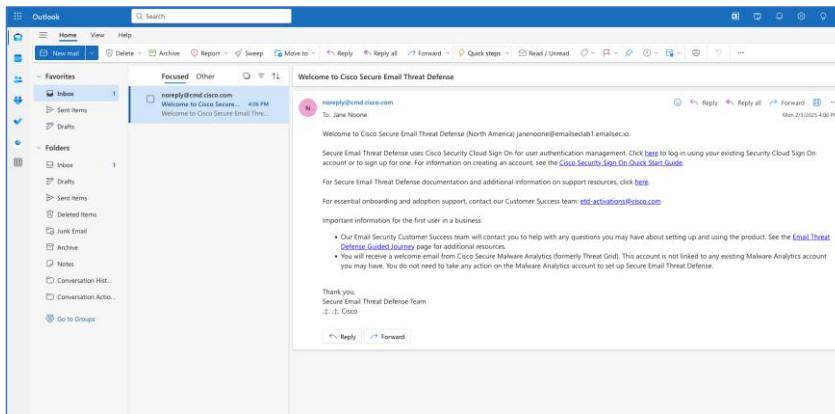
1. Please go to O365 portal <https://outlook.office.com/mail/>

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

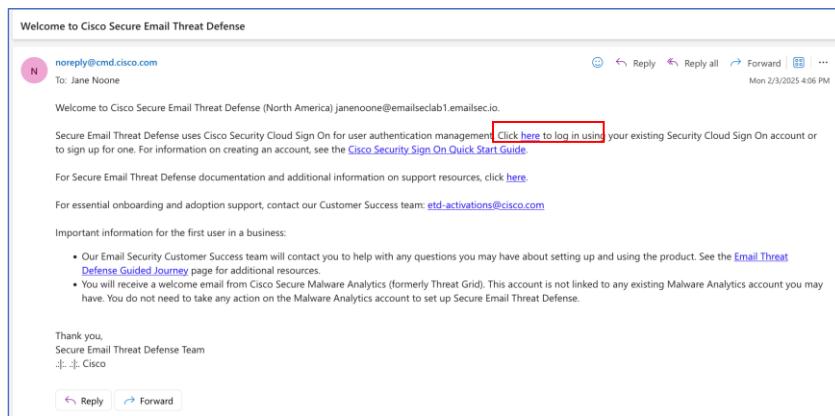
Administrator 1: [janenoone@emailseclabXX.emailsec.io](mailto:janenoone@emailseclabXX.emailsec.io)

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)



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

4. For the email address, please use the one you used to log in to O365.  
 Click on ***Sign up now***.

The screenshot shows the 'Security Cloud Sign On' page. It features a 'Email' input field, a 'Continue' button, and a 'Don't have an account? [Sign up now](#)' link, which is enclosed in a red box. Below this, there's an 'Or' link and 'Other login options'. At the bottom, there are links for 'System status' and 'Policy statement'.

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

Commented [S(1): why is this here?]

### 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>

I agree to the [End user license agreement](#) and [Privacy statement](#).

**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'

[Sign up](#)

[Cancel](#)



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

6. You should expect this screen:



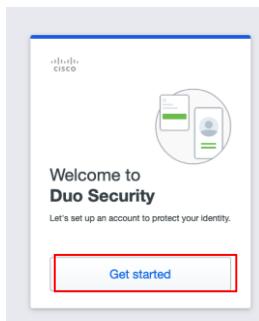
7. Go back to your administrator mailbox in O365: <https://outlook.office.com/mail/>  
8. Open the new message and press "Activate Account."



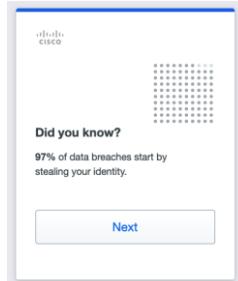
9. By default, you need to set up MFA when creating an ETD account. Press the “**Get started**” button:



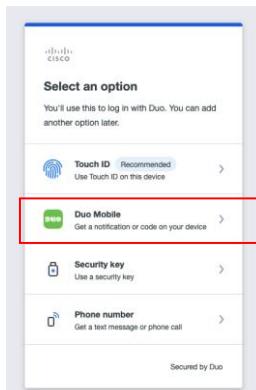
Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.



10. Click on **Next**.



11. Press the “**Duo Mobile**” button.



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



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

The screenshot shows a mobile application interface for Duo Mobile setup. At the top, there is a back arrow labeled '< Back'. Below it, the title 'Enter your phone number' is displayed, followed by the sub-instruction 'You'll have the option to log in with Duo Mobile.' A 'Country code' dropdown menu is set to '+1' with a small American flag icon. To its right is a text input field labeled 'Phone number'. Below these fields, a note says 'Example: "201-555-5555"'. A large blue 'Continue' button is centered at the bottom of the screen. At the very bottom, there is a link 'I have a tablet' and a 'Secured by Duo' logo.

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

The screenshot shows a mobile application interface for Duo Mobile setup. At the top, there is a back arrow labeled '< Back'. Below it, the question 'Is this correct?' is displayed. Two buttons are present: a large blue 'Yes, it's correct' button and a smaller white 'No, I need to change it' button. At the bottom, there is a 'Secured by Duo' logo.

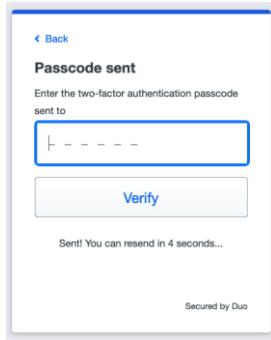
14. Now, click on “Send me a passcode” to confirm that you are the owner.

The screenshot shows a mobile application interface for Duo Mobile setup. At the top, there is a back arrow labeled '< Back'. Below it, the title 'Confirm ownership' is displayed. A large blue 'Send me a passcode' button is centered on the screen. Below it, there is a link 'Or call my phone'. At the bottom, there is a 'Secured by Duo' logo.

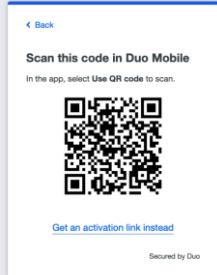


Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

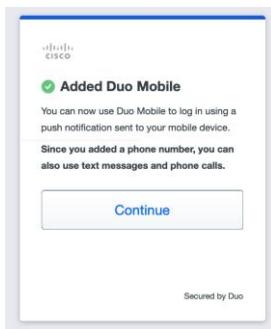
15. Introduce the code and press **Verify**.



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.

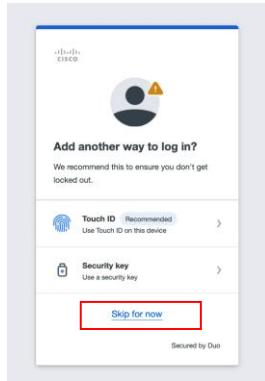


18. Press **Continue**

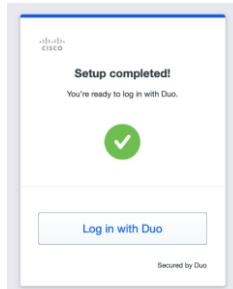
19. Click on **Skip for now**.



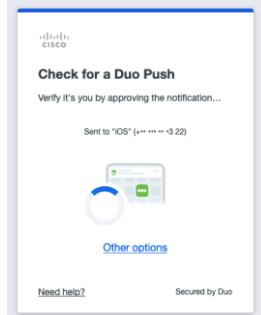
Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.



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>



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

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**.

The screenshot shows a login interface titled "Security Cloud Sign On". At the top, there is a Cisco logo. Below it, an "Email" input field contains the value "janemzone@emailclab1.emailsec.io". Directly beneath the input field is a large blue "Continue" button, which is highlighted with a red rectangular border. Below the "Continue" button, there is a link "Don't have an account? [Sign up now](#)". Further down, there is a separator line with the word "Or" and a link "Other login options". At the bottom of the form, there are links for "System status" and "Policy statement".

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

The screenshot shows the "Welcome to Cisco Secure Email Threat Defense" page. At the top, there is a Cisco logo and a "SECURE" badge. Below the header, there is a "Terms and Conditions" section. This section contains several paragraphs of text about the Cisco End User License Agreement (EULA) and Privacy Statement. At the bottom of this section, there is a blue button with the text "I agree with the terms and conditions." A red rectangular box surrounds this button. To the right of the button, there is a small circular icon with a white "X" inside.

**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.

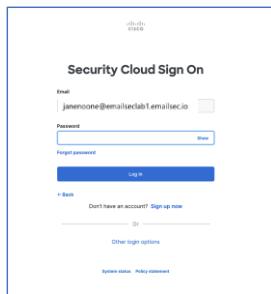


Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

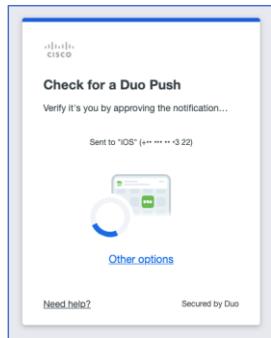
## Task – Configure Email Threat Defense account.

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>



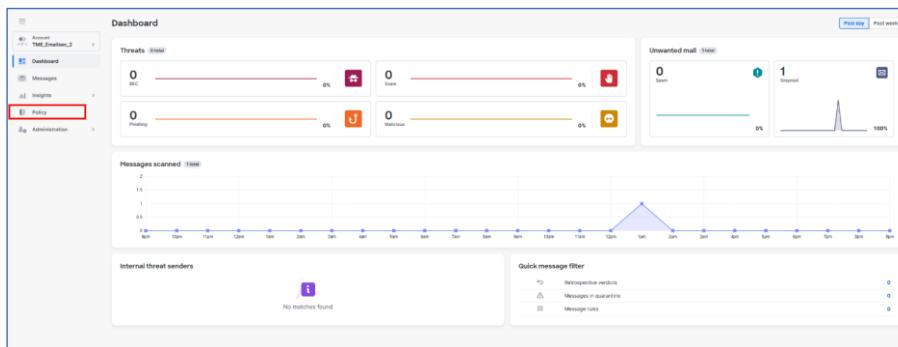
2. Accept the push from DUO on your mobile.



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



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

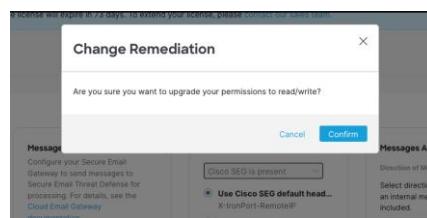


- The Email Threat Defense account you have access to is already activated to work with a gateway with no integration with O365. We need to connect with O365 and to do this, we need to move from Gateway/No auth to Microsoft 365/Read-Write.

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

This screenshot shows the policy configuration for 'Policy: TME\_Emailsec\_2'. It includes sections for Message Source (with a red box around 'Incoming'), Secure Email Gateway (SEG) settings, Messages Analysis, and an Automated Remediation Policy table. The 'Incoming' checkbox under 'Message Source' is highlighted with a red box.

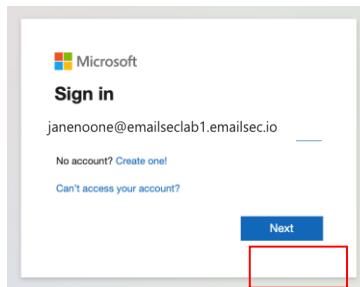
- Click on **Confirm**.



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

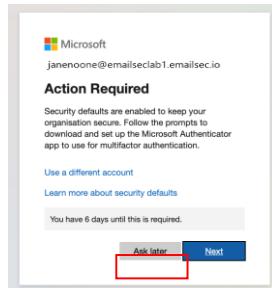
[janenoone@emailseclabXX@emailsec.io](mailto:janenoone@emailseclabXX@emailsec.io)

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**.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.



#### 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.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

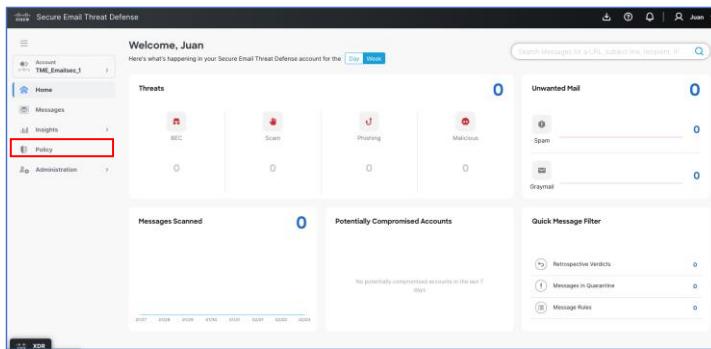
## Configure Cisco Secure Email Threat Defense Policy

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:

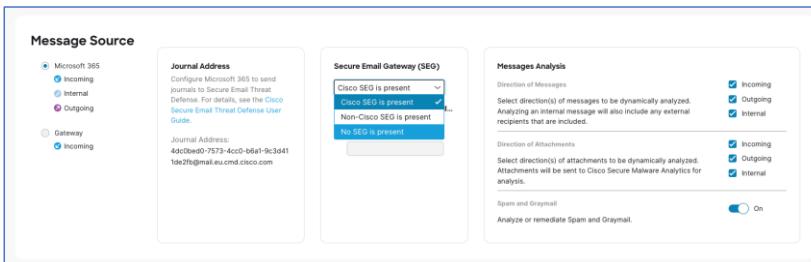
<https://www.cisco.com/c/en/us/td/docs/security/email-threat-defense/user-guide/secure-email-threat-defense-user-guide/policy.html>

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

**Secure Email Gateway (SEG)**

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

**Messages Analysis**

**Direction of Messages**

Incoming  
 Outgoing  
 Internal

**Direction of Attachments**

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.

- 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.	<input type="button" value="Move to Quarantine"/>
Spam	Spam includes messages with unwanted content, including undesirable URLs.	<input type="button" value="Move to Junk"/>
Graymail	Graymail is mail that has been determined to be marketing, social, or junk.	<input type="button" value="No Action"/>

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

- Click on **Save and Apply**.

**Policy: THE\_Emailsec\_2**

**Message Source**

**Journal Address**

**Secure Email Gateway (SEG)**

**Messages Analysis**

**Automated Remediation Policy**  Off

**Visibility & Remediation**

**Imported Domains**

**Automated Remediation**

**Save and Apply**



## **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.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

## Task – Configure Exchange Online.

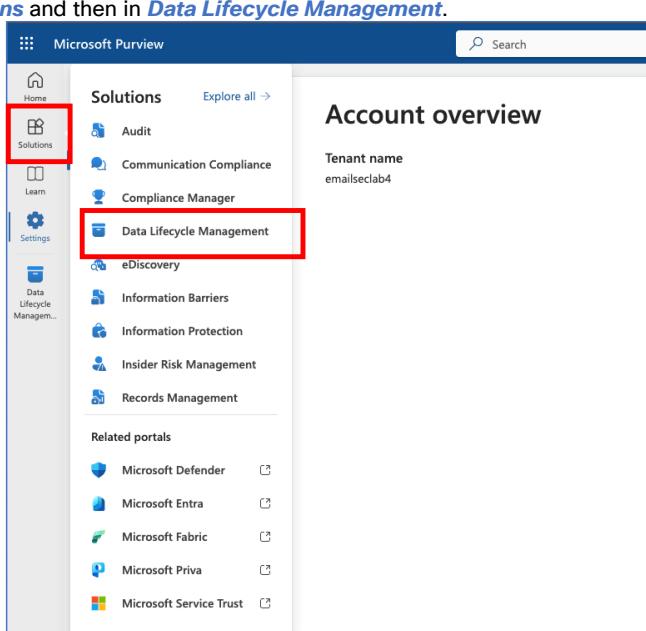
In this task, we will configure Exchange Online and review the permissions automatically configured in the previous step.

1. 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**.



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



3. 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.

In the new Microsoft Pureview 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)



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

The screenshot shows the Microsoft Purview interface with the 'Data Lifecycle Management' section selected in the sidebar. The main content area is titled 'Data Lifecycle Management settings' and shows the 'Exchange (legacy)' tab selected under 'Adaptive protection'. A message indicates that undeliverable journal reports have been saved to an alternative mailbox. A 'Replace' button is visible.

- Click on "**Data Lifecycle management**".

The screenshot shows the Microsoft Purview interface with the 'Data Lifecycle Management' section selected in the sidebar. The main content area is titled 'Overview' and displays information about data lifecycle management, including retention labels and policies. A red box highlights the 'Data Lifecycle Management' icon in the sidebar.

- Click on "**Exchange Legacy**" and on "**journal Rules**".  
If you see a rule created, please select and remove it.



Microsoft Purview

Search

New Microsoft Purview portal

Journal rules

As part of our commitment to customers, Microsoft continues to make improvements to our features. Although journaling content outside Microsoft 365 is still supported, please familiarize yourself with its limitations and considerations. Microsoft Purview solutions offer the most up-to-date customer experience by assisting customers to meet legal, regulatory, and organizational compliance requirements. Microsoft Purview manages email data in-place avoiding issues that may be caused by transmitting the data externally such as duplication or inability to deliver to a journaling destination.

Use journal rules to record all communications in support of your organization's email retention or archival strategy. Learn about journaling in Exchange Online

+ New rule Refresh

No data available

6. Click on “**New Rule**”

Microsoft Purview

Search

New Microsoft Purview portal

Journal rules

As part of our commitment to customers, Microsoft continues to make improvements to our features. Although journaling content outside Microsoft 365 is still supported, please familiarize yourself with its limitations and considerations. Microsoft Purview solutions offer the most up-to-date customer experience by assisting customers to meet legal, regulatory, and organizational compliance requirements. Microsoft Purview manages email data in-place avoiding issues that may be caused by transmitting the data externally such as duplication or inability to deliver to a journaling destination.

Use journal rules to record all communications in support of your organization's email retention or archival strategy. Learn about journaling in Exchange Online

+ New rule Refresh

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**.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

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**":



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

**Define journal rule settings**

Messages matching the rule's conditions will be delivered to the journaling address specified in the rule. [Learn more to manage journaling in Exchange Online](#)

**Send journal reports to \***

b1561ae4-bfc4-44af-bdca-49363af23613@beta.cmd.cisco.com

**Journal rule name \***

(Apply to all messages)

**Journal messages sent or received from \***

Everyone

A specific user or group

**Type of message to journal \***

All messages

Internal messages only

External messages only

**Next >** **Cancel**

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.

**Review journal rule and finish**

**Send journal reports to**  
b1561ae4-bfc4-44af-bdca-49363af23613@beta.cmd.cisco.com  
[Edit](#)

**Name**  
(Apply to all messages)  
[Edit](#)

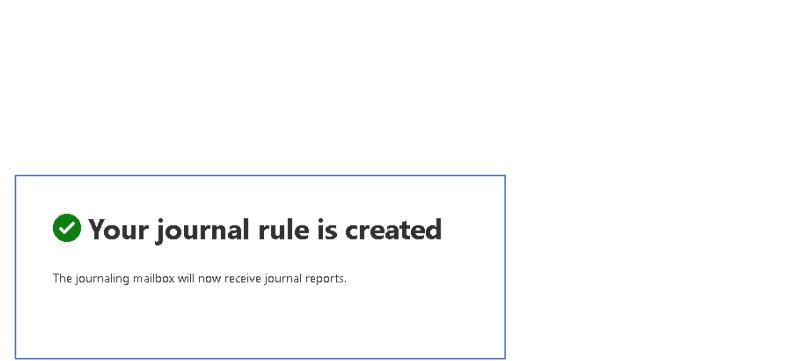
**Journal messages sent or received from**  
[Edit](#)

**Type of message to journal**  
All messages  
[Edit](#)

**Back** **Submit** **Cancel**

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**”.

3. Click on “**Add a connector**”.



The screenshot shows the Exchange admin center interface. On the left, there's a navigation sidebar with categories like Home, Recipients, Mail flow, Connectors (which is selected), Roles, Migration, and Mobile. Under Connectors, there are sub-options: High Volume Email (Preview), Alerts, Alert policies, and a connector named "High Volume Email (Preview)". The main content area is titled "Connectors" and contains a brief description: "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." Below this is a button labeled "+ Add a connector" which is highlighted with a red box. A "Refresh" button is next to it. To the right, there's a search bar and a table header with columns: Status, Name, From, and To. The table body says "No data available". At the bottom right, there are two small icons.

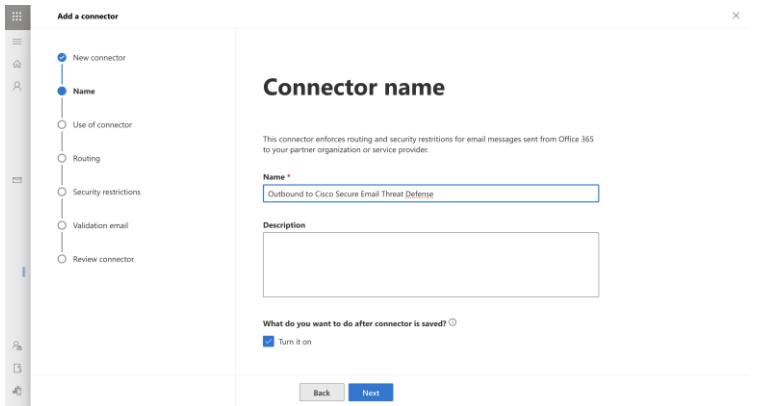
4. Select Connection From "**Office 365**" and Connection to "**Partner Organization**" and click **Next**

This is a screenshot of the "Add a connector" wizard. On the left, there's a sidebar with a tree view: "New connector" is selected, followed by "Name", "Use of connector", "Routing", "Security restrictions", "Validation email", and "Review connector". The main panel is titled "New connector" and contains the instruction: "Specify your mail flow scenario, and we'll let you know if you need to set up a connector." Below this, there are two sections: "Connection from" and "Connection to". In "Connection from", the radio button "Office 365" is selected and highlighted with a red box. In "Connection to", the radio button "Partner organization" is selected and highlighted with a red box. At the bottom right of the panel is a blue "Next" button.

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

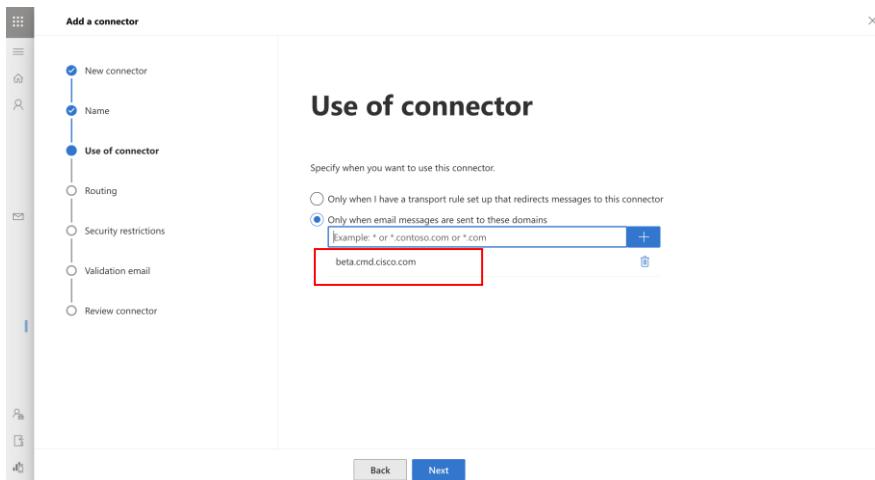


Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.



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**



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

**Add a connector**

**Routing**

How do you want to route email messages?

Specify one or more smart hosts to which Office 365 will deliver email messages. A smart host is an alternative server and can be identified by using a fully qualified domain name (FQDN) or an IP address.

Use the MX record associated with the partner's domain  
 Route email through these smart hosts

**Back** **Next**

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

**Add a connector**

**Security restrictions**

How should Office 365 connect to your partner organization's email server?

Always use Transport Layer Security (TLS) to secure the connection (recommended)  
 Connect only if the recipient's email server certificate matches this criteria  
 Any digital certificate, including self-signed certificates  
 Issued by a trusted certificate authority (CA)  
 Add the subject name or subject alternative name (SAN) matches this domain name:  
 Example: contoso.com or \*.contoso.com

**Back** **Next**

- Copy the journaling address to validate the connector. Click on “**Validate**”



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

**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.

Add a connector >

- New connector
- Name
- Use of connector
- Routing
- Security restrictions
- Validation email
- Review connector

## Validation email

Specify an email address for an active mailbox that's on your partner domain. You can add multiple addresses if your partner organization has more than one domain.

Example: user@contoso.com  +

d24ff1c54-c134-40c4-9a30-dea6a8322e28@beta.cmd.cisco.com

Back

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

Validation successful

Task	Status
> Send test email	Succeed

11. Click on “[Create Connector](#)”



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

Add a connector

**Review connector**

**Mail flow scenario**  
From: Office 365  
To: Partner organization

**Name**  
Outbound to Cisco Secure Email Threat Defense  
[Edit name](#)

**Status**  
Turn it on after saving  
[Edit status](#)

**Use of connector**  
Use only for email sent to these domains: beta.cmd.cisco.com  
[Edit use](#)

**Routing**  
Use the MX record associated with the partner's domain.  
[Edit routing](#)

**Security restrictions**

[Back](#) [Create connector](#)

**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.



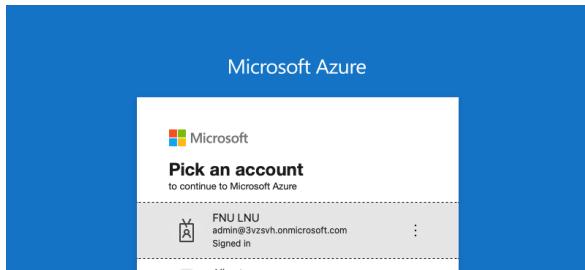
Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

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

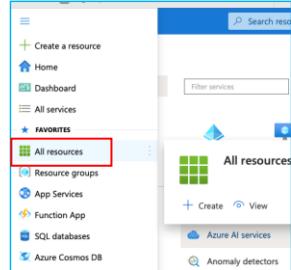
Frequently, customers ask about the permissions required to integrate ETD with Microsoft to be able to use the Read-Write mode on ETD.

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

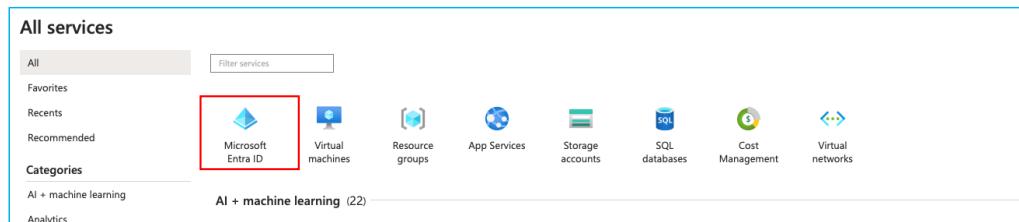
1. Open the Azure portal with the O365 account provided for this lab:  
<https://azure.microsoft.com/en-us/get-started/azure-portal/>



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

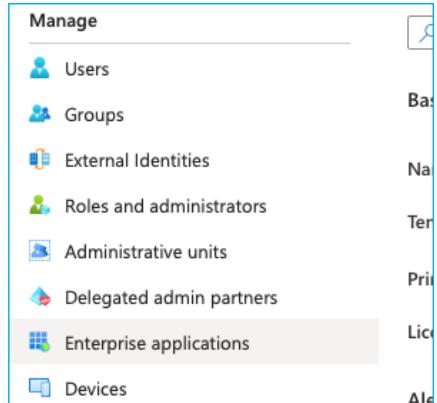


3. Click on "**Microsoft Entra ID**".



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

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 'Overview', 'Manage' (with 'All applications' selected), and 'Security'. The main area displays a table of applications. A single row is shown, with the 'Name' column containing 'Cisco Secure Email...' and the 'Application ID' column containing 'f657cena-48f8-47df-aee...'. The entire row is highlighted with a red box.

Name	Application ID	Homepage URL	Created on	Certificate Expiry St...	Active Certificate Ex...	Identifier URI (Entity...
Cisco Secure Email...	f657cena-48f8-47df-aee...	23b06408-7389-43a1-a9...	https://portal.cmd.cisco...	20/09/2023	-	23b06408-7389-43a1-a9...

6. Click on Permissions

7. 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



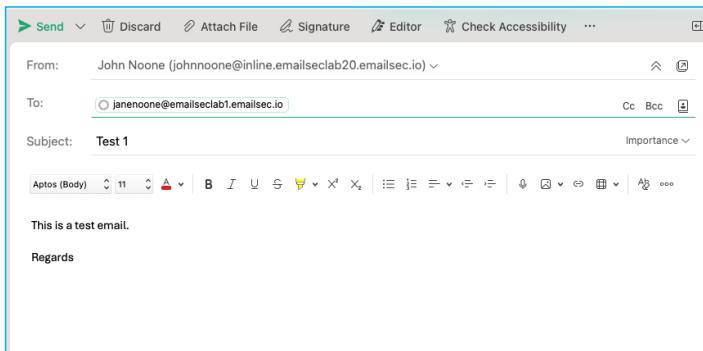
Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

## 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.

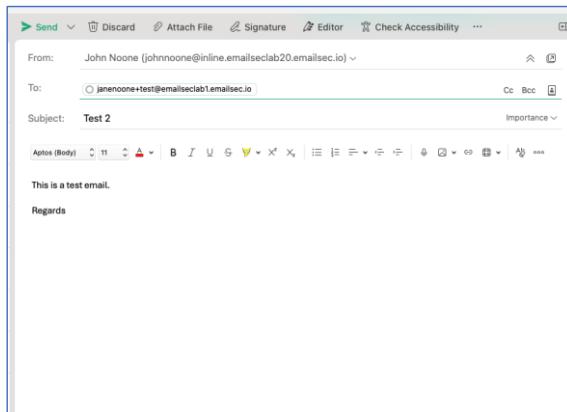
You will test all the options to verify that everything is working as expected.

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:

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.

Verdict	Action	Rule	Received	Sender ID	Recipients	Subject	Direction
—	—	—	Jan 27 2025 02:13 PM CST	Greg Barnes (prebame) <prebame...>	janenoone+test@emailseclab2@emailsec...	test 3	Incoming
—	—	—	Jan 27 2025 02:03 PM CST	Greg Barnes (prebame) <prebame...>	janenoone@emailseclab2@emailsec...	Test 2	Incoming
—	—	—	Jan 27 2025 01:42 PM CST	Greg Barnes (prebame) <prebame...>	janenoone@emailseclab7@emailsec...	test	Incoming

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.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

6. 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.

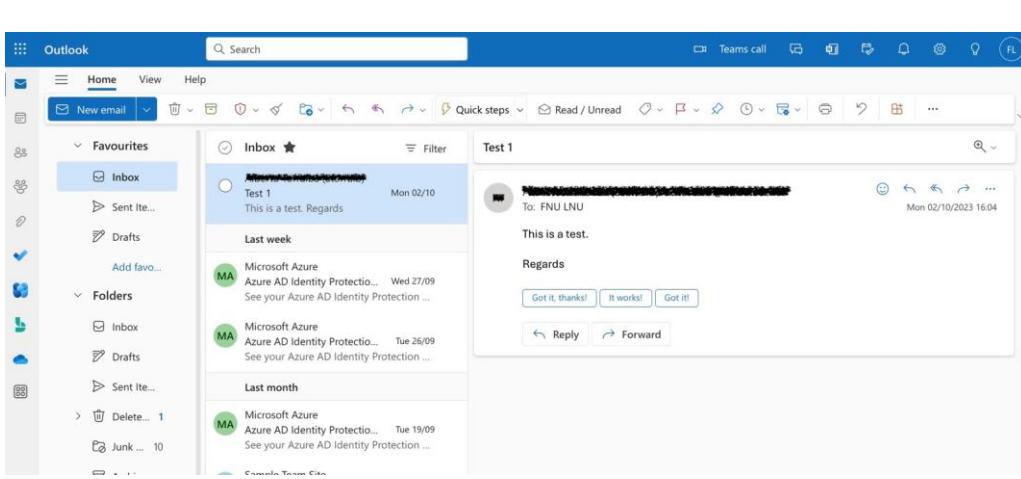
The screenshot shows the Microsoft Outlook inbox interface. On the left, there's a sidebar with 'Favourites' (Inbox, Sent Itms., Drafts) and 'Folders' (Inbox, Drafts, Sent Itms., Junk E..., Archive, Notes, Conversations). The main area shows an 'Inbox' folder with two items: 'TEST 2' (Mon 02/10, 'this is a test.') and 'Test 1' (Mon 02/10, 'This is a test. Regards'). Below these are 'Last week' and 'Last month' sections, each containing a single Microsoft Azure message about Azure AD Identity Protection. At the bottom, there's a 'Sample Team Site' message from 'SS' (Sat 16/09, 'You've joined the Sample Te...'). On the right, a preview pane titled 'Test 1' shows the content of the 'Test 1' email.

7. 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 dashboard with the 'Messages' tab selected. There are three messages listed in a table. Above the table, there are four buttons: 'Reclassify' (highlighted with a red box), 'Keep verdict' (highlighted with a red box), 'Request action' (highlighted with a red box), and 'Move to Junk'. To the right of the table are 'Cancel' and 'Update' buttons. The table columns include Verdict, Action, Rule, Received, Sender, Recipients, Subject, and Direction. The first message has a checked 'Verdict' box and a checked 'Action' box. The second message has an unchecked 'Verdict' box and an unchecked 'Action' box. The third message has an unchecked 'Verdict' box and an unchecked 'Action' box. The 'Received' column shows dates like Jan 27 2025 02:13 PM CST. The 'Sender' column lists Greg Barnes (grebam...). The 'Recipients' column lists johnnoone+test@em... and test 3. The 'Subject' column lists 'Test 2'. The 'Direction' column shows 'Incoming' for all messages.

8. 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.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

## 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 'Business' (0 Scam, 0%), 'Unwanted mail' (0 Spam, 0%, 0 Graymail, 0%), and a timeline graph showing message volume from 6pm to 2pm. At the bottom, a 'Quick message filter' section shows 0 matches found and filters for Retrospective verdicts, Messages in quarantine, and Message rules.

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	
Jane	Noone	
Title	Business Phone	Mobile Phone
Email Address		
janenoone@emailseclabXX.emailsec.io		
Enter multiple email addresses separated by comma		

**Cancel** **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



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

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			[janenoone@email...]	Juan Torribia	Feb 04 2025 10:14 AM GMT+1	Juan Torribia	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 Mailer interface. At the top, it says "Free online fake mailer with attachments, encryption, HTML editor and advanced settings...". Below that are input fields for "From Name", "From E-mail", "To", "Subject", "Attachment" (which is currently empty), and "Content-Type" (set to "text/plain"). There is a large text area for "Text". At the bottom, there is a CAPTCHA section with a checkbox for "I am human" and a reCAPTCHA logo. Below the CAPTCHA are "Send" and "Clear" buttons.

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



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

# EUREKA'S MAILER

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

From Name: Veronica Sirroll  
From E-mail: veronica@pepe.com  
To: johnnoone@post100.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   
[hcaptcha](#) [Privacy - Terms](#)

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   
[hcaptcha](#)

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



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.



- 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>

This screenshot shows the Microsoft Defender interface, specifically the Quarantine section. On the left, there's a navigation sidebar with various security modules like Home, Investigation & response, Threat intelligence, and Microsoft Sentinel. The main pane displays a list of emails in quarantine, filtered by 'Time received: Last 30 days'. Two messages are listed: one from 'veronica@pepe.com' and another from 'diego@pepe.com', both marked as 'Malware'. Below this, a modal window titled 'Release email to recipients' is open, containing options to release the email to all recipients or specific ones, and checkboxes for sending a copy to other recipients and submitting the message to Microsoft for detection improvement. 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**".



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

The screenshot shows the 'Administration' section of the Cisco Secure Email Threat Defense interface. On the left, there's a sidebar with links for Account, Home, Messages, Insights, Policy, and Administration. The 'Administration' link is currently selected and highlighted in blue. In the main content area, there's a heading 'High Impact Personnel' with a dropdown arrow. Below it is a table with columns: First Name, Last Name, Title, Business Phone, Mobile Phone, Email Address, Created By, Date Created, Last Updated By, Date Last Updated, and Actions. There are three rows in the table. The first row has a red box around the 'Last Name' column value 'None'. The second row has a red box around the 'Last Name' column value 'None'. The third row has a red box around the 'Last Name' column value 'Stroll'.

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' section of the Cisco Secure Email Threat Defense interface. On the left, there's a sidebar with links for Account, Home, Messages, Insights, Policy, and Administration. The 'Administration' link is currently selected and highlighted in blue. In the main content area, there's a heading 'High Impact Personnel' with a sub-section 'Impersonations Last 30 Days'. Below it is a table with columns: First Name, Last Name, Title, Business Phone, Mobile Phone, Email Address, Created By, Date Created, Last Updated By, Date Last Updated, and Actions. There are two rows in the table. The first row has a red box around the 'Last Name' column value 'None'. The second row has a red box around the 'Last Name' column value 'None'.

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

The screenshot shows the 'Timeline' and 'Verdict & Techniques' sections of the Cisco Secure Email Threat Defense interface. At the top, there's a timeline bar with a marker at 'Apr 24 2024 02:16:02 PM'. Below it, there's a section labeled 'Received Incoming'. In the 'Verdict & Techniques' section, there's a 'Spam' button and a 'Remediate & Reclassify' button. A red box highlights a yellow box labeled 'USER IMPERSONATION'. Below it, a message says 'Detected a possible impersonation for high impact user Veronica Stroll'.



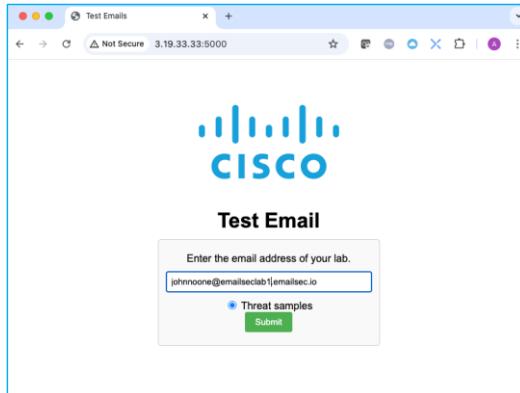
## Task – “Attack” your environment.

### 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

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.**



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

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

The screenshot shows the ETD dashboard with the 'Messages' tab selected. At the top, there are two donut charts: one for 'Threats' (4 Total) and one for 'Messages' (7 Total). Below these are two line graphs: 'Trend comparison' for the last 24 hours and 'Mon, Jan 27' for threats and messages. The main area lists 7 results as of Jan 27 2025 02:44 PM CST, filtered by 'Verdict & Techniques'. The results include:

Verdict	Action	Date	Received	Sender ID	Recipients	Subject	Direction
BEC	—	Jan 27 2025 02:43 PM CST	Veronica Stroll <john...	johnnone@emailsec...	test	Incoming	
Malicious	—	Jan 27 2025 02:38 PM CST	Veronica Stroll <john...	johnnone@emailsec...	This is a test	Incoming	
BEC	—	Jan 27 2025 02:36 PM CST	Veronica Stroll <john...	johnnone@emailsec...	This is a test	Incoming	
Malicious	—	Jan 27 2025 02:32 PM CST	Greg Barnes (grebarn...	johnnone@emailsec...	test rep	Incoming	
—	—	Jan 27 2025 02:19 PM CST	Greg Barnes (grebarn...	johnnone+test@em...	Test 3	Incoming	
—	—	Jan 27 2025 02:03 PM CST	Greg Barnes (grebarn...	johnnone@emailsec...	Test 2	Incoming	
—	—	Jan 27 2025 01:42 PM CST	Greg Barnes (grebarn...	johnnone@emailsec...	test	Incoming	

At the bottom, there are links for 'Privacy policy' and 'Terms of service'.

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

The screenshot shows a detailed view of a message identified as a 'Phishing' threat. The message was received on April 24 2024 03:08 PM (GMT+0). The subject is 'Options for VoIP phone services'. The message ID is #77396410554.31361672899415434556440@verifian-linx.internal.cloudapp.net. The message content includes several redacted links and attachments. The 'Sender Information' section shows the sender's name as 'John Doe' and email as 'john.doe@verifian-linx.internal'. The 'Sender Messages (Last 30 Days)' section shows a timeline of messages sent by this user. The 'Attachments' section indicates there are no attachments.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

- 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.

- Open one message and click on “Conversation view”.

The screenshot shows the Cisco Secure Email Threat Defense interface. On the left is a navigation sidebar with 'Messages' selected. The main area displays a message detail page for an incoming email. The 'Verdict & Techniques' section shows 'Phishing' as the verdict. The 'Conversation View' button is highlighted with a red box in the top right corner of the main content area.

- 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 central part of the screen features a large circular icon with two '+' symbols, which is highlighted with a red box. Another red box highlights the same '+' symbols on the circular icon. Below this, there is a table with columns for Verdict, Action, Rule, Received, Sender, Recipients, Subject, and Direction. The 'Verdict' column shows 'Phishing'. The 'Received' column shows 'Apr 24 2024 ...'. The 'Sender' column shows 'VoIP Central <VoIP...>'. The 'Recipients' column shows 'johnnoone@pod100...'. The 'Subject' column shows 'Options for VoIP phone services'. The 'Direction' column shows 'Incoming'.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

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. The search bar at the top contains the query "Search results For: Solar-Power In Homes". Below the search bar, there are several messages listed:

- Solar Energy Systems**: A message from "Solar Energy Systems <SolarEnergySystems@sniffishic.download>" dated 12:50. It includes a note about blocked content and a link to trust the sender.
- Premium Pure Forkolin**: A message from "Premium Pure Forkolin Ellen: Melissa McCarthy, On..." dated 12:49. It says "No preview is available."
- Mail**: A message from "Programma для электрон...<k12z3y4 M-PM-IM-PM->M-QM-^..." dated 12:49.
- Business Degree Classes**: A message from "Business Degree Classes Want to get a Business Degr..." dated 12:48. It says "Want to get a Business Degree? See...".
- AT**: A message from "Alberto Torralba (atorralb)" dated 12:48. It says "Text 1" and "This is a test. Regards".

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 email compose window. The recipient field "To" is populated with "Joni Sherman". The subject line is "Fw: " Search results For: Solar-Power In Homes ". The message body contains the forwarded content from the previous screenshot, including the search results and the "Search results For: Solar-Power In Homes" link.

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

<input type="checkbox"/> Verdict	Action	Rule	Received	Sender (Display Name)	Recipients	Subject	Direction	Actions
<input type="checkbox"/>			Apr 24 202...	John Noone <Jo...	veronicastrolli@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**"

The screenshot shows the Cisco Secure Email Threat Defense dashboard. On the left, there's a sidebar with options like Account, Home, Messages (which is selected), Insights, Policy, and Administration. The main area displays a message from John Noone to Veronica Stroll. The subject is "Fw: " Search results For: Solar-Power In Homes ". Below the subject, it says "Internal (Received Apr 24 2024 03:14 PM GMT+2) Message ID: A58P193MB1544E5E90DE651B3CCF1E77FD102@A58P193MB1544.EURP193.PROD.OUTLOOK.COM>". There are buttons for Preview Email, Download EML, and Conversation View, with the latter being highlighted by a red box. Below this, there's a Timeline section showing the message was received at 03:14:52 PM on April 24, 2024, and a Verdict & Techniques section indicating no verdict details available.

12. Your output should be as the next picture.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

The screenshot shows the Cisco Secure Email Threat Defense interface. At the top, there's a navigation bar with account information ('Account Motofan100'), a search bar ('Juan'), and various icons. Below the bar is a sidebar with links to Home, Messages (which is selected), Insights, Policy, and Administration. The main content area displays a single message in a table format. The message details are as follows:

Verdict	Action	Rule	Received	Sender (Display Name/Email)	Recipients	Subject	Direction
			Apr 24 2024 ...	Solar Energy Syst...	johnnoone@pod100...	Ø "Search results For: Solar-Power In Homes"	Incoming
			Apr 24 2024 ...	John Noone <JohnN...	veronicastroll@pod1...	Ø Fw: "Search results For: Solar-Power In Homes"	Internal

At the bottom of the page, there are links for 'Privacy policy' and '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 with a search bar ('Search Messages for a URL, subject line, recipient, or IP') containing 'Gregory'. The results section shows 7 messages received on Jan 27, 2025, at 02:44 PM CST. The messages are listed in a table with the following details:

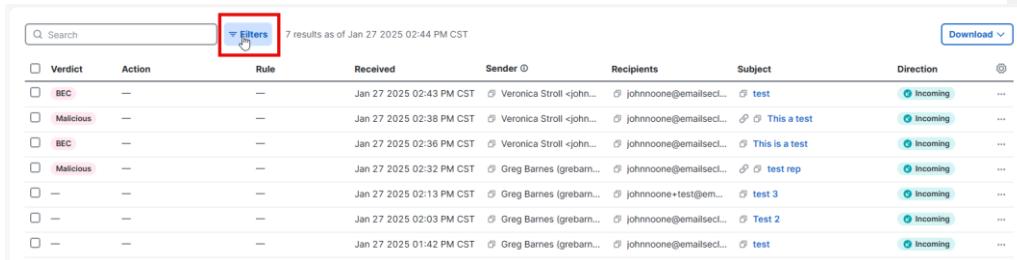
Verdict	Action	Rule	Received	Sender	Recipients	Subject	Direction	Timestamp
BEC	—	—	Jan 27 2025 02:43 PM CST	Veronica Stroll <john...	johnnoone@emailsec...	Ø test	Incoming	...
Malicious	—	—	Jan 27 2025 02:38 PM CST	Veronica Stroll <john...	johnnoone@emailsec...	Ø This a test	Incoming	...
BEC	—	—	Jan 27 2025 02:36 PM CST	Veronica Stroll <john...	johnnoone@emailsec...	Ø This is a test	Incoming	...
Malicious	—	—	Jan 27 2025 02:32 PM CST	Greg Barnes (gabarn...	johnnoone@emailsec...	Ø test rep	Incoming	...
—	—	—	Jan 27 2025 02:19 PM CST	Greg Barnes (gabarn...	johnnoone@test@email...	Ø test 3	Incoming	...
—	—	—	Jan 27 2025 02:03 PM CST	Greg Barnes (gabarn...	johnnoone@emailsec...	Ø Test 2	Incoming	...
—	—	—	Jan 27 2025 01:42 PM CST	Greg Barnes (gabarn...	johnnoone@emailsec...	Ø test	Incoming	...

At the bottom of the page, there are links for 'Privacy policy' and 'Terms of service'.



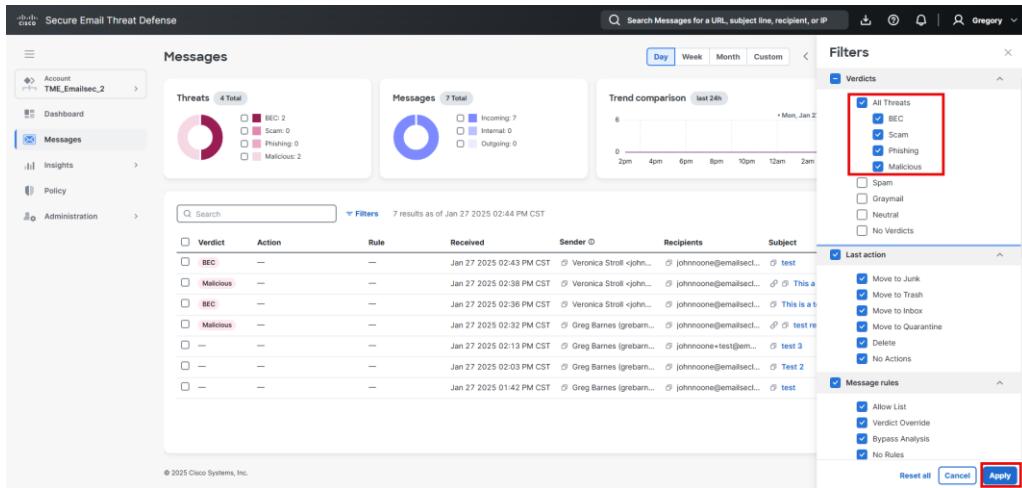
Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

2. Click on the “filters” text.



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

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



The screenshot shows the Cisco Secure Email Threat Defense interface. On the left, there's a navigation sidebar with 'Account TME\_Emailsec\_2', 'Dashboard', 'Messages' (which is selected), 'Insights', 'Policy', and 'Administration'. The main area displays a 'Messages' section with a pie chart showing Threats (4 Total) and a donut chart showing Messages (7 Total). Below these are two small charts: 'Trend comparison last 24h' and 'Mon, Jan 2'. To the right, a large 'Filters' dialog box is open. In the 'Verdicts' section, the 'All Threats' checkbox is checked, along with 'BEC', 'Scam', 'Phishing', and 'Malicious'. There are also other filter options like 'Spam', 'Graymail', 'Neutral', and 'No Verdicts'. Under 'Last action', several actions are listed with checkboxes: 'Move to Junk', 'Move to Trash', 'Move to Inbox', 'Move to Quarantine', 'Delete', and 'No Actions'. Under 'Message rules', options include 'Allow List', 'Verdict Override', 'Bypass Analysis', and 'No Rules'. At the bottom of the dialog are 'Reset all', 'Cancel', and a red-bordered 'Apply' button.



## 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. A single email from 'Breathaking Alaskan Cruises' is selected. The subject line is 'You should consider going on an Alaskan Cruise'. A warning message at the top of the email body reads: 'This message may not be sent by the sender that's displayed. If you aren't certain this message is safe, please be cautious when interacting with this email, and avoid clicking on any links or downloading attachments that are on it. Click here to learn more.' Below the message, there is a preview of the email content which includes several links and attachments.

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.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

Secure Email Threat Defense

Messages

Threats 4 Total

Messages 4 Total

Trend comparison last 24h

Message selected | Reclassify

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 (gbarn...	johnnoone@emailsec...	test rep	Incoming

Reclassify

Select verdict

- BEC
- Scam
- Phishing
- Malicious
- Graymail
- Neutral
- Keep verdict

Request action

Cancel Update

Rows per page 100

Privacy policy Terms of service

#### 4. Click on the Reclassify dropdown menu.

Secure Email Threat Defense

Messages

Threats 4 Total

Messages 4 Total

Trend comparison last 24h

Message selected | Reclassify

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 (gbarn...	johnnoone@emailsec...	test rep	Incoming

Reclassify

Select verdict

- BEC
- Scam
- Phishing
- Malicious
- Graymail
- Neutral
- Keep verdict

Request action

Cancel Update

Rows per page 100

Privacy policy Terms of service

#### 5. Select "Keep verdict".



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

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.

Verdict	Action	Received	Sender	Recipients	Subject	Direction
<input checked="" type="checkbox"/> BEC	—	7/2025 02:43 PM CST	Veronica Stroll <john...>	johnnone@emailsec...	test	Incoming
<input type="checkbox"/> Malicious	—	7/2025 02:38 PM CST	Veronica Stroll <john...>	johnnone@emailsec...	② This a test	Incoming
<input type="checkbox"/> BEC	—	7/2025 02:36 PM CST	Veronica Stroll <john...>	johnnone@emailsec...	② This is a test	Incoming
<input type="checkbox"/> Malicious	—	7/2025 02:32 PM CST	Greg Barnes (gbarn...)	johnnone@emailsec...	② test rep	Incoming

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

Verdict	Action	Rule	Received	Subject	Direction	
<input checked="" type="checkbox"/> BEC	—	—	Jan 27 2025 02:43 PM CST	johnnone@emailsec...	test	Incoming
<input type="checkbox"/> Malicious	—	—	Jan 27 2025 02:38 PM CST	johnnone@emailsec...	② This a test	Incoming
<input type="checkbox"/> BEC	—	—	Jan 27 2025 02:36 PM CST	Veronica Stroll <john...>	② This is a test	Incoming
<input type="checkbox"/> Malicious	—	—	Jan 27 2025 02:32 PM CST	Greg Barnes (gbarn...)	② test rep	Incoming

Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

7. Click on **Update**

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

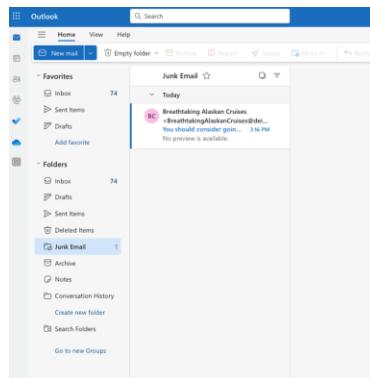
8. You should see this information.

Verdict	Action	Rule
<input type="checkbox"/> BEC	<span style="background-color: pink; border: 1px solid pink; padding: 2px;">Move Requested</span>	—

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



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.



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.

[Back to Messages](#)

**Subject:** You should consider going on an Alaskan Cruise

[Preview Email](#) [Download EML](#) [Conversation View](#)

[Incoming](#) (Received Apr 24 2024 03:16 PM GMT+2) **Message ID:** <171396457109.5136.7791883840582384316@motofan-linux.internal.cloudapp.net> [Not Read](#)

**Timeline**

Date	Action	Verdict	Technique
Apr 24 2024 03:16:14 PM	Received Incoming		
Apr 24 2024 03:16:18 PM		Verdict Phishing Automatic	
Apr 24 2024 03:24:04 PM		Junk Manual	Remediated by Juan Torralba

**Verdict & Techniques**

- Phishing**

**LOW CONTENT REPUTATION**  
Email content has a bad reputation

[Remediate & Reclassify](#)

### 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.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

## 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*”.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

3. Click on “[Add New Client](#)”.

4.

5. Fill in the “[Client Name](#)” box. We can name it “[Postman](#)”, and then click on “[Submit](#)”.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

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  
GVsQIL22F7Qyc1waCKbgmef3DE8EtP8-gUzEWgmgOE

7. Click on “**Close**”

8. Open “**Postman**” application

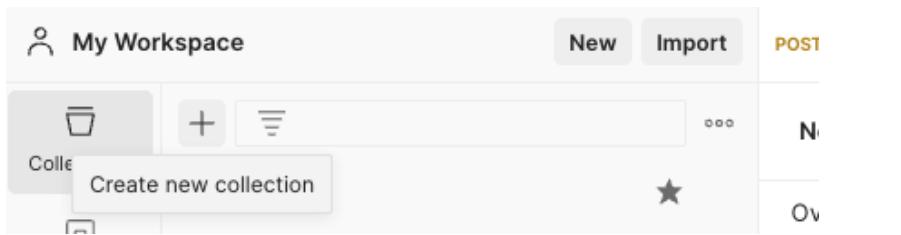
If you don't have the Postman application installed, you can go to Appendix A and check the steps to create an account or install the application on your desktop.

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

9. Create a “New collection”.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.



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

**ETD LAB BETA**

Overview Authorization Pre-request Script Tests Variables Runs

Speed up your work with collection templates NEW

RESTful API basics Authorization me... API testing basics More templates

Created by You  
Created on 03 Oct 2023, 3:49 PM

**ETD LAB BETA**

Make things easier for your teammates with a complete collection description.

[View complete documentation →](#)

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.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

The screenshot shows the Postman interface with the following details:

- Method:** GET
- URL:** https://api.beta.etd.cisco.com/v1/oauth/token
- Headers:** (6) - This tab is highlighted.
- Body:** None
- Pre-request Script:** None
- Tests:** None
- Settings:** None
- Query Params:** A table with one row and two columns. The first column is "Key" and the second is "Value". Both are currently empty.

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.

The screenshot shows the Postman interface with the following details:

- Method:** POST
- URL:** https://api.de.etd.cisco.com/v1/oauth/token
- Headers:** (10) - This tab is highlighted.
- Body:** None
- Pre-request Script:** None
- Tests:** None
- Settings:** None
- Headers Table:**

Key	Value	Description	Actions
x-api-key	hGEauJ04Vyi3WLAs5HfjuA12RstqT7dgf7mDaxKTL		Bulk Edit Presets
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**”.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

The screenshot shows the Postman interface with the following details:

- Request Type:** POST
- Collection:** ETD API Search / ETD Token Request
- URL:** https://api.beta.etd.cisco.com/v1/oauth/token
- Method:** POST
- Authorization:** Basic Auth (selected)
- Headers:** (8) (not explicitly listed in the screenshot)
- Body:** (empty)
- Pre-request Script:** (empty)
- Tests:** (empty)
- Settings:** (empty)
- Cookies:** (empty)

The authorization section shows:

- Type: Basic Auth
- Username: 1515c3bd-8e3a-4d30-9784-a3eeb42be700
- Password: zNldtYg4maJobRlA9eF-TPlzECU5xCuN

The response details are as follows:

- Status: 200 OK
- Time: 2.79 s
- Size: 103 KB
- Save as Example

The response body is displayed in JSON format:

```
1 "accessToken": "eyJhbGciOiJIUzI1NiIsInRSclIkpXVCJ9.eyJleHAiOiJzNDIyZmDgsImlhdcI6MTY5NjMzODc5OCwiC3ViIjoiYXBplwNsawVudCis
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.

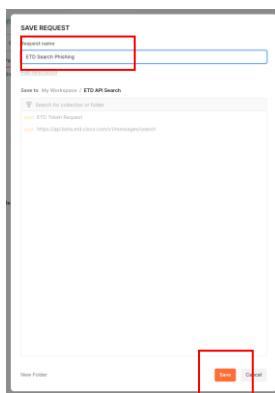
The screenshot shows the Postman interface. At the top, there is a search bar labeled "Search Postman". Below it, a list of requests includes "POST ETD Token Request" with a red box around its "+" button. To the right of the list are buttons for "Invite", "Settings", "Upgrad", "Save", and "Send". The URL field contains "v1/oauth/token". Below the URL field are tabs for "Pre-request Script", "Tests", and "Settings". A "Cookies" tab is also visible.

2. Click on **Save**.

The screenshot shows the Postman interface with an "Untitled Request" tab. The "Save" button is highlighted with a red box. The request details show a "GET" method, URL "Enter URL or paste text", and a table for "Query Params".

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>



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedford Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

And Select **Post**.

The screenshot shows the Postman interface with a POST request to `https://api.beta.etd.cisco.com/v1/messages/search`. The 'Authorization' tab is selected. A red box highlights the URL field.

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

The screenshot shows the Postman interface with the 'Authorization' tab selected. A red box highlights the 'Authorization' tab. The 'Type' dropdown is set to 'Bearer Token'. The 'Token' field is empty.

6. Copy the Access Token from the previous task.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

HTTP ETD API Search / ETD Search Phishing

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

Authorization: Bearer Token

Token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOiE2OTY4NDU2MzgslmhdC16MTY5Njg0MjAzaCwic3VljiqjYXBpLWNsaWvuClsmf1ZC16InB1mxpyYlhcgkILCjbGlbRJZC16Ie1MTViM2JkLThiM2EtNGQzMC05NzYOLWEzZWVnDjIZTcwMCIslnRlbmFudElkjoiYjE1NjFhZTQ1YmZjNC00NGFmLWJkY2EtNDkzNjNhZjznJEzln0.rSWTxelA2rgiqEab1RlmiT8He0PTThyNxF7wGgLrc

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

Params Authorization 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.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

POST ETD Search Phishing

POST ETD Token Request

No Environment

HTTP ETD API Search / ETD Search Phishing

Save Send

Params Authorization Headers (3) Body Pre-request Script Tests Settings Cookies

Body Type: raw

```

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

```

- 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]

- Click on **Send**.



```

POST /v1/messages/search
Content-Type: application/json

{
  "verdicts": [
    "phishing"
  ],
  "timestamp": [
    "2023-10-09T06:00:00Z",
    "2023-10-09T08:00:00Z"
  ]
}

```

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

```

{
  "data": [
    {
      "messages": [
        {
          "clientIP": "52.137.113.198",
          "direction": "incoming",
          "domains": "3zvzn.onmicrosoft.com",
          "fromAddress": "office@movenpick.rs",
          "toAddress": "mailto:10.13.183.93#45c8-89fc-3902d099297",
          "subject": "[REDACTED]",
          "toAddresses": [
            "joni@3zvzn.onmicrosoft.com"
          ],
          "internetMessageId": "<2927347ba5cc73f017a9939e7ef0d90@localhost.localdomain>",
          "replyTo": [
            "office@movenpick.rs"
          ],
          "returnPath": "office@movenpick.rs",
          "serviceIP": "10.13.183.100",
          "subject": "Circuit Veneta Padova Verona Lecul di Garda",
          "toAddresses": [
            "joni@3zvzn.onmicrosoft.com"
          ],
          "timestamp": "2023-10-09T07:48:12Z",
          "url": [
            "http://client.campanigndesde.yo/u.php?p=30da",
            "http://client.campanigndesde.yo/to.to",
            "https://onlined.bisad1.repl.co/hey/index.php",
            "http://client.campanigndesde.yo/u.php?p=4bm/rs/E7w/ltw/4Bb/rs",
            "http://www.vision-nl.biz/movendic",
            "http://www.vision",
            "http://www.vision-nl",
            "http://www.movenpick.rs",
            "http://client.campanigndesde.yo/t1.php?p=",
            "http://www.vision-nl.biz/movenpick/images/2.jpg?count"
          ],
          "verdict": {
            "isManualVerdict": false,
            "timestamp": "2023-10-09T07:48:15Z",
            "category": "phishing"
          }
        }
      ]
    }
  ]
}

```

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

<https://jsonpathfinder.com/>

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



```

1: {
2:   "date": [
3:     {
4:       "messages": [
5:         {
6:           "clientIP": "62.157.111.158",
7:           "direction": "incoming",
8:           "domain": "3zvzh.onmicrosoft.com",
9:           "fromAddress": "Defeating.Diabetes@writer.pacecf.us",
10:          "id": "e3244c92-288f-42c9-b5e3c8073155d8",
11:          "mailbox": "admin@3zvzh.onmicrosoft.com",
12:          "internetMessageId": "<9977165-Goatskin7114719-f8f706c398feec43df11ad3cb0470llan.anderson@acmepackets.net><sid=1>",
13:          "returnPath": "Defeating.Diabetes@writer.pacecf.us",
14:          "serverIP": "10.13.182.230",
15:          "subject": "Mysterious \"super starch\" saves diabetes",
16:          "toAddresses": [
17:              "admin@3zvzh.onmicrosoft.com"
18:          ],
19:          "timestamps": {
20:              "creation": "2023-10-02T15:36:13Z",
21:              "last": {
22:                  "http://defotolishere.pacecf.us/unsabing",
23:                  "http://defotolishere.pacecf.us/receive-mail-allan.anderson@acmepackets.net&sid=1",
24:                  "http://defotolishere.pacecf.us/receive",
25:                  "http://www.w3.org/1998/xhtml/1/DTD/xhtml1-strict.dtd",
26:                  "http://www.w3.org/1998/xhtml/1/DTD/xhtml1-transitional.dtd",
27:                  "http://defotolishere.pacecf.us/discontinue"
28:              },
29:              "renderName": "Defeating Diabetes",
30:              "secureEmailGateway": 0,
31:              "envelopeFrom": "admin@3zvzh.onmicrosoft.com"
32:          },
33:          "universal": [
34:              "admin@3zvzh.onmicrosoft.com"
35:          ]
36:      ],
37:      "clientIP": "62.157.111.158",
38:      "direction": "incoming"
39:  ]
40: }

```

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"
  ]
}
```



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

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

### Verdict `v string`

Search for messages with specific verdicts.

Enum:

`v [ spam, malicious, phishing, neutral, graymail, bcc, 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.



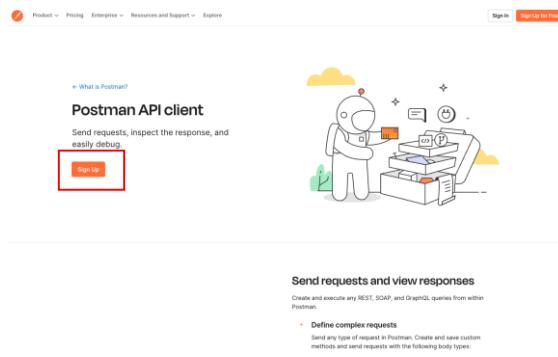
Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

## APPENDIX

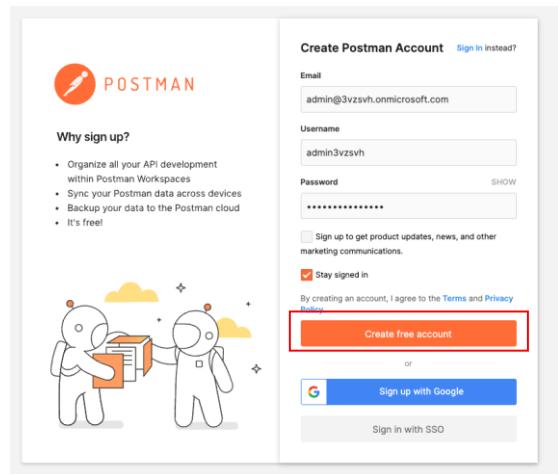
### Postman Installation

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**”.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedford Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

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 left sidebar shows 'My Workspace' with sections for 'Collections' (empty), 'Environments' (empty), and 'History' (empty). Below that is a section for creating collections. The main area shows 'My First collection' with 'First folder inside collection' and 'Second folder inside collection'. A modal window titled 'Use a template to quickly set up your workspace' offers options like 'API demos', 'API development', and 'API testing'. The top navigation bar includes 'Home', 'Workspaces', 'API Network', 'Explore', 'Overview', 'Search Postman', 'Invite', 'Upgrade', and 'Workspace Settings'.

6. Save and reserve the credentials for the lab.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedford Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

7. If you want, you can download a local client. Click on **Home**

The screenshot shows the Postman application interface. At the top, there is a navigation bar with links for 'Home', 'Workspaces', 'API Network', and 'Explore'. A search bar labeled 'Search Postman' is positioned next to the navigation. On the right side of the header, there are buttons for 'Invite', 'Upgrade', and workspace settings. Below the header, the main area is titled 'My Workspace'. It displays a collection tree under 'Collections' with two main items: 'My first collection' and 'Second folder inside collection'. Each item has several sub-folders. To the left of the collection tree, there is a section titled 'Create a collection for your requests' with a brief description and a 'Create Collection' button. On the right side of the workspace, there is a modal window titled 'Use a template to quickly set up your workspace' with options like 'API demos', 'API development', 'API testing', and 'More templates'. Below the modal, there are sections for 'About' (with a placeholder for a workspace summary), 'Contributors' (listing 'You'), and a link to 'View workspace activity'.

8. Click on "Download Desktop App"

This screenshot shows the same Postman interface as the previous one, but with a different focus. The left sidebar now includes a 'Download Desktop App' link under the 'What is Postman?' section. The main content area features sections for 'Recently visited workspaces' (showing 'My Workspace') and 'Explore popular APIs' (listing 'Salesforce Platform APIs', 'Postman API', and 'Day 05: Variables'). The overall layout is identical to the first screenshot, with the addition of the desktop app download link in the sidebar.



Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.

9. Select your SO and install the application.

The screenshot shows the Postman website. At the top, there's a navigation bar with links for Product, Pricing, Enterprise, Resources and Support, and Explore. On the far right, there's a red "Launch Postman" button. The main heading "Download Postman" is centered above a sub-headline: "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." Below this, there are two download buttons: "Mac Intel Chip" and "Mac Apple Chip". A note below the buttons says: "By downloading and using Postman, I agree to the [Privacy Policy](#) and [Terms](#)". There are also links for "Release Notes" and "Product Roadmap". A note at the bottom says: "Not your OS? Download for Windows (x64) or Linux (x64, arm64)".

**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 right side of the page shows the Postman application interface. It has a sidebar with sections like Home, Workspaces, API Network, and Explore. Under "Workspaces", it shows "Notion's Public Workspace". The main area is titled "Databases / Retrieve a database". It shows a GET request to "https://api.notion.com/v1/databases/{id}" with a "Send" button. Below this, there are tables for "Query params" and "Path Variables", both with columns for KEY, VALUE, DESCRIPTION, and Bulk Edit. The "Path Variables" table has one entry: "id" with value "DATABASE\_ID" and description "Required. Enter database id...". At the bottom, there are tabs for Body, Cookies, Headers, Test Results, and a "Save Responses" button. The "Body" tab shows a JSON response with code numbers 109 to 119. The "View complete collect..." link is visible at the bottom right of the interface.



Americas Headquarters  
Cisco Systems, Inc.  
San Jose, CA

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)

Copyright © 2025 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Cisco International Ltd, 9-11 New Square, Bedfont Lakes, Feltham, Middlesex, TW14 8HA, United Kingdom. Registered number: 2558939 Registered in England and Wales.