Communication Compliance

Lab Guide

Updated: February 12th, 2020

Table of Contents

Lab summary

Overview: With Microsoft 365 Compliance Center mitigating insider risk through communication compliance is easier than ever. Policies for monitoring code of conduct violations allow administrators to track repeated behaviors that break the code of conduct. Policies for monitoring for regulatory compliance allow administrators to track communications containing insider information.

Technologies: Microsoft 365, Microsoft Outlook, Microsoft Teams

Intended audience: ITDM, BDM

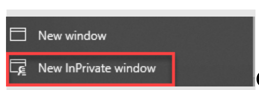
Total length: 10 Minutes

Before you begin

Tenant type and add-ins

Before you start you should have completed the "Getting started with Microsoft 365 Compliance Master Class Labs". If you have not completed this you will not be able to do this lab. You can find this document which you can download from https://aka.ms/m365masterclass-labs Each tenant will take 24 hours to provision so its important that you complete this prior to Tuesday when the event starts.

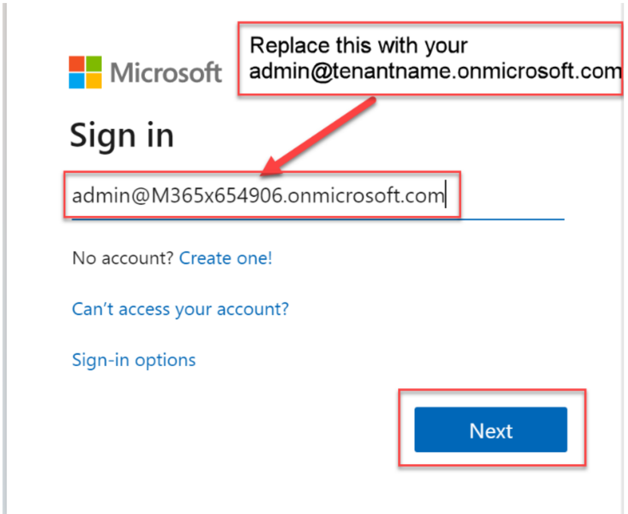
User accounts

Open an In-private browser (Edge) 

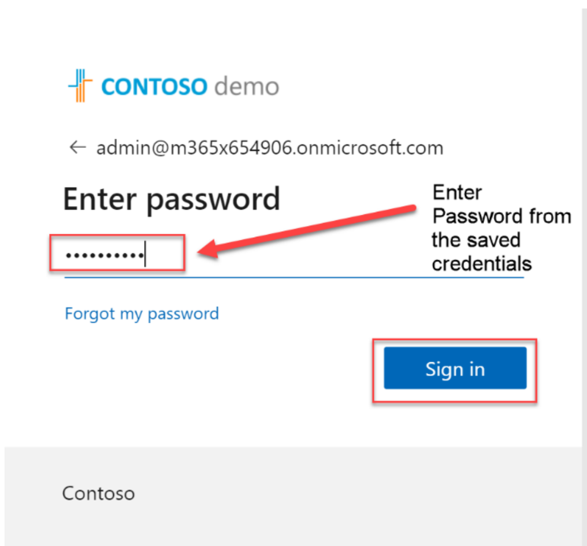
or New in-Cognito (Chrome) 

on your machine and then go to https://df.protection.office.com/insiderriskmgmt?viewid=overview&flight=enablem365compliancecenter,enableinsiderriskmgmt,enableinsiderriskservice,EnableFakeData

a) Enter the admin account username that you saved in "Getting started with Microsoft 365 Compliance Master Class Labs" to gain credentials.
b) Enter your admin credentials in the sign in as below and click NEXT

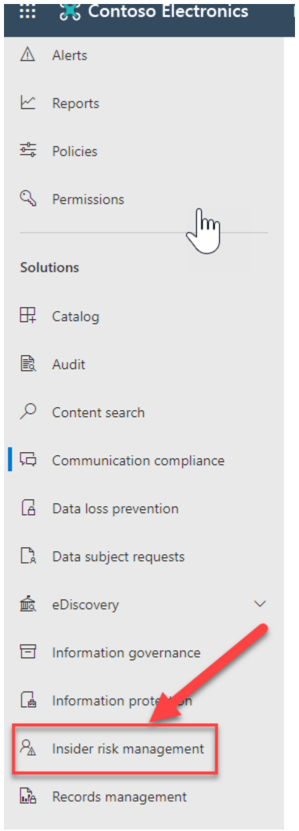


c) Enter the password and then click "Sign in"



Primary persona setup

1. Start an InPrivate Edge browser session and sign in to https://compliance.microsoft.com as admin@<Tenant>.onmicrosoft.com.
2. In the left-hand navigation click **Show all**.
3. Click **Communication Compliance**.



Lab steps

Complete the following one-time setup steps once to complete the configuration of your demo environment.

Add Communication Compliance Permissions to Admin user

1. In a browser, navigate to https://protection.office.com/permissions and login with the admin@<Tenant>.onmicrosoft.com credentials.
2. Click **+Create**.
3. Under **Name**, enter **M365 Communication Compliance**.
4. Click **Next**.
5. Click **Choose roles**.
6. Click **+Add**.
7. Search for and click **Supervisory Review Administrator**.
8. Click **Add**.
9. Click **+Add**.
10. Search for and click **Review**.
11. Click **Add**.
12. Click **+Add**.
13. Search for and click **Case Management**.
14. Click **Add**.
15. Click **Done**.
16. Click **Next**.
17. Click **Choose members**.
18. Click **+Add**.
19. Search for and click **MOD Administrator**.

20. Click **Add**.
21. Click **Done**.
22. Click **Next**.
23. Click **Create role group**.

Disable tenant DLP policies

24. In the left-hand navigation, click **Data loss prevention**.
25. Click **Policy**.
26. Click **U.S. Financial Data**.
27. In the **U.S. Financial** pane, next to **Status**, click **Edit**.
28. Click **No, keep it off. I'll turn it on later**.
29. Click **Save**.
30. Click **Close**.
31. Click **General Data Protection Regulation (GDPR)**.
32. In the **General Data Protection Regulation (GDPR)** pane, next to **Status**, click **Edit**.
33. Click **No, keep it off. I'll turn it on later**.
34. Click **Save**.
35. Click **Close**.

Create Offensive Language and Regulatory Compliance Policies

36. In a browser, navigate to https://compliance.microsoft.com and login with the admin@<Tenant>.onmicrosoft.com credentials.
37. In the left-hand navigation click **Show all**.
38. Click **Communication compliance**.
39. Close any **Welcome to…** popups.

40. At the top, click **Policies**.
41. Click **+Create policy**.
42. Click **Monitor for offensive language**.
43. Under **Users or groups to supervise**, search for and click **Isaiah Langer**.
44. Click **Create policy**.
45. Once the policy is created, click **Close**.
46. In the policy list, next to **Offensive or threatening language, click** the vertical **ellipsis**.
47. Click **Edit**.

    NOTE: Wait 15min to an hour after policy creation for **Edit** to be available.

48. In **Name and describe your policy**, click **Next**.
49. In **Choose supervised users and reviewers** under **Supervised users and groups**, click **All users**.
50. In **Choose locations to monitor communications**, click **Next.**
51. In **Choose conditions and review percentage**, click **Next**.
52. In **Review and finish**, click **Save**.

    NOTE: It might take up to 1 hour to activate your policy and up to 24 hours to start capturing communications.

53. Once the policy is updated, click **Done**.
54. Click **+Create policy**.
55. Click **Monitor for regulatory compliance**.
56. Under **Users or groups to supervise**, search for and click **Isaiah Langer**.
57. Under **Dictionary/lexicon**, click **Select a dictionary/lexicon**.
58. In the list check the following:
    a. **Credit Card Number**
    b. **U.S./U.K. Passport Number**
    c. **U.S. Bank Account Number**

    d. **U.S. Driver's License Number**
    e. **U.S. Individual Taxpayer Identification Number (ITIN)**
    f. **U.S. Social Security Number (SSN)**

59. Click **Create policy**.

    NOTE: It might take up to 1 hour to activate your policy.

60. Once the policy is created, click **Close**.
61. In the policy list, next to **Regulatory compliance**, click the vertical **ellipsis**.
62. Click **Edit**.

    NOTE: It might take up to 1 hour to activate your policy and up to 24 hours to start capturing communications.

63. In **Name and describe your policy**, click **Next**.
64. In **Choose supervised users and reviewers** under **Supervised users and groups**, click **All users**.
65. In **Choose locations to monitor communications**, click **Next.**
66. In **Choose conditions and review percentage**, under **Communication direction,** click the check box for **Internal.**

    NOTE: This should result in all 3 options being checked.

67. Under **Review percentage**, drag the slider to **100%** (may need to scroll to see this).
68. Click **Next**.
69. In **Review and finish**, click **Save**.

    NOTE: It might take up to 1 hour to activate your policy and up to 24 hours to start capturing communications.

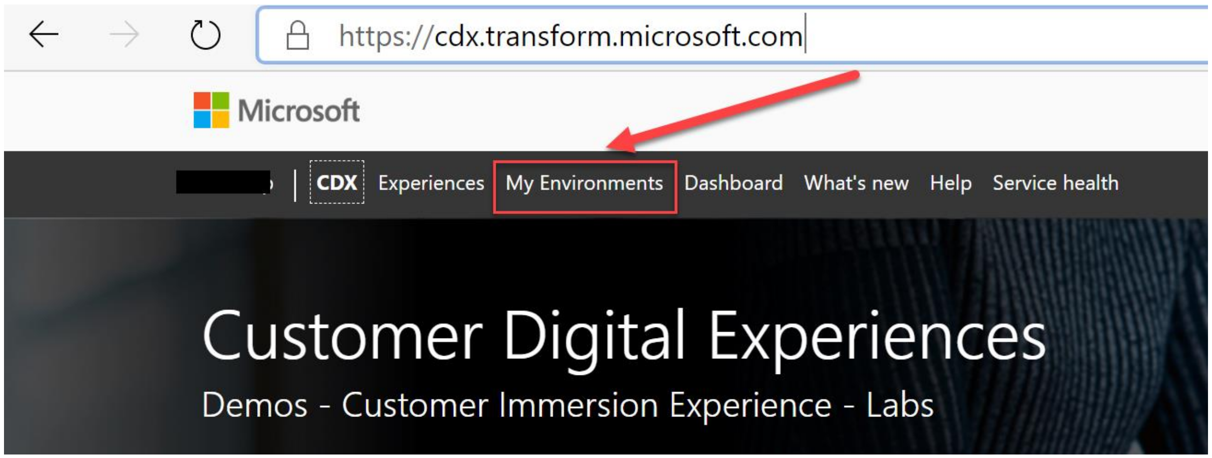
70. Once the policy is updated, click **Done**.
71. Wait 24 hours after creating these policies before moving to the next section to allow them to fully enable in your tenant.

Add the Communication Compliance content pack add-on to your tenant

Complete the following steps to add the **Communication Compliance** content pack to your tenant.

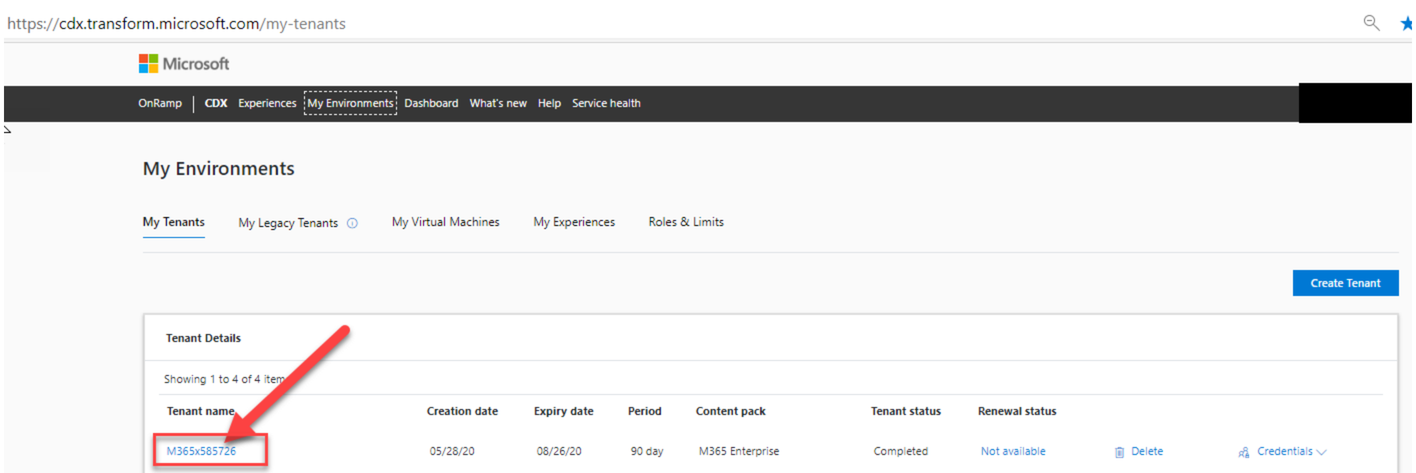
NOTE This content pack will enable audit logging and send the required Microsoft Teams messages and emails to trigger policy matches and alerts in your tenant.

1. Logon to https://cdx.transform.microsoft.com/ You should use your partner email address and password that you use to connect to https://partner.microsoft.com
2. At the top of the page select My Environments Tab as shown below



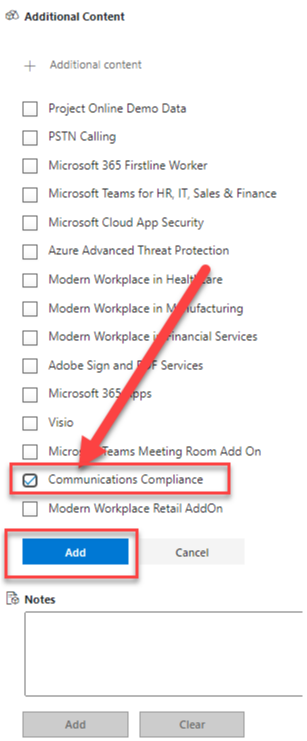
72.

73. In the **Tenant Details** card, under **Tenant name**, click on the name of your tenant.



74. Under **Additional Content,** click on **+ Additional content** to expand the add-on options.

75. Click the check box for the **Communication Compliance** add-on.



76. Click the **Add** button.

77. You will receive an email notification once the add-on has completed. This may take up to 12 hours to complete.

Create Notification Templates

78. In a browser, navigate to https://compliance.microsoft.com and login with the admin@<Tenant>.onmicrosoft.com credentials.

79. In the left-hand navigation click **Show all**.

80. Click **Communication compliance**.

81. Click **Close** on any **Welcome** popups.

82. At the top, click **Notice templates**.
83. Click **+Create notice template**.
84. Under **Template name**, enter **First notification**.
85. Under **Send from**, search for and click **MOD Administrator**.
86. Under **Subject**, enter **IMPORTANT - Notice of Code of Conduct Violation**.
87. Under **Message body**, enter

    Hello,

    Your communications have been flagged as breaching Contoso's Code of Conduct.

    As this is a first notification, no disciplinary action will be taken aside from this notification being added to your record.

    Thank you,

    Contoso Human Resources
88. Click **Create**.
89. Click **Close**.
90. Click **+Create notice template**.
91. Under **Template name**, enter **Final notification**.
92. Under **Send from**, search for and click **MOD Administrator**.
93. Under **Subject**, enter **IMPORTANT – Final Code of Conduct Violation Notification**
94. Under **Message body**, enter

    Hello,

Your communications have been found to violate Contoso's Code of Conduct.

This is your second notification. Your manager maybe notified and any further violations of the code of conduct will result in disciplinary action.

Thank you,

Contoso Human Resources

95. Click **Create**.
96. Click **Close**.
97. Close the browser.

Introduction

What to say	What to show
Insider risk mitigation requires monitoring communications for code of conduct violations. Previously, this monitoring was a largely manual process relying on admins or reviewers to parse through various communications by hand. Microsoft 365 Communication Compliance is an AI and Machine Learning driven service that can detect code of conduct violations such as offensive or threatening language and regulatory non-compliant communications, through a more automated process.	No click steps.

Monitoring for Offensive or Threatening Language

What to say	What to show
Here in the Microsoft Office 365 Communication Compliance portal, the Contoso administrator can see all types of communications that have been flagged as code of conduct violations, including **Offensive Language** and **Regulatory Compliance** violations. These communications are monitored across all Microsoft communication channels like Teams, Exchange, and Yammer, as well as in third party applications.	1. In the browser session signed in as tenant admin admin@<Tenant>.onmicrosoft.com, See (User accounts if you don't know which account to use) click **Policies.** 2. Click on the words **Offensive or threatening language**. 3. At the top, click **Pending**. 4. Scroll through the listed alerts.
The communications are placed together in threads so that the reviewer can see the entire conversation instead of having to hunt through to find the chain.	5. Point out the communication types in the column ( ) to the left of **Subject** header.
Here we see that a user started by harassing another user and ends the conversation with a threat. The conversation is monitored from the beginning and the context of the conversation is flagged by the AI and Machine learning driving the **Communication compliance** service.	6. Click the top **Things I need to say**. 7. In the alert details, point out the thread of communications between the users.
Typically, employees are given notifications that their actions are breaking the code of conduct. In the alert, the admin has access to view the offending user's history for previous violations. Here the admin sees that this user has not been notified of an offense before and can send a notification to him that their actions are breaking the code of conduct. The admin can use the pre-created templates instead of having to craft a new notification.	8. Click **User history**.
These templates are preconfigured in the Communication Compliance service but can also be created by admins. Templates give admins the option to send the notification from	9. To the left, above the list of policy matches, click **Notify**. 10. Click **Choose a notice template**.

What to say	What to show
a particular mailbox. This allows different notification messages to be sent automatically by different departments and managers. The message **Subject** and **Body** can also be prepopulated to ensure consistent notification wording.	11. Click **+ Create a new notification**. 12. Point out **Send from**, **Subject**, and **Message body**. 13. Click **Cancel**.
Like the notifications, the policy used to monitor communications for these violations are easy to create. There are pre-configured templates for **Offensive or Threatening Language**, **Regulatory Compliance**, and **Sensitive Information Monitoring**. The policies can also be customized to target everyone, or specific users or groups. Allowing for policies to be customized to different roles, a CEO might be held to a more stringent regulatory rule than a shipping clerk. Reviewers can be set per policy, so that a single reviewer isn't responsible for all alerts. This also allows for having reviewers more familiar with the group the policy is targeted to. Policies can also be scoped to different Microsoft 365 locations, including Exchange, Teams, and Skype for Business. Communications can be monitored based on the direction. For example, a policy can be created to only monitor for sensitive information sent to those the policy is not target to. That way if the finance department is sending each other account information as part of their work, their communications are not being flagged as violations. However, if they send account information to someone in IT, the communication will be flagged. Conditions allow policies to monitor for specific criteria in communications. These conditions can be specific words,	14. At the top click **Policies**. 15. Click **+ Create policy**. 16. Click **Custom policy**. 17. In the **Name and describe your policy** pane, under **Name**, enter **Language policy**. 18. Click **Next**. 19. Under **Supervised users and groups**, point out **All users** and **Select users**. 20. Click **All users**. 21. Point out **Excluded users and groups** and **Reviewers.** 22. Under **Reviewers**, search for and click **MOD Administrator**. 23. Click **Next**. 24. Under **Choose locations to monitor communications**, point out **Exchange**, **Teams**, and **Skype for Business**. 25. Click **Next**. 26. Under **Communication direction,** point out **Inbound, Outbound,** and **Internal**.

What to say	What to show
recipient domains, attachment size, file types, classification labels, etc. This allows admins to fine tune what communications cause an alert. The **Classifiers** are the communication classifications that the AI and Machine learning Communication Compliance have been trained on and are consistently learning to identify. These classifiers include **Offensive Language**, **Targeted Harassment**, **Profanity**, **Threat**, and even **Source Code**. These types of communications are hard to identify by keyword monitoring, but due to the power of Machine Learning and AI, the Communication Compliance service can detect and identify them. Review percentage allows admins to adjust how much content is reviewed. For the Offensive or Threatening Language policy Contoso reviews 100% of communications. This is due to their no tolerance policy for harassment. Whereas for Regulatory Compliance, Contoso has the policy set to review 10% of communications, as that is what is required by their regulating body and what auditors want to see. Admins can select these amounts or an amount from 1%-100%.	27. Under **Conditions**, click **+ Add condition**. 28. Point out the long list of conditions. 29. Click **Content matches any of these classifiers**. 30. Under **Content matches any of these classifiers**, click **Add**. 31. Click **Classifiers**. 32. Point out **Offensive Language**, **Targeted Harassment**, **Profanity**, **Threat**, and **Source Code**. 33. Click **Cancel**. 34. Under **Review percentage**, point out the percentage slider. 35. Click **Cancel**.

Monitoring for Regulatory Compliance

What to say	What to show
Monitoring for offensive or threatening language is one thing, but users might also discuss confidential data in inappropriate ways. Fortunately, checking for regulatory violations can be done from the same Microsoft 365 Communication Compliance portal.	1. In the left-hand navigation, click **Communication compliance**. If it is not shown, click **Show all**, then click **Communication compliance**. 2. At the top, click **Overview**.

What to say	What to show
The dashboard shows an overview of all alerts that have flagged on any policy that has been created by Contoso. The admin can go directly to the alert or they can see which policies have had the most recent alerts.	3. Point out **Alerts**, **Recent policy matches, Resolved items by policy,** and **Policies with most matches**.
Again, the alerts for Regulatory Compliance are collected from monitoring across all of Microsoft communication channels, like Teams, as well as third party applications. Here some communications in Teams and Outlook have been flagged for review.	4. Under **Policies with most matches,** next to **Regulatory compliance**, click the number in the **Total matches** column. 5. Point out the types of communications as seen in the column ( ) to the left of the **Subject** header (scroll down as needed).
This policy match is for a user and who appears to be sending an email with some confidential information outside of his team. The admin can see what was said and check if the user has been notified for a violation before.	6. Click the top policy match in the list. 7. Under the policy match details, point out the communications there. 8. Click **User history**.
Since the thread indicates that he may have already sent sensitive information, the admin will escalate this for review.	9. To the left, above the list of policy matches, click **Escalate**. 10. Under **Reason for escalation**, enter **Please review for possible regulatory violation.**
Escalations can be set to go to managers, department heads, or anyone who is designated as an escalation reviewer for the type of alert. In this case the escalation point is the Administrator.	11. Click **MOD Administrator**. 12. Click **Escalate**.
The Administrator receives the review escalation in his email. The email gives a quick summary of what has happened and links directly to the alert that the Administrator needs to review. This keeps Lee from having to sort through all the other alerts that may not require his attention. He is able to see the	13. In a new browser tab, navigate to https://outlook.office.com and sign in as admin@<Tenant>.onmicrosoft.com. 14. Click the email titled **Request to review items matching a communication compli…**.

What to say	What to show
activity that caused the alert, any associated activity, and the triggering text is highlighted in the text view. The Administrator now has the information he needs in order to take action.	15. In the email, click **Microsoft 365 compliance center**. 16. Point out the alerts viewable. 17. In the alert details, click **Text view**. 18. Point out the highlighted text.

Conclusion

What to say	What to show
Contoso's admin was alerted to code of conduct violations by an employee who was harassing and threatening a coworker. These types of violations would usually have to be reported by the victim and then investigations launched. However, with Microsoft 365 Communication Compliance the admin was automatically alerted that the communications happened. This allowed the admin to quickly respond and in this case the admin was also able to see regulatory non-compliant activities and alert the employee's manager right away. This automated and proactive approach has helped Contoso stop and quickly respond to insider risk activities.	No click steps.