

Task 1: Setting Up and Configuring User Accounts

Open 365 admin center and select add multiple users from the active users

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar has a 'Copilot' icon, followed by 'Users' with 'Active users' selected, 'Groups', 'Marketplace', and 'Billing'. The main area title is 'Active users'. Below it are buttons for 'Add a user', 'User templates', 'Add multiple users', 'Multi-factor authentication', and a search bar. A table lists several users: 'help 1' (Microsoft 365 E5), 'Loic Curtis' (Microsoft Power Automate Free, Microsoft 3 Teams), 'Loic Curtis1' (Microsoft 365 E5), 'Loic Shared box' (Unlicensed), and 'newuser' (Microsoft 365 E5). A context menu is open over the last row, with options 'Help & support' and 'Give Feedback' highlighted.

Click upload csv

The screenshot shows the 'Add multiple users' wizard. The left sidebar is identical to the previous screenshot. The main area title is 'Active users > Add multiple users'. It shows a flow: 'Basics' (selected), 'Licenses', and 'Finish'. A checkbox 'I'd like to upload a CSV with user information' is checked. Below it is a note: 'Download one of the files below. Open the file in Excel or a similar app, add user info, save, and upload.' There are links to 'Download a blank CSV file with the required headers' and 'Download a CSV file that includes example user info'. A 'Browse' button is available to upload a CSV file. At the bottom are 'Next' and 'Cancel' buttons. A context menu is open over the 'Help & support' button.

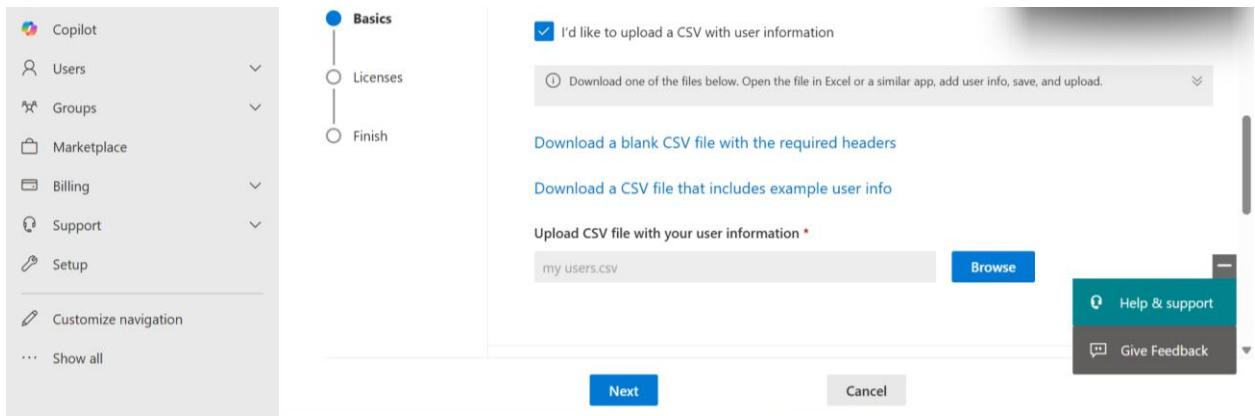
Here is my csv file for my users created with notepad

my users.csv

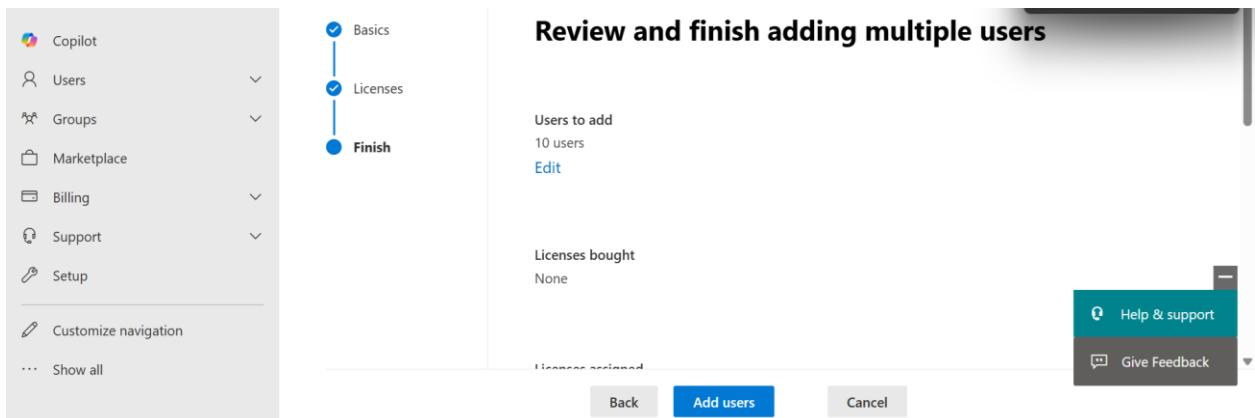
File Edit View

Username	First name	Last name	Display name	Job title	Department	Office number	Office phone	Mobile phone	Fax	Alternate email address	Address	City	State or province	ZIP or postal code	Country or region
usersmith@loicsolutions.onmicrosoft.com	User	Smith	User Smith	HR Manager	HR	101	123-456-7890	123-456-7891		usersmith.alt@loicsolutions.com	123 Main Street, Toronto, ON, M5J 2N8, Canada				
userjohnson@loicsolutions.onmicrosoft.com	User	Johnson	User Johnson	HR Assistant	HR	102	123-456-7892	123-456-7893		userjohnson.alt@loicsolutions.com	123 Main Street, Toronto, ON, M5J 2N8, Canada				
userwilliams@loicsolutions.onmicrosoft.com	User	Williams	User Williams	HR Coordinator	HR	103	123-456-7894	123-456-7895		userwilliams.alt@loicsolutions.com	123 Main Street, Toronto, ON, M5J 2N8, Canada				
userjones@loicsolutions.onmicrosoft.com	User	Jones	User Jones	IT Support Specialist	IT	201	123-456-7896	123-456-7897		userjones.alt@loicsolutions.com	456 Elm Street, Toronto, ON, M5J 3B2, Canada				
userbrown@loicsolutions.onmicrosoft.com	User	Brown	User Brown	System Administrator	IT	202	123-456-7898	123-456-7899		userbrown.alt@loicsolutions.com	456 Elm Street, Toronto, ON, M5J 3B2, Canada				
userdavis@loicsolutions.onmicrosoft.com	User	Davis	User Davis	Network Engineer	IT	203	123-456-7800	123-456-7801		userdavis.alt@loicsolutions.com	456 Elm Street, Toronto, ON, M5J 3B2, Canada				
usermiller@loicsolutions.onmicrosoft.com	User	Miller	User Miller	Marketing Manager	Marketing	301	123-456-7802	123-456-7803		usermiller.alt@loicsolutions.com	789 Pine Avenue, Toronto, ON, M5J 4C3, Canada				
userwilson@loicsolutions.onmicrosoft.com	User	Wilson	User Wilson	Marketing Coordinator	Marketing	302	123-456-7804	123-456-7805		userwilson.alt@loicsolutions.com	789 Pine Avenue, Toronto, ON, M5J 4C3, Canada				
usermoore@loicsolutions.onmicrosoft.com	User	Moore	User Moore	Digital Strategist	Marketing	303	123-456-7806	123-456-7807		usermoore.alt@loicsolutions.com	789 Pine Avenue, Toronto, ON, M5J 4C3, Canada				
usertaylor@loicsolutions.onmicrosoft.com	User	Taylor	User Taylor	Content Creator	Marketing	304	123-456-7808	123-456-7809		usertaylor.alt@loicsolutions.com	789 Pine Avenue, Toronto, ON, M5J 4C3, Canada				

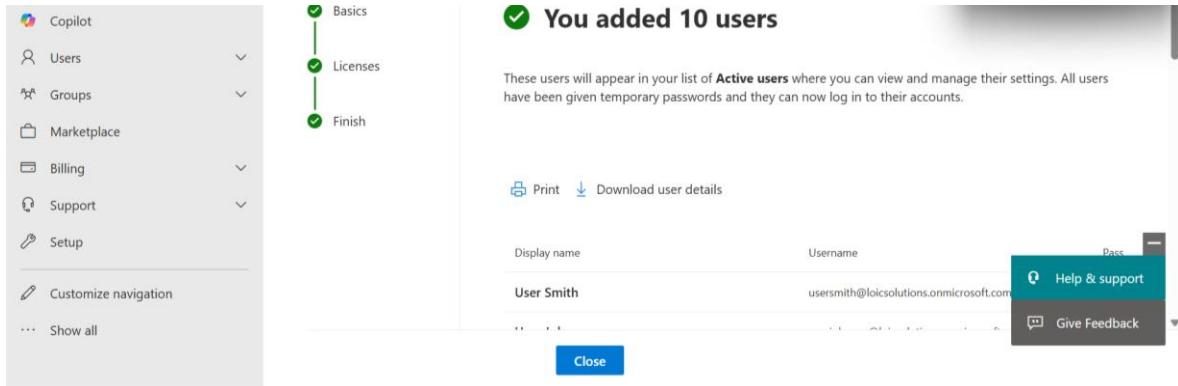
After uploading csv file, click next



Click add users



10 new users successfully added



Task 2: Monitoring and Reporting

1. Configure Audit Logs:

Under purview admin center, select audit

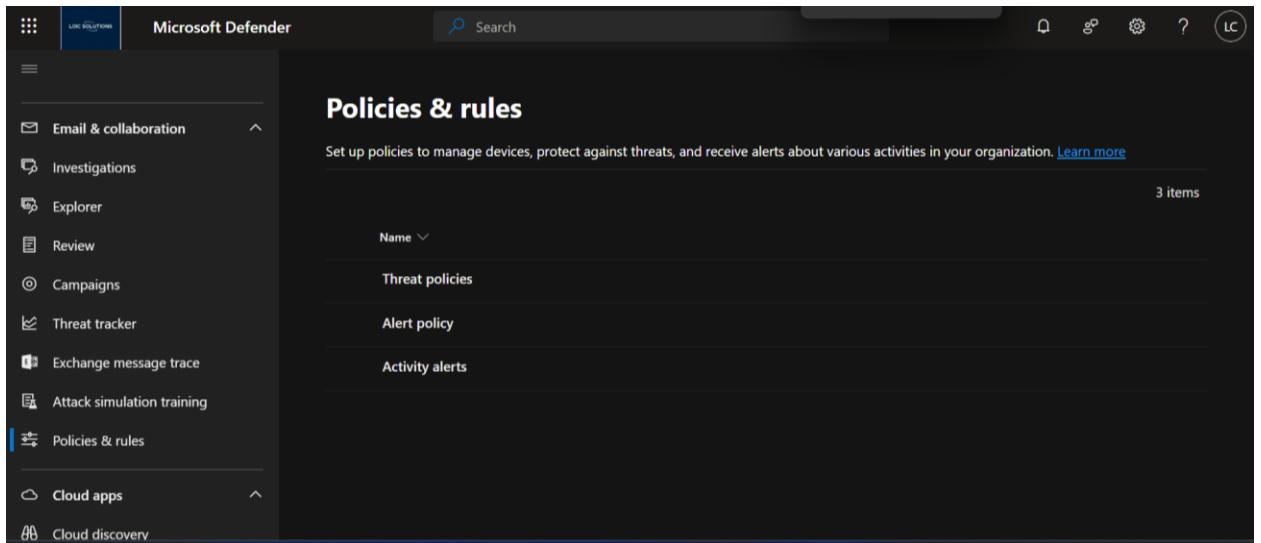
The screenshot shows the Microsoft Purview Admin Center Audit search interface. The left sidebar includes Home, Audit (selected), Search, Policies, Solutions, and other related solutions like eDiscovery and Compliance Manager. The main area is titled "Search" and contains fields for "Searches completed" (16), "Active searches" (0), and "Active unfiltered searches" (0). It has sections for "Date and time range (UTC)" (Start: Apr 00:00, End: Apr 00:00), "Activities - friendly names" (Choose which activities to search...), "Users" (Add the users whose audit logs you ...), "Activities - operation names" (Enter operation values, separated by...), "File, folder, or site" (Enter all or a part of the name of a fi...), "Keyword Search" (Enter the keyword to search for), "Record Types" (Select the record types to search ...), "Workloads" (Enter the workloads to search for), "Admin Units" (Choose which Admin Units to s...), and "Search name" (Give the search a name). There are "Search" and "Clear all" buttons at the bottom.

If you get any results you can view them to check

The screenshot shows the Microsoft Purview Admin Center Audit search results interface. The left sidebar is identical to the previous screenshot. The main area displays search results with 18 items. The columns include "Search name" (e.g., "Apr 17 - Apr 18 sharingset"), "Job status" (Completed), "Prog..." (100%), "Sear..." (3m, 25s), "Total results" (0), "Creation ti..." (Apr 18, 2025 2:31...), and "Search performed by" (loiccurtis@loicsolutions.onmicrosoft.com). There are buttons for "Copy this search", "Delete", and "Refresh".

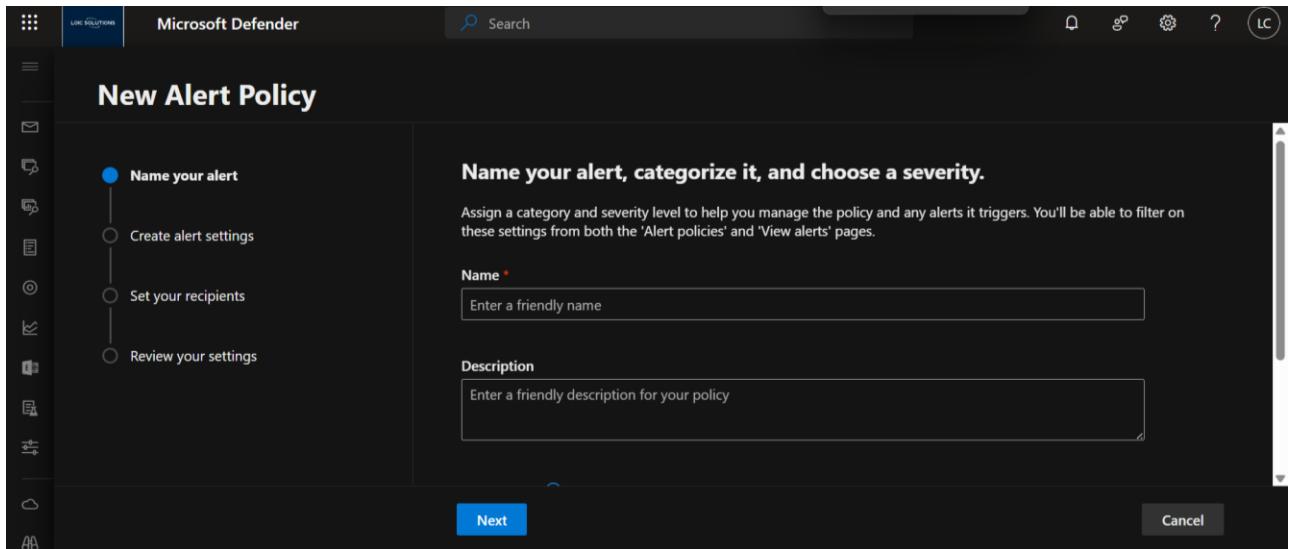
2. Set Up Alerts:

Open defender and select policy and rules under email and collaboration



The screenshot shows the Microsoft Defender interface with the 'Policies & rules' section selected. The left sidebar includes options like Email & collaboration, Investigations, Explorer, Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, and Policies & rules. The main area displays sections for Threat policies, Alert policy, and Activity alerts, with a note indicating 3 items.

Select alerts and create new alert policy



The screenshot shows the 'New Alert Policy' setup screen. On the left, a vertical navigation bar lists icons for Email, Investigations, Explorer, Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, Policies & rules, Cloud apps, and Cloud discovery. The main panel has a title 'New Alert Policy' and a sub-section 'Name your alert'. It includes a numbered list: 'Name your alert' (selected), 'Create alert settings', 'Set your recipients', and 'Review your settings'. To the right, there's a descriptive text about naming and severity, a 'Name' input field with placeholder 'Enter a friendly name', a 'Description' input field with placeholder 'Enter a friendly description for your policy', and 'Next' and 'Cancel' buttons at the bottom.

Alert name

The screenshot shows the 'New Alert Policy' wizard in Microsoft Defender. The left sidebar has icons for Mail, File, Database, and Cloud. The top navigation bar includes 'Microsoft Defender', 'Search', and various status indicators. The main area title is 'New Alert Policy'. A vertical progress bar on the left lists four steps: 'Name your alert' (selected), 'Create alert settings', 'Set your recipients', and 'Review your settings'. To the right, a section titled 'Name your alert, categorize it, and choose a severity.' contains fields for 'Name' (set to 'Deleted files') and 'Description' (set to 'alert for deleted files'). Buttons at the bottom are 'Next' (highlighted in blue) and 'Cancel'.

Select the alert activity

The screenshot shows the 'New Alert Policy' wizard in Microsoft Defender, continuing from the previous step. The left sidebar and top navigation bar are identical. The main area title is 'New Alert Policy'. The vertical progress bar now shows 'Name your alert' (with a checkmark) and 'Create alert settings' (selected). A section titled 'Choose an activity, conditions and when to trigger the alert' displays a configuration panel. It shows 'Activity is' set to 'Deleted file' (with a note: 'User deletes a document from a site.') and 'AND' (with a dropdown menu). Buttons at the bottom are 'Back', 'Next' (highlighted in blue), and 'Cancel'.

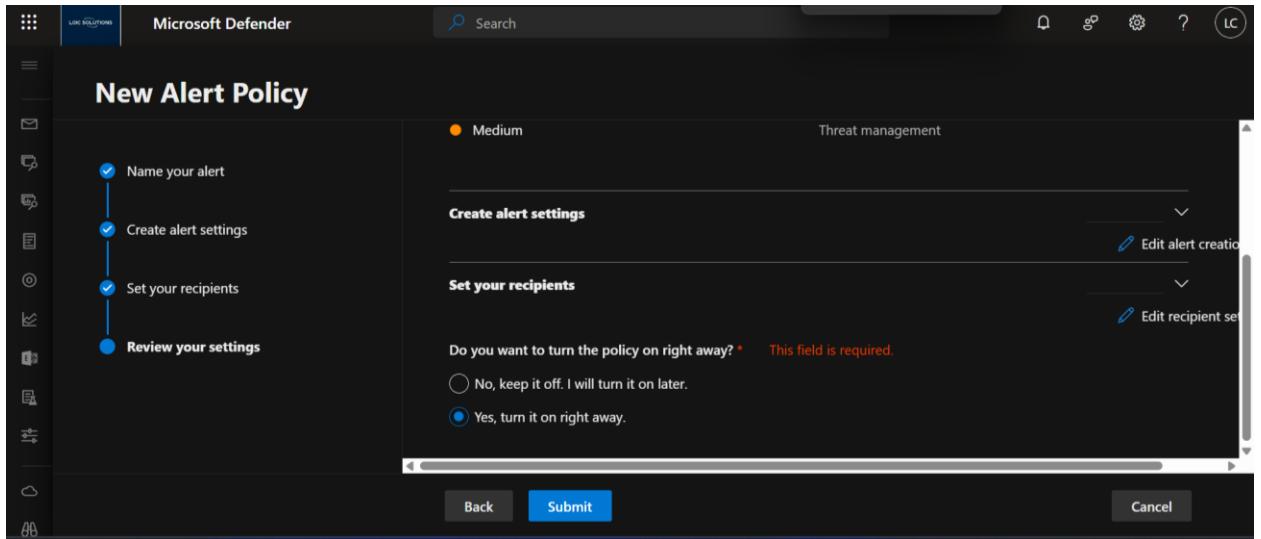
Select how you want the alert to be triggered

The screenshot shows the Microsoft Defender interface for creating a new alert policy. The title is "New Alert Policy". On the left, a vertical navigation menu lists: Name your alert, Create alert settings (which is selected), Set your recipients, and Review your settings. The main panel has a heading "How do you want the alert to be triggered?". It contains two radio button options: "Every time an activity matches the rule" (selected) and "When the volume of matched activities reaches a threshold". Below these are input fields: "More than or equal to" with value "10" and "activities", "During the last" with value "60" and "minutes", and a dropdown "On" set to "All users". At the bottom are "Back", "Next", and "Cancel" buttons.

Select at least 2 global administrators to receive the alerts

The screenshot shows the Microsoft Defender interface for creating a new alert policy. The title is "New Alert Policy". The left sidebar shows the steps: Name your alert, Create alert settings (selected), Set your recipients, and Review your settings. The main panel has a heading "Decide if you want to notify people when this alert is triggered". It includes a checked checkbox for "Opt-in for email notifications" and a section for "Email recipients *". The recipient list shows "Loic Curtis" and "Loic Curtis1" with a "Select users" button. Below is a "Daily notification limit" dropdown set to "No limit". At the bottom are "Back", "Next", and "Cancel" buttons.

Select turn policy right away and select submit



Alert has been created

The screenshot shows the 'Alert policy' list in Microsoft Defender. The left sidebar includes links to Home, Incidents & alerts, Hunting, Actions & submissions, Threat intelligence, Learning hub, Trials, Partner catalog, Exposure management, Overview, and Attack surface. The main area is titled 'Alert policy' and displays a table of existing alert policies:

Name	Severity	Type	Category	Date modified (UTC -04:00)
Deleted files	Medium	Custom	Threat management	Apr 18, 2025 3:05 PM
CC Inappropriate Text	Medium	Custom	Supervision	Apr 18, 2025 2:18 PM
Forwarding inbox rules	Medium	Custom	Threat management	Apr 10, 2025 9:17 PM
MIP AutoLabel simulation completed	Low	System	Threat management	Mar 9, 2021 12:02 PM

At the top of the main area, there are buttons for 'New Alert Policy', 'Manage Activity Alerts', 'Refresh', and a search bar. A blue banner at the top states: 'Mail flow alerts have moved to the new Exchange admin center. Starting Oct 2021, customers will only be able to create/view/edit mail flow alerts in the new Exchange admin center.' with a 'Try it now' button.

Under purview, select insider risk management

The screenshot shows the Microsoft Purview Insider Risk Management interface. On the left, a sidebar lists various solutions: Home, Solutions (Data Catalog, Data Lifecycle Management, Data Loss Prevention, Data Security Posture Management (preview), DSPM for AI, eDiscovery, Information Barriers, Information Protection, Insider Risk Management, Records Management), and ... (Information Barriers). The 'Insider Risk Management' option is selected. The main pane displays 'Policy recommendations' with 0 items. A message at the top states: 'You currently aren't assigned to a role group that allows you to view alerts. Consider assigning somebody to this role. Learn which role groups are needed to review alerts.' Below this, there's a section about turning on analytics with a 'Turn on analytics' button. The bottom of the pane includes filters for 'Policy', 'Status', 'Users in scope', 'Active alerts', 'Confirmed alerts', and 'Actions'.

Select custom new policy

The screenshot shows the Microsoft Purview Insider Risk Management interface. The sidebar is identical to the previous screenshot. The main pane is titled 'Policies' and displays 'Policy warnings' with 0 items. It also shows 'Policy recommendations' with 0 items and 'Healthy policies' with 0 items. A message at the top is identical to the previous screenshot. Below these sections, there's a note about turning on analytics with a 'Turn on analytics' button. At the bottom, there's a 'Create policy' dropdown menu with options: 'Quick policy' and 'Custom policy'. The bottom of the pane includes filters for 'Status', 'Users in scope', 'Active alerts', 'Confirmed alerts', and 'Actions'.

Review the template and select next

The screenshot shows the 'New insider risk policy' wizard in Microsoft Purview. On the left, a vertical navigation pane lists steps: 'Policy template' (selected), 'Name and description', 'Users and groups', 'Content to prioritize', 'Triggering event', and 'Indicators'. The main panel is titled 'Data theft' and contains sections for 'Data theft by departing users', 'Data leaks', 'Risky AI usage (preview)', and 'Security policy violations (preview)'. A right sidebar for 'Data theft by departing users' includes a note about detecting data theft by departing users near their resignation or termination date, prerequisites for an HR data connector (optional, recommended), and options for devices onboarded and physical badging connector.

Name the policy

The screenshot shows the 'Name your policy' step of the wizard. The left navigation pane now shows 'Name and description' as the selected step. The main panel has a title 'Name your policy' and fields for 'Name *' (containing 'DLP alert') and 'Description' (containing 'An alert for DLP'). Navigation buttons include 'Back', 'Next', and 'Cancel'.

Select all users and groups

Microsoft Purview

Insider risk management > New insider risk policy

Policy template
Name and description
Users and groups
Content to prioritize
Triggering event
Indicators

Choose users, groups, & adaptive scopes

Choose users, groups, and adaptive scopes within your organization who this policy will apply to.

All users, groups, and adaptive scopes
 Specific users, groups, and adaptive scopes

Back Next Cancel

Select the triggering event

purview.microsoft.com/insiderriskmgmt/policiespage?tid=488c6957-abac-4094-831c-4a1034a3546a

Microsoft Purview

Insider risk management > New insider risk policy

Policy template
Name and description
Users and groups
Content to prioritize
Triggering event
Indicators
Finish

Choose triggering event for this policy

Choose one or more triggering events to determine when a policy will begin assigning risk scores to a user's activity.[Learn more](#)

(Recommended) HR data connector events
Configure the HR connector to send employee termination or resignation records.
ⓘ Your organization doesn't have an HR connector. You can create this policy now using the 'User account deleted from Microsoft Entra ID' triggering event and edit the policy later after you have a connector set up. [Learn how to configure an HR connector](#)

User account deleted from Microsoft Entra ID
Policy will start assigning risk scores when a user's account is deleted from Microsoft Entra ID. Good option to choose if an HR connector isn't set up or not actively connected.

Back Next Cancel

Select alerts from selected dlp policies

The screenshot shows the Microsoft Purview Insider risk management interface. The top navigation bar includes 'Microsoft Purview', a search bar, and various icons like Copilot, Copilot AI, and help. The main title is 'Insider risk management > New insider risk policy'. On the left, a vertical navigation pane lists steps: 'Policy template' (checked), 'Name and description' (checked), 'Users and groups' (checked), 'Content to prioritize' (checked), 'Triggering event' (checked), 'Indicators' (selected), and 'Finish'. To the right, under 'Indicators', there is a list of alert types: 'Cloud storage indicators (0/11 selected)', 'Cloud service indicators (0/10 selected)', 'Generative AI apps (preview) (0/6 selected) [New]', 'Microsoft Fabric indicators (0/8 selected)', 'Communication compliance indicators (0/4 selected) [New]', 'Detect messages matching specific trainable classifiers (0/3 selected) [New]', 'Detect messages matching specific sensitive info types (0/1 selected) [New]', 'Data loss prevention (DLP) alert indicators (preview) (0/1 selected) [New]', 'Detect when DLP policies generate alerts (preview) (0/1 selected) [New]', and 'Generating alerts from selected DLP policies [Info]'. Buttons at the bottom include 'Back', 'Next', and 'Cancel'.

Detection options select all

The screenshot shows the Microsoft Purview Insider risk management interface. The top navigation bar includes 'Microsoft Purview', a search bar, and various icons like Copilot, Copilot AI, and help. The main title is 'Insider risk management > New insider risk policy'. On the left, a vertical navigation pane lists steps: 'Users and groups' (checked), 'Content to prioritize' (checked), 'Triggering event' (checked), 'Indicators' (selected), 'Detection options' (selected), and 'Indicator thresholds' (unchecked). Below the navigation pane, the title 'Detection options' is displayed. A descriptive text states: 'These advanced detection options are used to generate alerts for the activity detected.' Under 'Sequence detection', it says: 'A sequence is a group of two or more activities performed one after the other over a period of 7 days that might suggest an elevated risk. Specific indicators are used to detect each step in a sequence, which are organized into four main types of activity: download, exfiltrate, obfuscate, and delete. [Learn more about sequences](#)'. There is a checked checkbox labeled 'Select all' and three unchecked checkboxes for sequence detection types: 'Download from Microsoft 365 location then exfiltrate [Info]', 'Download from Microsoft 365 location, obfuscate, then exfiltrate [Info]', and 'Download from Microsoft 365 location, exfiltrate, then delete [Info]'. Buttons at the bottom include 'Back', 'Next', and 'Cancel'.

Choose threshold type for indicators

The screenshot shows a navigation sidebar on the left with the following steps:

- Users and groups
- Content to prioritize
- Triggering event
- Indicators** (selected)
- Detection options
- Indicator thresholds
- Finish

The main content area is titled "Choose threshold type for indicators". It contains the following text:

Each indicator you selected uses thresholds to influence the activity's risk score, which in turn determines whether an alert's severity is low, medium, or high. Each threshold is based on the number of events recorded for an activity per day.

Two radio button options are shown:

- Turn on analytics to get recommended thresholds based on daily scans of user activity in your org. First scan takes 48 hours, so you can edit this policy afterward to quickly update thresholds based on real-time insights. Learn more about analytics X
- Apply thresholds provided by Microsoft Built-in thresholds will be applied to all indicators you selected.
- Choose your own thresholds Customize thresholds that are prepopulated with built-in values from Microsoft.

Buttons at the bottom include Back, Next (highlighted in blue), and Cancel.

Review and submit

The screenshot shows a navigation sidebar on the left with the following steps:

- Policy template
- Name and description
- Users and groups
- Content to prioritize
- Triggering event
- Indicators** (selected)

The main content area is titled "Review settings and finish". It contains the following text:

Review the settings for your insider risk policy. The policy will take effect immediately after you create it, but may take up to 24 hours to start generating alerts. User productivity won't be impacted in any way.

One suggestion is listed:

① 1 suggestion below for improving your policy. X

Policy template: Data theft by departing users [Edit policy type](#)

Policy name and description: DLP alert An alert for DLP [Edit policy name and description](#)

Buttons at the bottom include Back, Submit (highlighted in blue), and Cancel.

Policy has been created

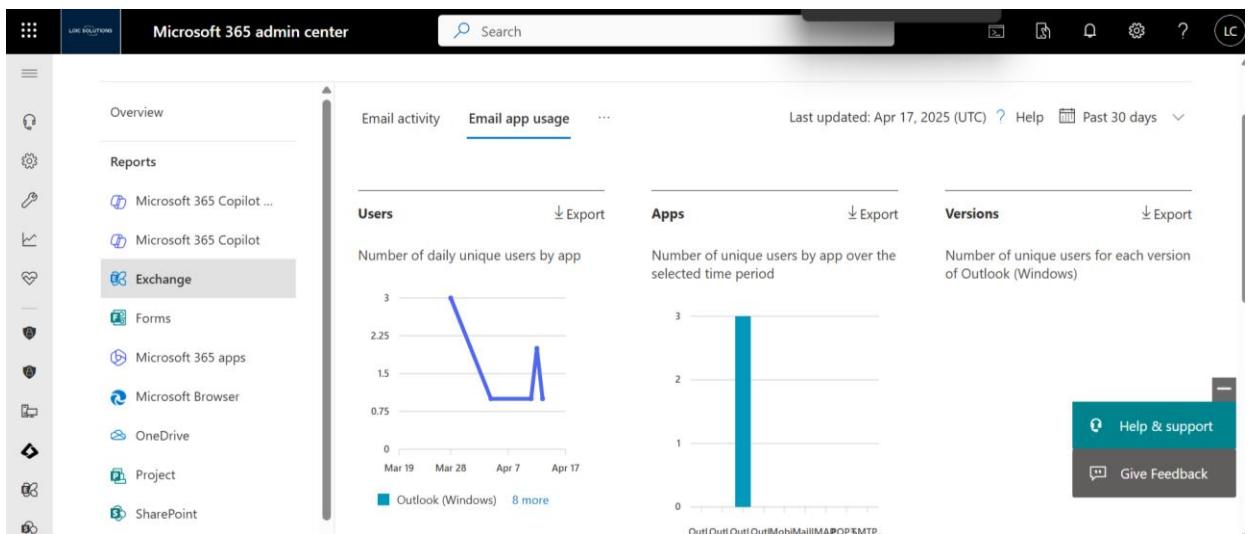
The screenshot shows the Microsoft Purview interface for creating a new insider risk policy. On the left, a vertical checklist indicates the steps completed: Policy template, Name and description, Users and groups, Content to prioritize, Triggering event, Indicators, and Finish. The main area displays a success message: "Your policy was created". It includes a note: "It might take up to 24 hours before policy matches will start showing up on the Alerts tab." Below this, a section titled "What happens next?" provides three bullet points: 1. A clock icon: "It'll take a few minutes to create the policy. You'll see it listed on the Policies tab." 2. A shield icon: "Once the policy is active, it could take at least 24 hours for the triggering event to occur and score user activity, at which point the first alert is generated. If admin notification are turned on, you'll get an email when this alert happens." 3. A hammer icon: "You or someone on your team will triage the alert and confirm it to a case for further investigation or dismiss it as normal behavior." At the bottom right is a blue "Done" button.

3. Generate Usage Reports:

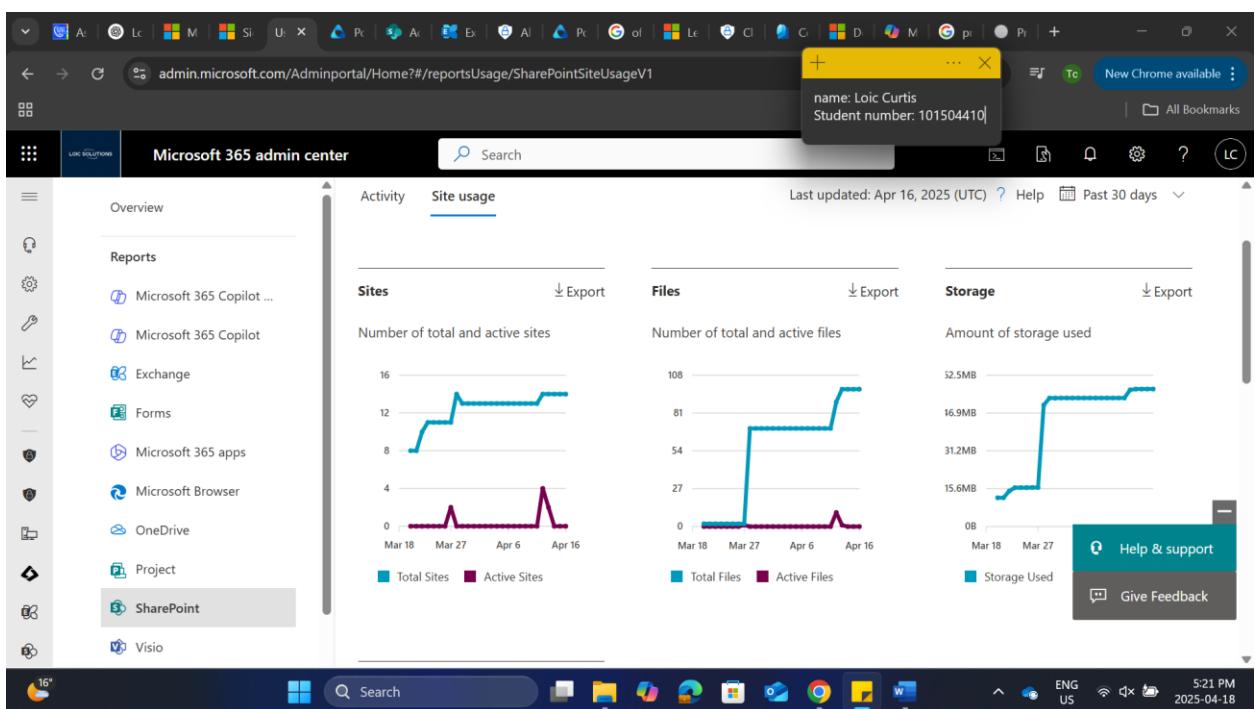
Go to Microsoft 365 admin center, under reports select usage

The screenshot shows the Microsoft 365 admin center interface. The left sidebar menu includes sections like Support, Settings, Setup, Reports (with Adoption Score, Usage, and Organizational messages), Health, Admin centers (Security and Compliance), and Loic solutions. The main content area greets the user with "Good evening, Loic Curtis" and describes the simplified view. It features two cards: "Set up email with a custom domain" (with a sub-note about connecting a domain) and "Help customers schedule appointments with you" (with a sub-note about setting up a calendar). At the bottom right are "Help & support" and "Give Feedback" buttons.

Email usage report



Sharepoint site usage report



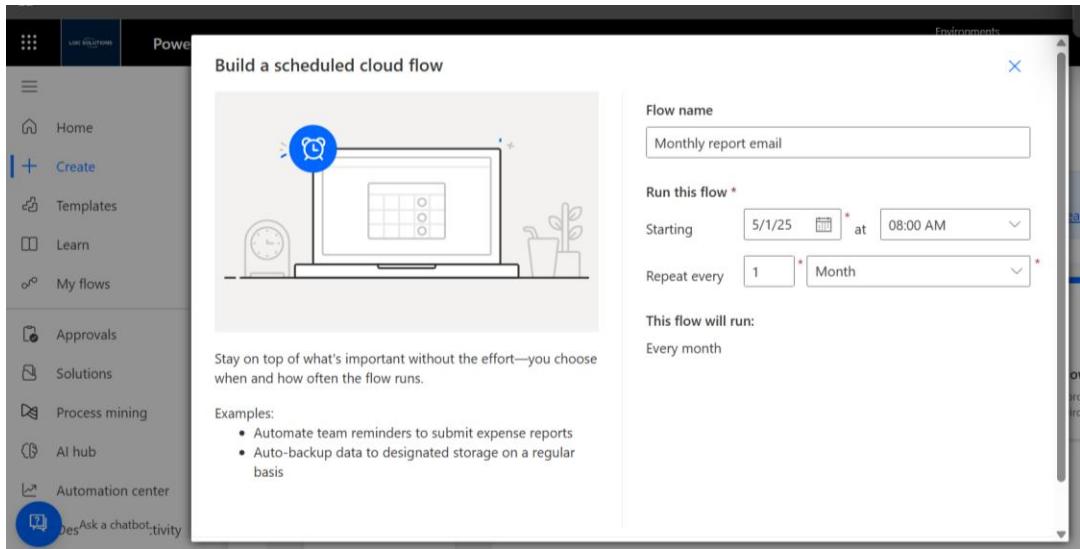
Signing into the power automate platform

The screenshot shows the Power Automate platform interface. At the top, it says "Hello, Loic". Below that is a button labeled "+ Create". On the left sidebar, there are several options: Home, Create, Templates, Learn, My flows, Approvals, Solutions, Process mining, AI hub, Automation center, and Ask a chatbot. Under "Create", there is a sub-option "Des...".

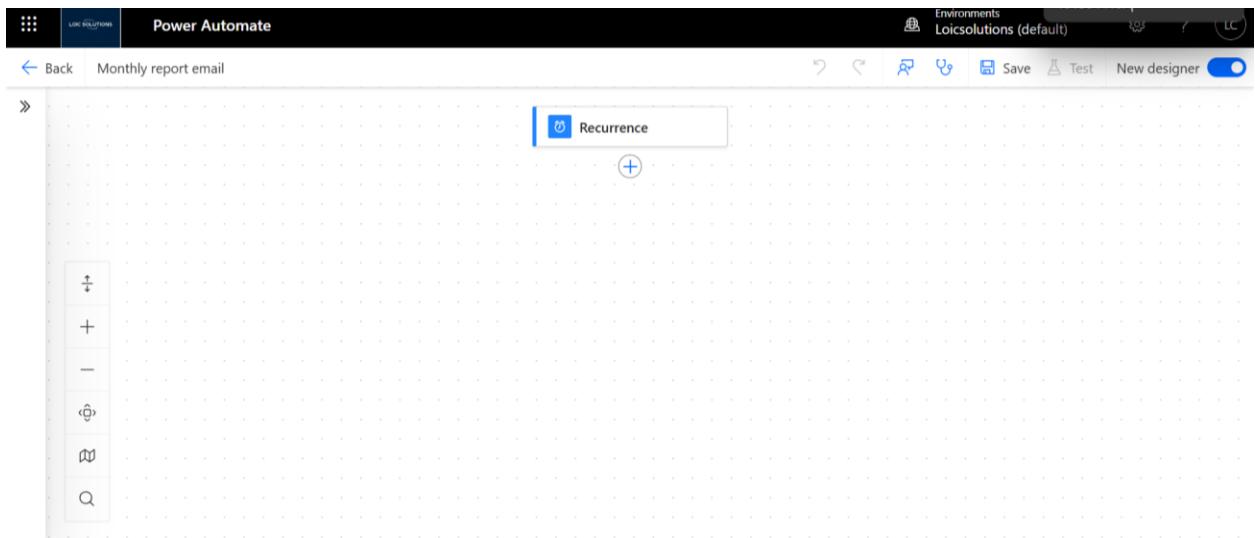
Select create and select schedule cloud flow

The screenshot shows the "Three ways to make a flow" section. It includes a "Start from blank" link and a note about enabling generative AI features. Below are four options: "Automated cloud flow" (Triggered by a designated event), "Instant cloud flow" (Triggered manually as needed), "Scheduled cloud flow" (You choose when and how often it runs), and "Desktop flow" (Automates processes on your desktop environment). The "Create" option is highlighted in the sidebar.

Configure the flow and select create



Select the plus sign below recurrence to add an action



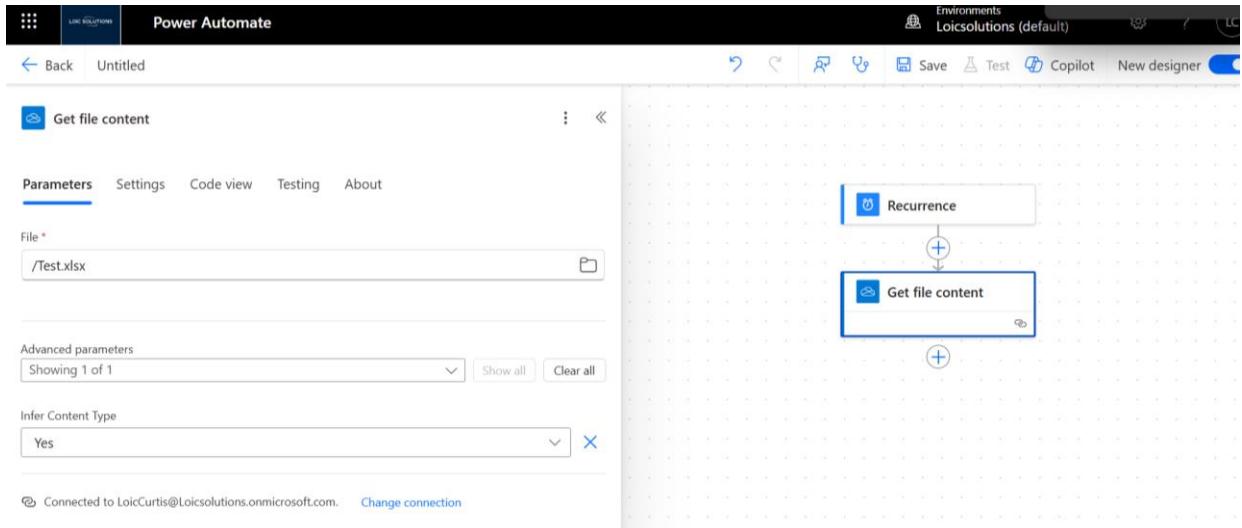
Under action, select get file content and sign into outlook

The screenshot shows the 'Power Automate' interface with the title bar 'Power Automate' and environment 'Loicsolutions (default)'. A search bar at the top contains the text 'get file content'. Below it, a list of actions is displayed under the heading 'OneDrive for Business' and 'SharePoint'. The 'Get file content' action is highlighted with a blue border.

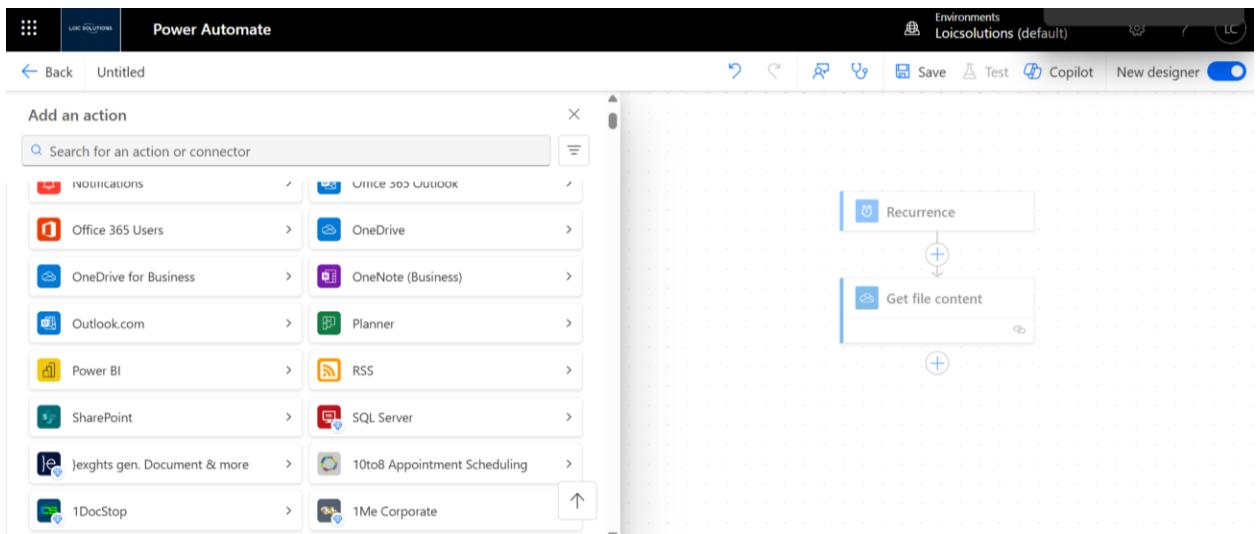
Select the file identifier document for the report

The screenshot shows the configuration screen for the 'Get file content' action. The left pane displays parameters: 'File' set to '/Test.xlsx', 'Infer Content Type' set to 'Yes', and a note about being connected to LoicCurtis@Loicsolutions.onmicrosoft.com. The right pane shows the Power Automate designer canvas with a 'Recurrence' trigger and a 'Get file content' action step.

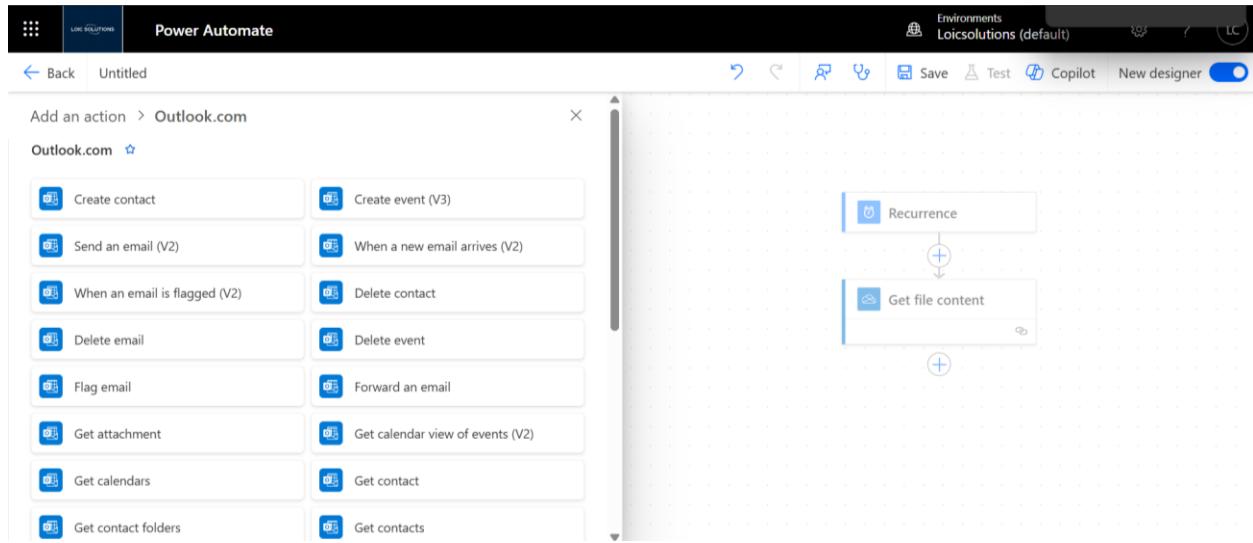
Select the plus sign under get file content



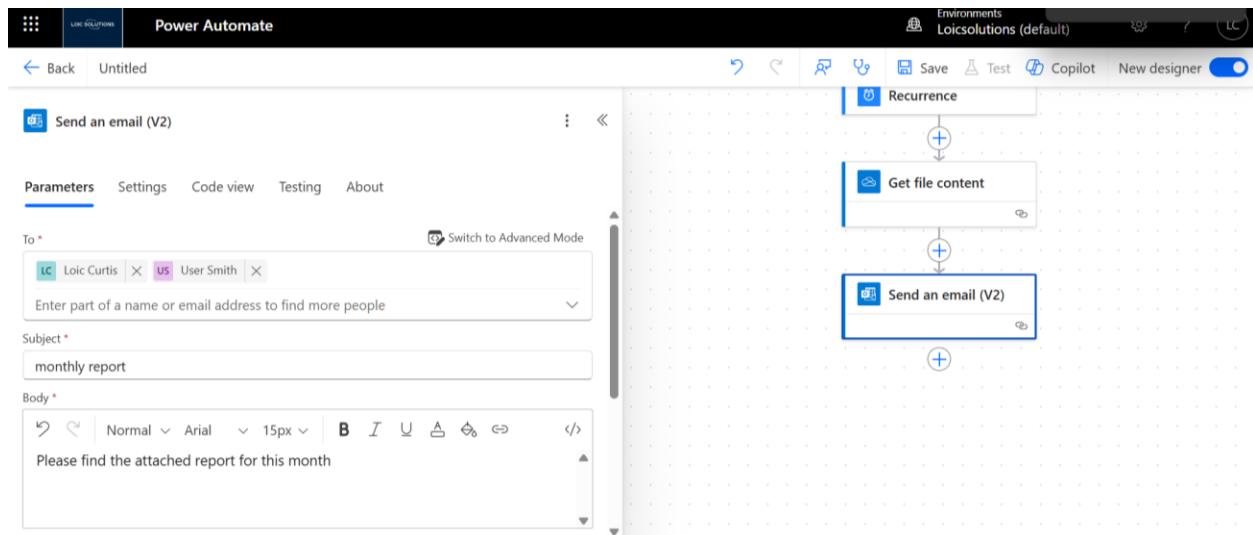
Select outlook



Select send an email v2 and signing into outlook to establish connection



Send to you can put your global admin and an additional manager to view the reports



Scroll down under advance parameters and select attachments

The screenshot shows the Microsoft Power Automate designer interface. On the left, there's a preview pane for a "Send an email (V2)" step, which includes a "Parameters" tab with a "monthly report" value and a "Body" rich text editor containing the text "Please find the attached report for this month". Below this is an "Advanced parameters" section showing "Showing 2 of 7" items. On the right, the main designer canvas displays a workflow starting with a "Recurrence" trigger, followed by a "Get file content" action, and finally a second "Send an email (V2)" action. The bottom of the screen shows the Power Automate ribbon with tabs like Environments, Save, Test, Copilot, and New designer.

Select add new item

This screenshot is similar to the previous one but focuses on the "Attachments" section. In the preview pane for the "Send an email (V2)" step, the "Attachments" section is expanded, showing a button to "+ Add new item". The main designer canvas shows the same workflow as before, but the "Send an email (V2)" step is highlighted with a blue border, indicating it is currently selected or being edited. The Power Automate ribbon at the top remains visible.

Put your attachment name, for content input / to enable dynamic expression and you'll see the option to add file content

The screenshot shows the Power Automate designer interface. On the left, the 'Send an email (V2)' step is selected, with its parameters and attachments visible. The attachments section shows a file named 'Monthly report.xlsx' with a 'File content' link. On the right, a workflow diagram is displayed, consisting of three main steps: 'Recurrence', 'Get file content', and 'Send an email (V2)'. The 'Get file content' step is connected to the 'Send an email (V2)' step.

Select save

The screenshot shows the Power Automate designer interface after saving the workflow. The 'Send an email (V2)' step now has populated fields: 'To' with 'Loic Curtis' and 'User Smith', and 'Subject' with 'monthly report'. The body of the email contains the text 'Please find the attached report for this month'. The workflow diagram on the right remains the same as in the previous screenshot.

Select test flow at the top, manual

The screenshot shows the Power Automate interface with a flow named "Recurrence -> Get file content,Send an email (V2)". The "Testing" tab is selected. A "Test Flow" dialog is open, showing two options: "Manually" (selected) and "Automatically". The flow itself consists of three steps: "Recurrence", "Get file content", and "Send an email (V2)". The "Send an email" step is currently highlighted. The "Parameters" tab is active, displaying recipient details ("To": Loic Curtis, User Smith), subject ("monthly report"), and body text ("Please find the attached report for this month"). A "Code view" tab is also present.

Flow was a success

The screenshot shows the Power Automate interface with the "Run results" tab selected. It displays the flow's execution details: Start time (4/18/2025, 6:44:32 PM), End time (4/18/2025, 6:44:32 PM), and Status (Succeeded). The flow history on the right shows three steps: "Recurrence" (0s), "Get file content" (0.4s), and "Send an email (V2)" (0.4s), each with a green checkmark indicating success. The "Edit" button is located in the top right corner of the main workspace.

4. Implement and Monitor Service Health:

Open 365 admin center and click service health

The screenshot shows the Microsoft 365 admin center interface. On the left, there's a navigation sidebar with sections like Viva, Partner relationships, Microsoft Edge, Setup, Reports, Health, Service health (which is selected and highlighted in blue), Windows release health, Message center, Product feedback, Network connectivity, and Software updates. Below this is an Admin centers section. The main content area is titled "Service health" and shows the "Overview" tab selected. It displays a summary message: "View the issues and health status of all services that are available with your current subscriptions. Learn more about Service Health". Below this are two buttons: "Report an issue" and "Customize". To the right, there's a timestamp "Apr 18, 2025, 8:58 PM EDT". At the bottom, there's a "Change view" button and a "Help & support" link. A small tooltip-like overlay is visible in the bottom right corner with options like "Issue", "Advisory", "Give Feedback", and "Advisory".

Select customize and go the email option

This screenshot is similar to the previous one but shows the "Customize" tab selected in the top navigation bar. The main content area remains the same, showing the "Service health" overview and active issues. A new tab labeled "Email" is visible in the "Customize" section. Below it is a checkbox labeled "Send me email notifications about service health". At the bottom right of the main content area is a "Save" button.

Enable send me email notifications about service health and you can add different email addresses for the notifications

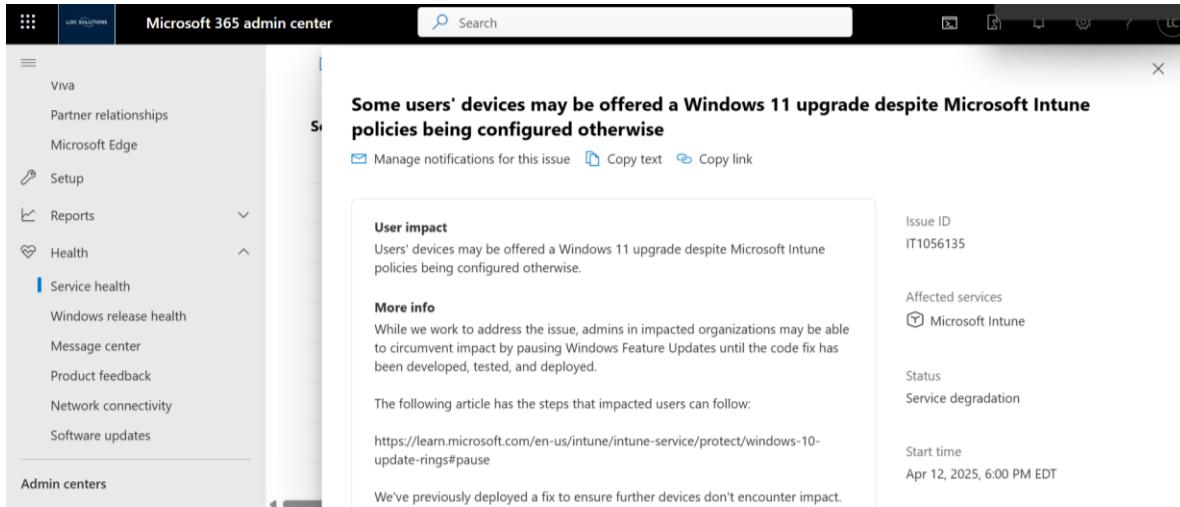
The screenshot shows the Microsoft 365 admin center interface. On the left, there's a navigation sidebar with sections like Viva, Partner relationships, Microsoft Edge, Setup, Reports, Health, and Admin centers. Under Health, the 'Service health' option is selected. The main content area is titled 'Service health' and has tabs for Overview, Issue history, and Reported issues. Below this, there's a section for 'Active issues Microsoft is working on' with some listed items. To the right, a 'Customize' panel is open under the 'Email' tab. It includes a checkbox for 'Send me email notifications about service health' (which is checked), a field for 'Primary email address' (LoicCurtis@Loicsolutions.onmicrosoft.com), and a checkbox for 'Other email addresses'. There's also a section for 'Include these issue types' with checkboxes for Incidents, Advisories, and Issues in your environment that require action (all three are checked). A 'Save' button is at the bottom of the customization panel.

Our service health dashboard shows most of our services are healthy

The screenshot shows the Microsoft 365 admin center Service status dashboard. The left sidebar is identical to the previous screenshot. The main area displays a table titled 'Service status' with columns for 'Service' and 'Status'. The table lists several services: Exchange Online (5 advisories), Microsoft Intune (1 advisory), SharePoint Online (2 advisories), Dynamics 365 Apps (Healthy), Microsoft 365 apps (Healthy), and Microsoft 365 for the web (Healthy). At the bottom right of the dashboard, there are two buttons: 'Help & support' and 'Give Feedback'.

Service	Status
Exchange Online	5 advisories
Microsoft Intune	1 advisory
SharePoint Online	2 advisories
Dynamics 365 Apps	Healthy
Microsoft 365 apps	Healthy
Microsoft 365 for the web	Healthy

We have a few advisories on the health dashboard. This has minimal impact and happens sometimes due to updates



The screenshot shows the Microsoft 365 admin center interface. On the left, there's a navigation sidebar with various service icons like Viva, Partner relationships, Microsoft Edge, Setup, Reports, Health, Service health, Windows release health, Message center, Product feedback, Network connectivity, Software updates, and Admin centers. The 'Health' section is expanded. The main content area displays an advisory titled 'Some users' devices may be offered a Windows 11 upgrade despite Microsoft Intune policies being configured otherwise'. It includes sections for 'User impact', 'More info', and a link to a troubleshooting article. On the right, there's a sidebar with details: Issue ID IT1056135, Affected services Microsoft Intune, Status Service degradation, and Start time Apr 12, 2025, 6:00 PM EDT.

Task 1: Setting Up and Configuring User Accounts

For task 1, I worked on setting up and configuring user accounts within Microsoft 365. The bulk import of users from a CSV file was straightforward, I used the csv notepad file. The csv for users could be done with an excel csv file as well. This enabled me to quickly add multiple users and assign Microsoft 365 E5 licenses. Configuring user profiles involved ensuring each user had a profile picture, contact information, and job title, which helped personalize their accounts and facilitate better communication and identification within the organization. I created Office 365 groups for IT, HR, and Marketing to be used by the members of their respective departments and assigned specific permissions to ensure that sensitive HR documents were secure.

Task 2: Monitoring and Reporting

In this task, configuring audit logs in the Microsoft 365 compliance center allowed me to track user activities, providing valuable insights into user behavior. Setting up alert policies to notify administrators of suspicious activities, like mass file deletions, helped in promptly addressing potential security threats. Generating usage reports on user activity, email usage, and SharePoint site usage provided me an understanding of organizational operations, and scheduling monthly reports ensured that IT administrators and department heads were kept informed. Implementing and monitoring service health alerts ensured that any issues with Microsoft 365 services were promptly addressed, maintaining smooth operations. And checking for the advisory notifications on the health dashboard to check the severity and possible outcome of the health status alert.

