

Microsoft 365 Administrator MS-102 Exam Guide

Preface:

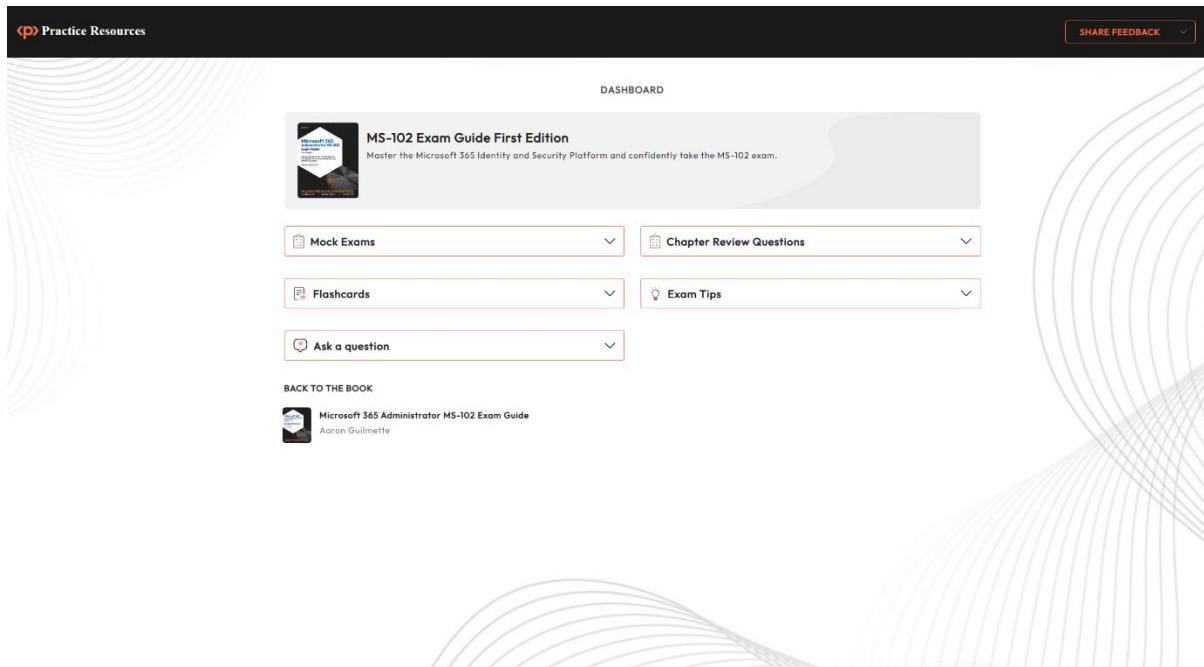


Figure 0.1 – Dashboard interface on a desktop device

A screenshot of the Microsoft 365 Administrator MS-102 Exam Guide practice questions interface. At the top left is a 'Practice Resources' button with a 'p' icon. At the top right is a 'SHARE FEEDBACK' button with a dropdown arrow. The top navigation bar shows 'DASHBOARD > CHAPTER1-QUIZ-1'. The main area displays 'Question 4 of 5' on the left and a timer on the right showing 'Time Left 0 hr 11 mins 41 secs'. An 'END QUIZ' button is at the top right of the question area. The question itself asks: 'Your organization wants to turn off Microsoft Bookings for all employees until the support staff has had time to read the documentation. From the available options, what should you do?'. Four options are listed in boxes with radio buttons: 'Disable all Azure AD user accounts', 'Disable directory synchronization', 'Disable Bookings from Org settings | Services', and 'Disable Bookings from Org settings | Security & privacy'. At the bottom are 'PREVIOUS', 'NEXT', and 'SKIP QUESTION' buttons.

Figure 0.2 – Practice Questions Interface on a desktop device



DASHBOARD > CHAPTER1-QUIZ-1

Question 4 of 5



Time Left

0 hr 10 mins 32 secs

Your organization wants to turn off Microsoft Bookings for all employees until the support staff has had time to read the documentation. From the available options, what should you do?

 Disable all Azure AD user accounts Disable directory synchronization Disable Bookings from Org settings | Services Disable Bookings from Org settings | Security & privacy[PREVIOUS](#)[NEXT](#)[SKIP QUESTION](#)

The screenshot shows the 'Flashcards' section of the Practice Resources interface. At the top, there's a header with the 'Practice Resources' logo and a 'SHARE FEEDBACK' button. Below the header, the navigation path is 'DASHBOARD > FLASHCARDS SET 1'. The main area is titled 'Stack 1'. It displays a single flashcard with the question 'What do Attack Surface Reduction rules do?'. Above the question, it says 'Flashcards memorized so far: 1' and below it says 'Flashcards not memorized yet: 19'. There's a checkbox labeled 'Mark as memorized'. Navigation buttons 'PREVIOUS' and 'NEXT' are at the bottom left, and a page number '5/20' is at the bottom right.

Figure 0.4 – Flashcards interface

The screenshot shows the 'Exam Tips' section of the Practice Resources interface. At the top, there's a header with the 'Practice Resources' logo and a 'SHARE FEEDBACK' button. Below the header, the navigation path is 'DASHBOARD > EXAM TIPS'. The main area is titled 'Utilize Microsoft Learn (2/30)'. It contains a tip text: 'Microsoft Learn is Microsoft's documentation and training platform to assist individuals in upskilling on Microsoft technologies. The platform has interactive and hands-on learning content developed to assist you in understanding the syllabi of Microsoft exams. This book frequently links to additional Microsoft Learn content (typically under the Further reading headings) to point you toward deep technical information. Microsoft exams now include the ability to look up content on Microsoft Learn during the exam. This does not mean you don't have to study—you'll exhaust all your allotted exam time if you look up every question. Instead, familiarize yourself with the topics for the products or features in the exam study guide and know where to go if you can't recall the particulars of a command's syntax or the correct wording of an option.' Navigation buttons '← PREVIOUS' and 'NEXT →' are at the bottom left, and a checkbox labeled 'Mark as Helpful (0 users found this tip helpful)' is at the bottom right. A 'Comments' section with a text input field 'Add your comment' is also present.

Figure 0.5 – Exam Tips Interface

The screenshot shows a dark-themed web interface for 'Practice Resources'. At the top right is a 'SHARE FEEDBACK' button. Below it, a navigation bar includes 'DASHBOARD > CHAPTER 1'. The main content area is titled 'Implementing and Managing a Microsoft 365 Tenant' under a 'Summary' section. A text box states: 'In this chapter, you learned about the fundamental aspects and terminology of configuring a Microsoft 365 tenant, such as selecting a tenant type, adding domains, and configuring the basic organization settings. In Chapter 2, Managing Users and Groups, you will begin to learn how to manage the life cycle of an identity.' To the right is a 'Chapter Review Questions' sidebar with the title 'The Microsoft 365 Administrator MS-102 Exam Guide by Aaron Guilmette'. It features a 'Select Quiz' section with 'Quiz 1' and a 'START' button, along with a 'SHOW QUIZ DETAILS' link.

Figure 0.6 – Chapter Review Questions Page

The screenshot shows a dark-themed web interface for 'Practice Resources'. At the top right is a 'SHARE FEEDBACK' button. Below it, a navigation bar includes 'DASHBOARD'. The main content area features a large 'MS-102 Exam Guide First Edition' card with a book cover thumbnail, the title, and a subtitle: 'Master the Microsoft 365 Identity and Security Platform and confidently take the MS-102 exam.'. Below this are four dropdown menu cards: 'Mock Exams', 'Chapter Review Questions', 'Flashcards', and 'Exam Tips'. At the bottom left is a 'BACK TO THE BOOK' card with a book cover thumbnail, the title 'Microsoft 365 Administrator MS-102 Exam Guide', and the author's name 'Aaron Guilmette'.

Figure 0.7 – Jump back to the book from the dashboard

Chapter 1: Implementing and Managing a Microsoft 365 Tenant

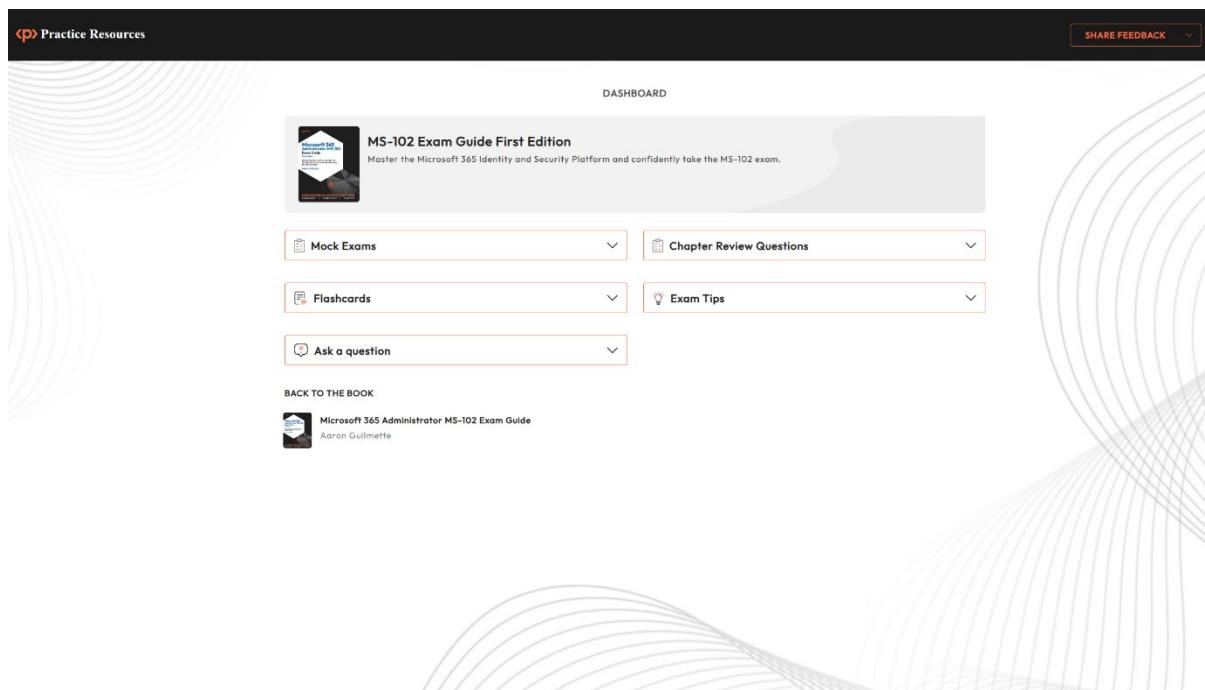


Figure 1.1 – Dashboard Interface Of MS-102 Practice Resources

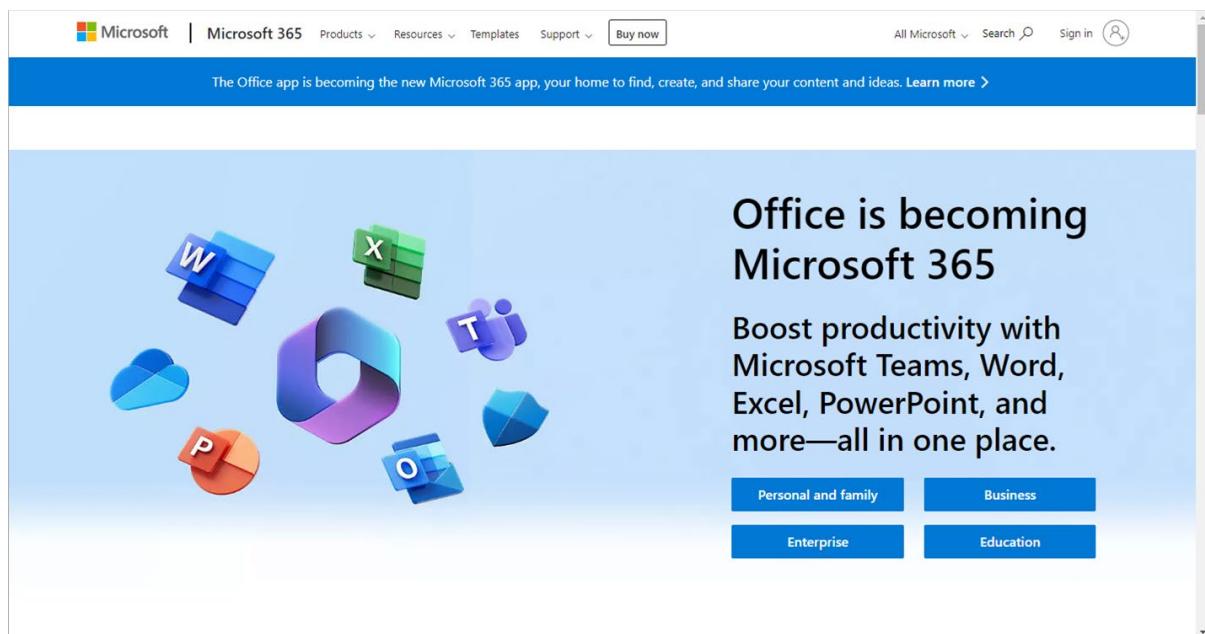


Figure 1.2 – Types of tenants

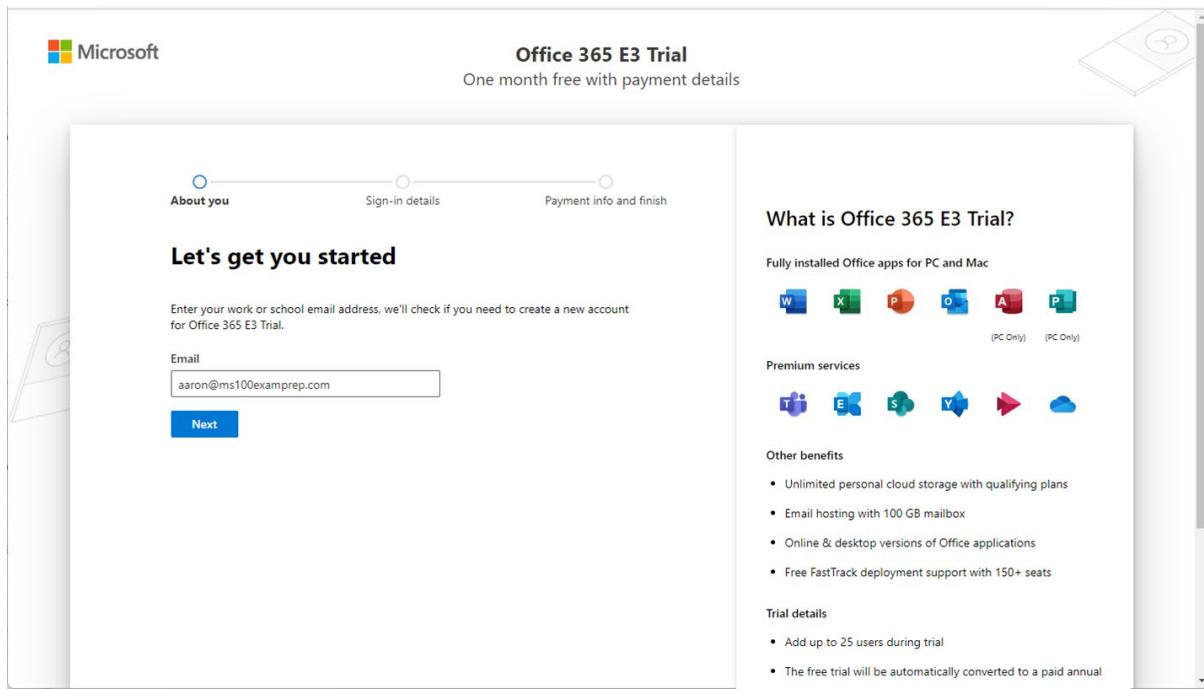


Figure 1.3 – Starting a trial subscription

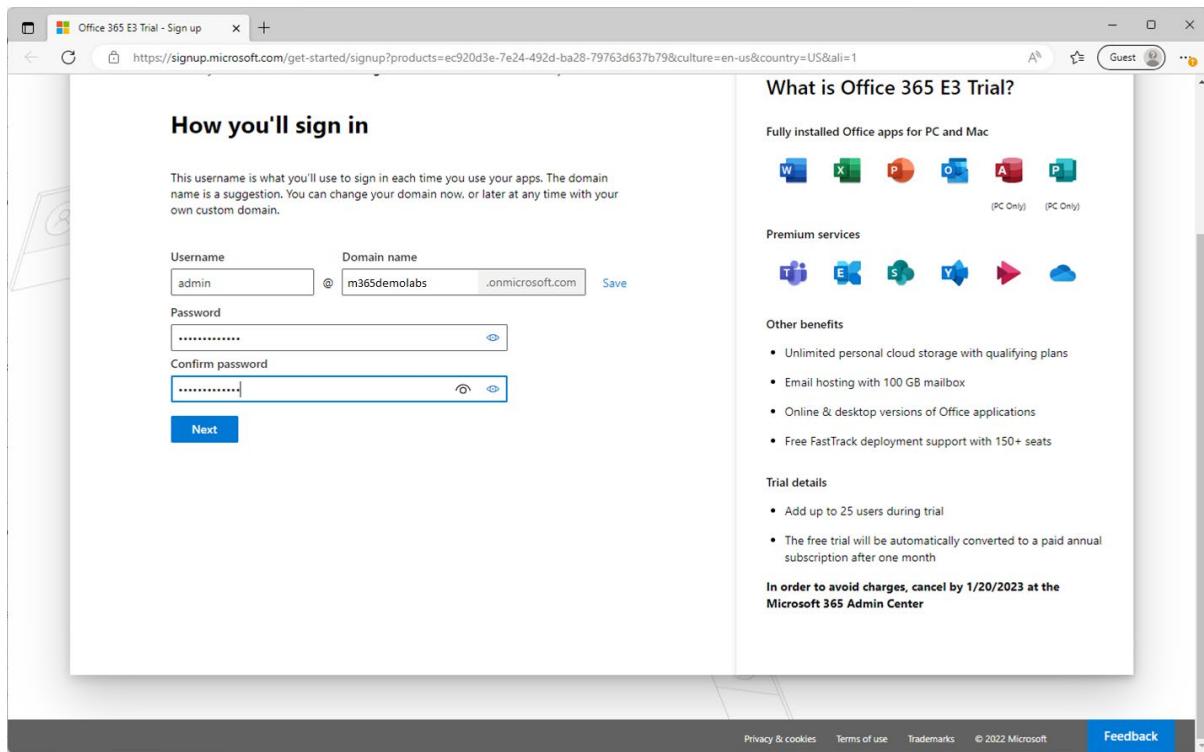


Figure 1.4 – Choosing a managed domain

The screenshot shows the Microsoft 365 admin center interface. The left sidebar has sections for Home, Users, Teams & groups, Roles, Billing, Purchase services, Your products, and Licenses. The main content area is titled 'Domains' and shows a table with one row. The row contains the domain name 'm365demolabs.onmicrosoft.com (Default)' and a status indicator 'Healthy'. There are buttons for '+ Add domain', 'Buy domain', and 'Refresh' at the top of the table.

Figure 1.5 – Purchasing a domain through the Microsoft 365 admin center

This screenshot is similar to Figure 1.5, but the left sidebar is expanded to show the 'Domains' option under the 'Settings' section, which is highlighted with a blue selection bar.

Figure 1.6 – Domains page of the Microsoft 365 admin center

This screenshot shows the 'Add domain' page. The left sidebar has a tree view with 'Add domain' selected. The main area is titled 'Add a domain' and contains a text input field for 'Domain name' with 'm365demolabs.com' typed in. Below the input field is a video player showing a 'Microsoft 365 Add a domain' tutorial. A progress bar indicates the video is 0:56 min long. At the bottom are buttons for 'Use this domain', 'Help & support', 'Give feedback', and 'Close'.

Figure 1.7 – Add domain page

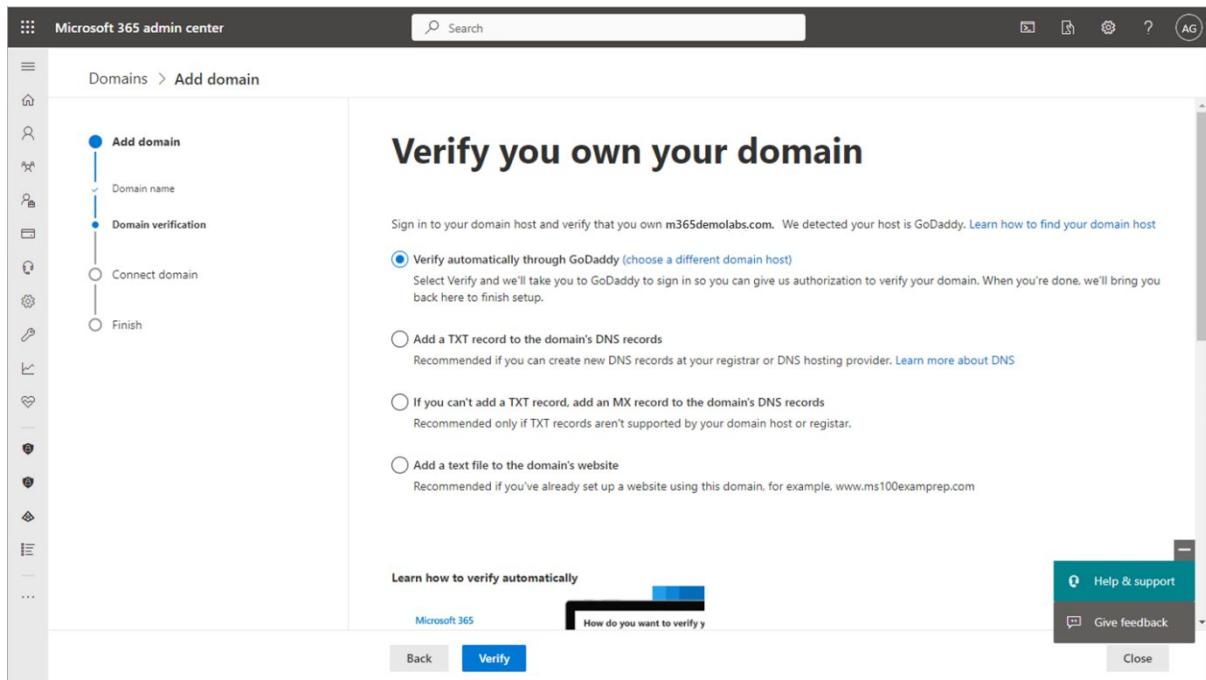


Figure 1.8 – Verify domain ownership

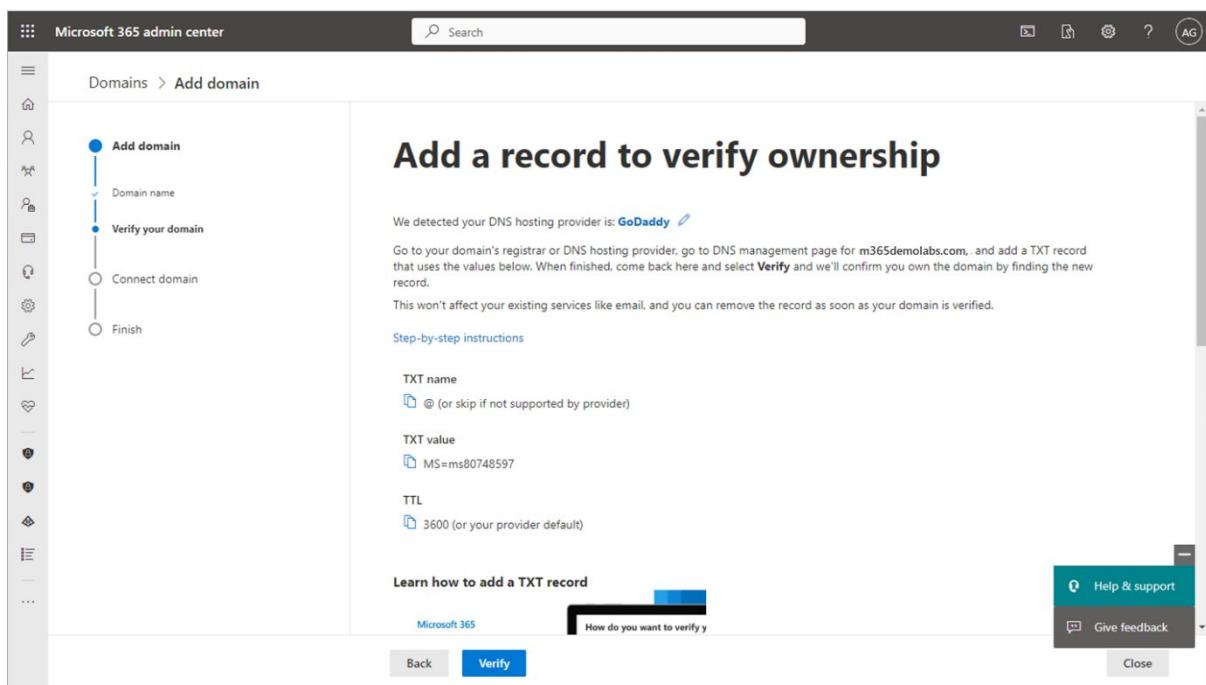


Figure 1.9 – Completing verification records manually

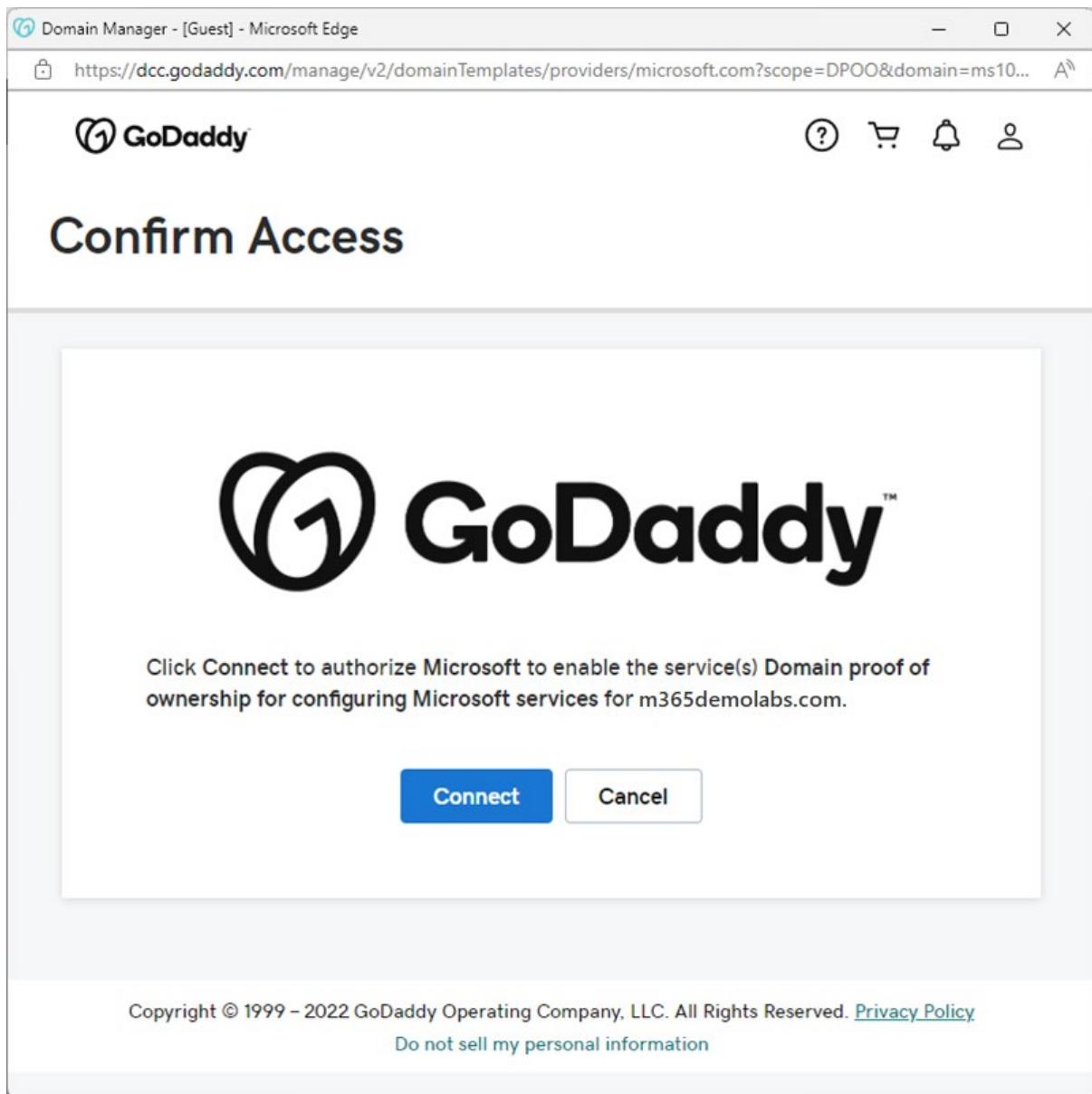


Figure 1.10 – Authorizing Domain Connect with GoDaddy to update DNS records

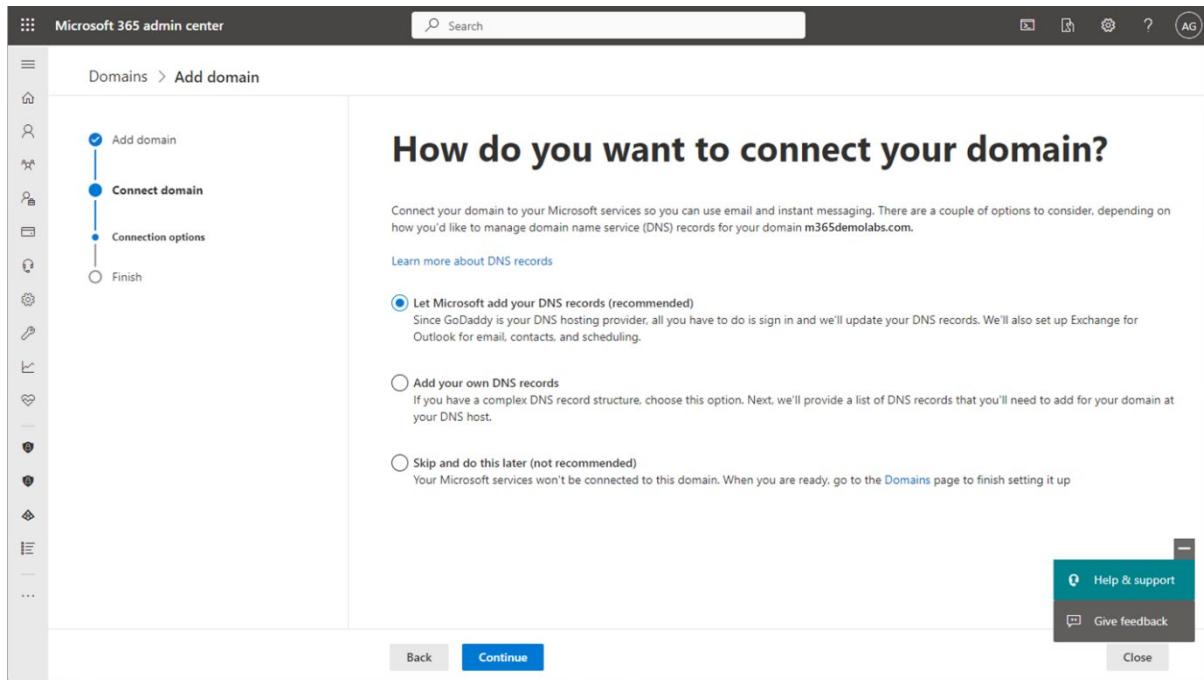


Figure 1.11 – Connecting domain to Microsoft 365

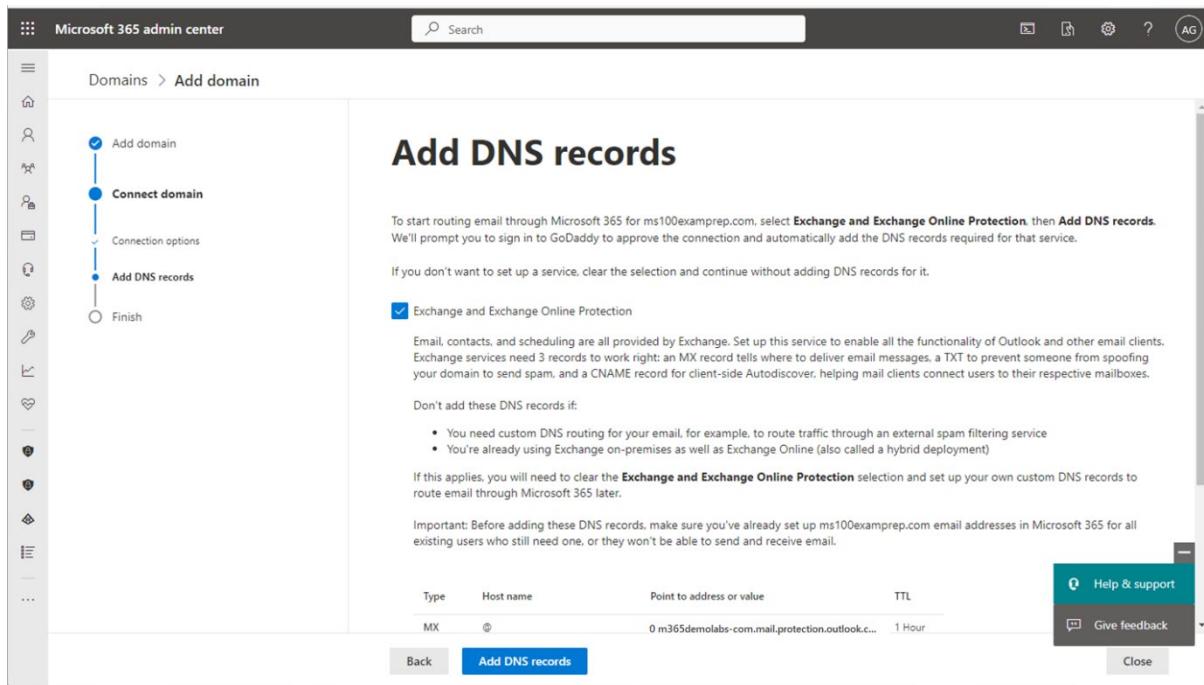


Figure 1.12 – Adding DNS records

The screenshot shows the Microsoft 365 admin center interface. The left sidebar has a 'Domains' section under 'Settings'. The main content area is titled 'Domains' and shows a list of domains. There are two entries: 'm365demolabs.onmicrosoft.com (Default)' and 'm365deolabs.com'. Both domains are listed as 'Healthy' with green status indicators. A search bar and filter options are at the top of the list.

Figure 1.13 – Managing DNS settings for a domain

The screenshot shows the 'Manage DNS' page in the Microsoft 365 admin center. On the left, there's a navigation tree with 'Domains' selected. The main area is titled 'Manage DNS' and shows a wizard-like process with steps: 'Connect domain', 'Connection options', 'Add DNS records', and 'Finish'. Under 'Add DNS records', there's a section for 'MX Records (1)'. A table lists one record: 'Expected' host name 'm365demolabs-mail.protection.outlook.com' with priority 0 and TTL 1 Hour. There are buttons for 'Back', 'Continue', and 'Close' at the bottom.

Figure 1.14 – Viewing DNS settings

The screenshot shows the 'Domains' page in the Microsoft 365 admin center. The left sidebar has a 'Domains' section under 'Settings'. The main content area shows a list of domains. The entry for 'm365deolabs.com' has a blue star icon next to it, indicating it is set as the default domain. Other entries include 'm365demolabs.onmicrosoft.com (Default)'. A search bar and filter options are at the top of the list.

Figure 1.15 – Setting the default domain

The screenshot shows the Microsoft 365 admin center interface. The left sidebar has a navigation menu with sections like Users, Teams & groups, Roles, Billing, Support, Settings, Domains, Admin centers, and Security. The 'Org settings' section is currently selected under 'Settings'. The main content area is titled 'Org settings' and shows a table of organization settings. The table has two columns: 'Name' and 'Description'. The rows include Adoption Score, Azure Speech Services, Bookings, Briefing email from Microsoft Viva, Calendar, Cortana, Directory synchronization, Dynamics 365 Applications, Dynamics 365 Customer Voice, Mail, and Microsoft Azure Information Protection. A search bar at the top right says 'Search all settings' and shows '37 items'.

Name	Description
Adoption Score	Manage privacy levels for Adoption Score.
Azure Speech Services	Allow use of your organization's emails and documents to improve speech recognition accuracy.
Bookings	Choose whether to allow Microsoft Bookings and its features in your organization.
Briefing email from Microsoft Viva	Allow people in your organization to receive Briefing email
Calendar	Allow users to share their calendars with people outside of your organization.
Cortana	Manage Cortana data access for Windows versions 1909 and earlier and Cortana app on iOS and Android.
Directory synchronization	Sync users to the cloud using Azure Active Directory.
Dynamics 365 Applications	Allow Dynamics 365 Applications to generate insights based on user data.
Dynamics 365 Customer Voice	Choose to record the names of people who fill out surveys.
Mail	Set up auditing, track messages, and protect email from spam and malware in the Exchange admin center.
Microsoft Azure Information Protection	Update your settings for Microsoft Azure Information Protection.

Figure 1.16 – Org settings in the Microsoft 365 admin center

The screenshot shows the Microsoft 365 admin center interface. The left sidebar has a navigation menu with sections like Support, Settings, Setup, Reports, and Health. The 'Health' section is currently selected. The main content area is titled 'Health dashboard' and shows a message: 'View data about your Microsoft 365 apps and services, and see recommended actions to keep your organization up-to-date and secure. This page is in preview, so please share your feedback.' Below this is a green banner stating 'Great! No critical alerts to show. Last updated on Dec 7, 2022'. The main section is titled 'Service health and usage' and shows a table of service status. The table has three columns: 'Apps and services', 'Health', and 'Active users'. The services listed are SharePoint, Exchange Online, OneDrive, and Yammer, all marked as 'Healthy' with 20, 20, 5, and 7 active users respectively.

Apps and services	Health	Active users
SharePoint	Healthy	20
Exchange Online	2 advisories	20
OneDrive	Healthy	5
Yammer	Healthy	7

Figure 1.17 – Service health dashboard

The screenshot shows the Microsoft 365 admin center interface. The left sidebar is collapsed. The main content area has a header bar with a search bar, a 'Report an issue' button, and a 'Customize' button. Below this is a section titled 'Active issues' with a table. The table has columns for 'Issue title', 'Affected service', and 'Issue type'. There are three entries under 'Microsoft service health (3)'. At the bottom of the table, it says 'Issues in your environment that require action (0)'. To the right of the table, there is a section titled 'Microsoft service health' with a sub-section 'Shows the current health status of your Microsoft services, and updates when we fix issues.' It lists two services: 'Exchange Online' with 2 advisories and 'Microsoft 365 Defender' with 1 advisory. A blue callout box points to the first advisory in the 'Active issues' table.

Issue title	Affected service	Issue type
Jordanian users' calendar invites from outside of the country may show the incorrect time	Exchange Online	Advisory
Users' email list downloads via Threat Explorer may fail to do...	Exchange Online	Advisory
Admins are unable to see malware detections using the Mic...	Microsoft 365 Defender	Advisory

Figure 1.18 – Service health page

This screenshot is identical to Figure 1.18, showing the 'Active issues' table. The first row of the table is highlighted with a blue selection bar. The 'Issue title' column contains the text 'Jordanian users' calendar invites from outside of the country may show the incorrect time'. The 'Affected service' column shows 'Exchange Online' and the 'Issue type' column shows 'Advisory'. A blue callout box points to this specific row.

Figure 1.19 – Service health active issues

The screenshot shows the Microsoft 365 admin center interface. On the left, there's a sidebar with various icons and links. The main area has a search bar at the top. A modal window is open, titled "Jordanian users' calendar invites from outside of the country may show the incorrect time". The modal contains the following information:

- Issue title: "Jordanian users' calendar invites from outside of the country may show the incorrect time"
- Affected services: Exchange Online
- Issue type: Advisory
- Issue origin: Microsoft
- Status: Service degradation
- Actions: "Manage notifications for this issue"
- User impact: (not visible)

Below the modal, there's a section titled "Active issues" which lists "Microsoft service health (3)" items.

Figure 1.20 – Expanded active issue

The screenshot shows the "Service health" page in the Microsoft 365 admin center. The left sidebar is visible with various navigation options. The main content area shows the "Service health" overview. At the bottom of the main content, there are "Report an issue" and "Customize" buttons. The "Customize" button is highlighted with a blue border. The right side of the screen shows a dark mode toggle and a timestamp: "June 13, 2023 at 10:11 AM EDT".

Figure 1.21 – Service health page with Customize highlighted

The screenshot shows the "Service health" page with the "Customize" button highlighted. A modal window titled "Customize" is open on the right. It has two tabs: "Page view" and "Email", with "Email" selected. Under the "Email" tab, there's a checkbox "Send me email notifications about service health" which is checked, and a text input field "Enter up to 2 email addresses, separated by a semicolon" containing "service@m365demolabs.com". Below this, there are sections for "Include these issue types" (Incidents, Advisories, Issues in your environment that require action) and "Include these services" (Azure Information Protection, Dynamics 365 Apps). A "Save" button is at the bottom of the modal.

Figure 1.22 – Enabling notifications

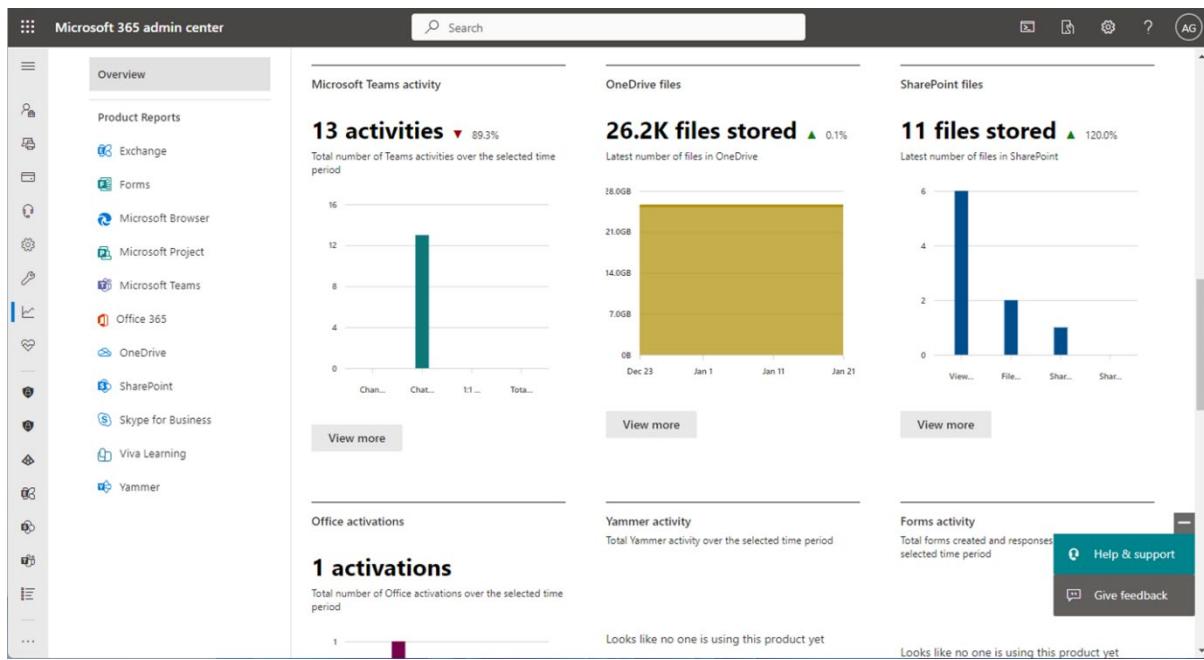


Figure 1.23 – Microsoft 365 usage reports

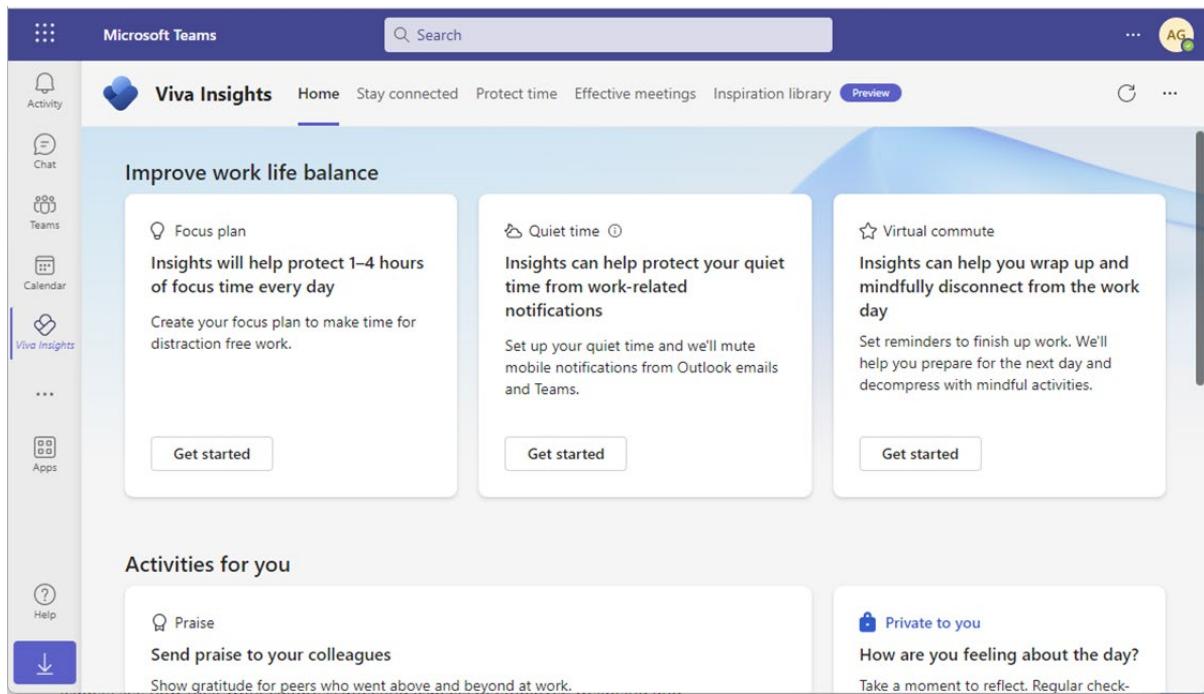


Figure 1.24 – Viva Insights app in Microsoft Teams

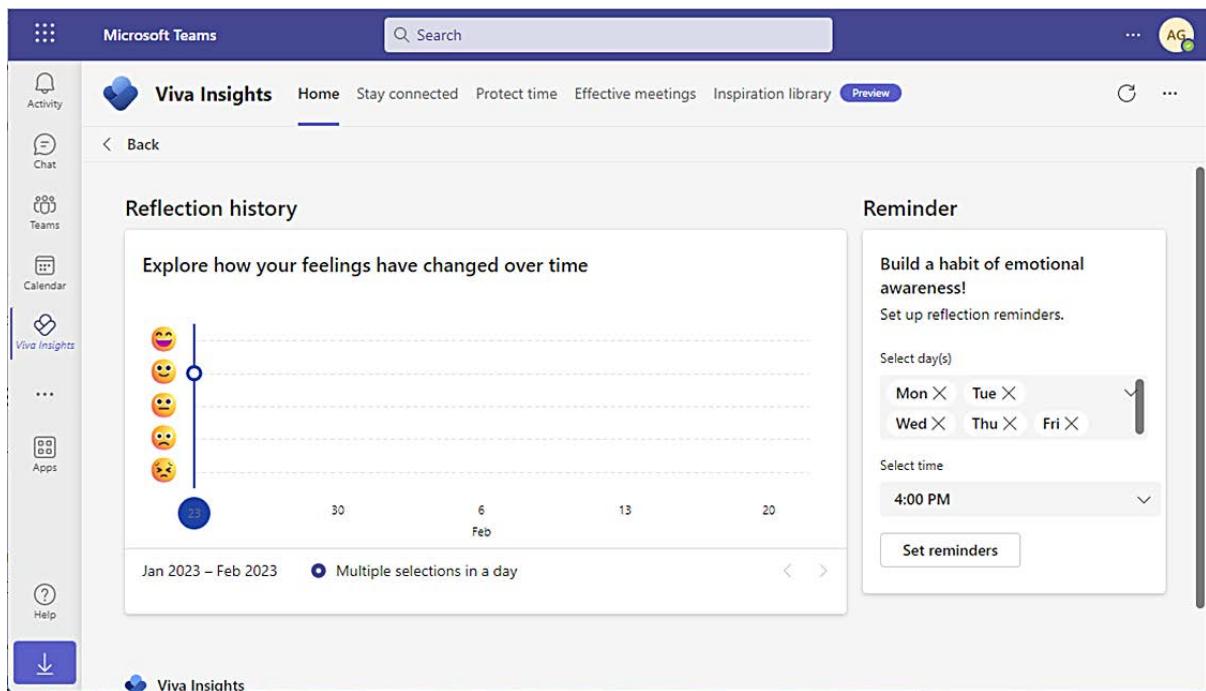


Figure 1.25 – Reflection activity card

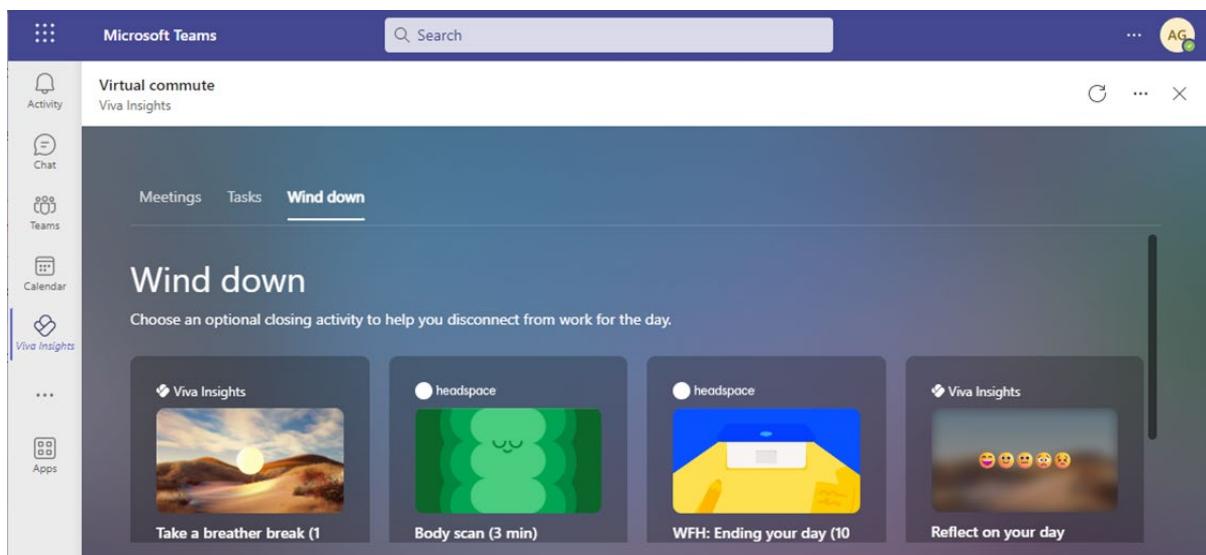


Figure 1.26 – Virtual commute activity card

The screenshot shows the Microsoft Teams Viva Insights Home page. On the left, there's a sidebar with icons for Activity (31), Chat (2), Teams (88), Calendar, Viva Insights (selected), and Help. The main content area has a search bar at the top. The 'Home' tab is selected in the Viva Insights navigation bar. Below it, a section titled 'Confirm your team' displays six team members: Alex Wilber, Christie Cline, Isaiah Langer, Megan Bowen, Adele Vance, and Lynne Robbins, each with a small profile picture. There are 'Confirm' and 'Edit' buttons. To the right is a large blue circular graphic. Below this, a section titled 'Improve work life balance' contains three cards: 'Focus plan' (with a note about protecting 1-4 hours of focus time every day), 'Quiet time' (with a note about protecting quiet time from work-related notifications), and 'Virtual commute' (with a note about wrapping up work and disconnecting). A download button is visible on the far left.

Figure 1.27 – Confirming team members

The screenshot shows the Microsoft Teams Viva Insights 'My organization' page. The sidebar on the left includes icons for Activity, Chat, Insights sim (selected), Apps, and Help. The main content area features a 'Outcomes' section with a sidebar listing: Organizational resiliency, Boost engagement, Improve agility, Foster innovation, Effective managers, Operational effectiveness, Accelerate change, Transform meeting culture, and Increase customer focus. Below this is a 'Download PowerPoint' button. The central part of the page shows 'Outcomes' from Dec 26, 2021 – Mar 19, 2022, for 549 included team members. It includes a 'Boost engagement' section with a note about burnout risk and a bar chart titled 'Average weekly time spent collaborating after hours'. The chart shows: 0-1 hours (62%), 1-3 hours (34%), and 3+ hours (4%). To the right, there are two 'Organizational' trend cards: one for '46%' (with a 'Is this helpful? Yes No' button) and another for '44%' (also with a 'Is this helpful? Yes No' button).

Figure 1.28 – Organization trends

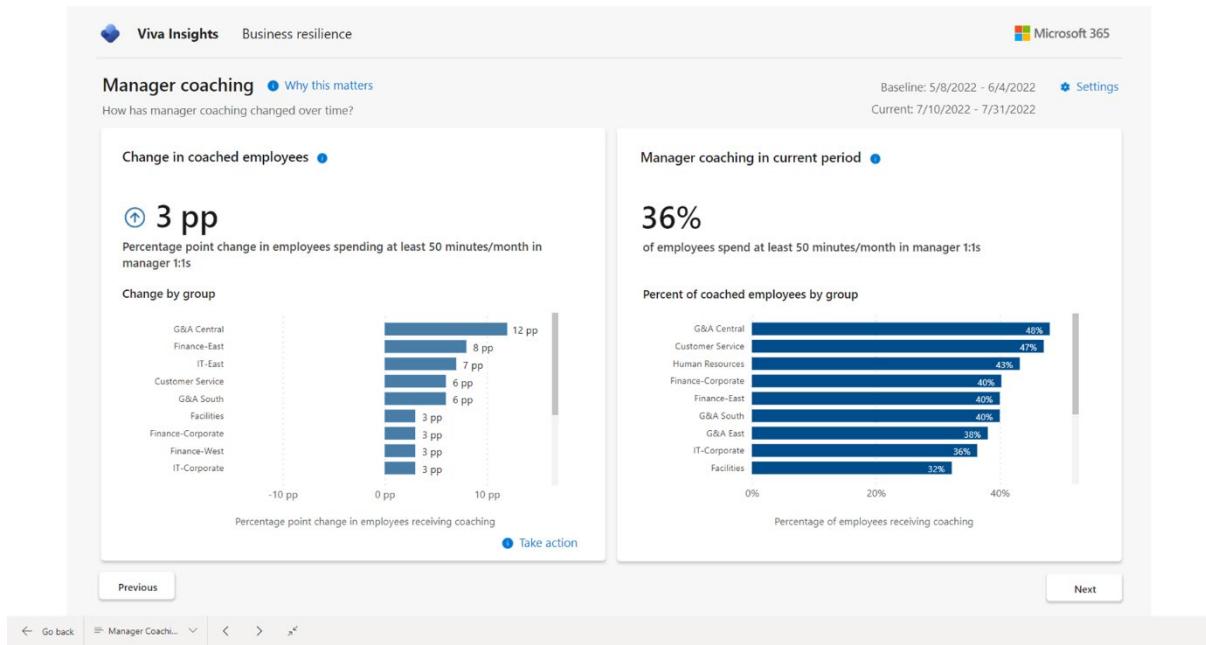


Figure 1.29 – Viva Insights Manager coaching report

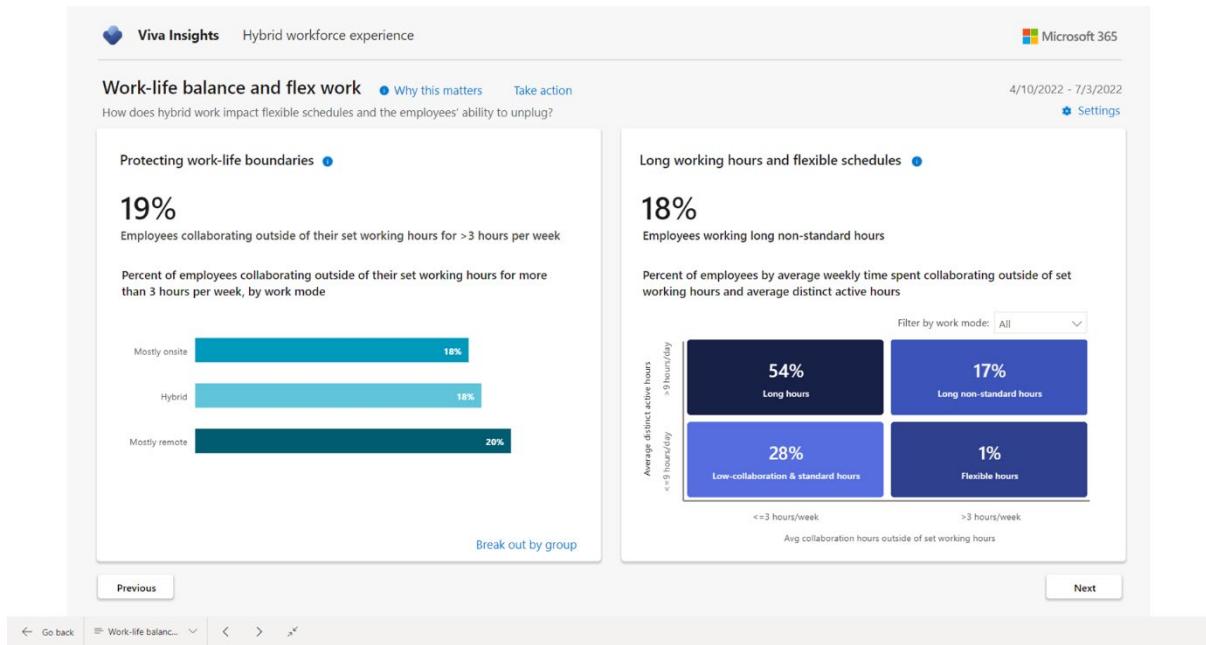


Figure 1.30 – Advanced insights working hour details

The screenshot shows the Microsoft 365 admin center interface. On the left, there is a navigation sidebar with various categories like Teams & groups, Roles, Resources, Billing, Support, Settings, Setup, Reports, Adoption Score (which is selected), Usage, Health, Admin centers, and Security. The main content area is titled "Adoption Score" and contains a brief description of what Adoption Score provides. Below the description, a message says "Adoption Score is now available" and "Enable Adoption Score to learn how people in your org use Microsoft 365, and how your org's Technology infrastructure influences productivity." A blue button labeled "Turn on Adoption Score" is visible. The top right corner has a "Dark mode" toggle, a user profile icon, and other standard interface icons.

Figure 1.31 – Enabling Adoption Score

The screenshot shows the "Practice Resources" page. At the top, there is a header with "Practice Resources" and a "SHARE FEEDBACK" button. Below the header, the breadcrumb navigation shows "DASHBOARD > CHAPTER 1". The main content area is titled "Implementing and Managing a Microsoft 365 Tenant" and has a "Summary" section. The summary text states: "In this chapter, you learned about the fundamental aspects and terminology of configuring a Microsoft 365 tenant, such as selecting a tenant type, adding domains, and configuring the basic organization settings. In Chapter 2, Managing Users and Groups, you will begin to learn how to manage the life cycle of an identity." To the right, there is a "Chapter Review Questions" section. It includes the title "Chapter Review Questions", the subtitle "The Microsoft 365 Administrator MS-102 Exam Guide by Aaron Guilmette", and a "Select Quiz" button. Below the quiz selection, it shows "Quiz 1" and a "START" button. There is also a "SHOW QUIZ DETAILS" link.

Figure 1.32 – Chapter Review Questions for Chapter 1

Chapter 2: Managing Users and Groups

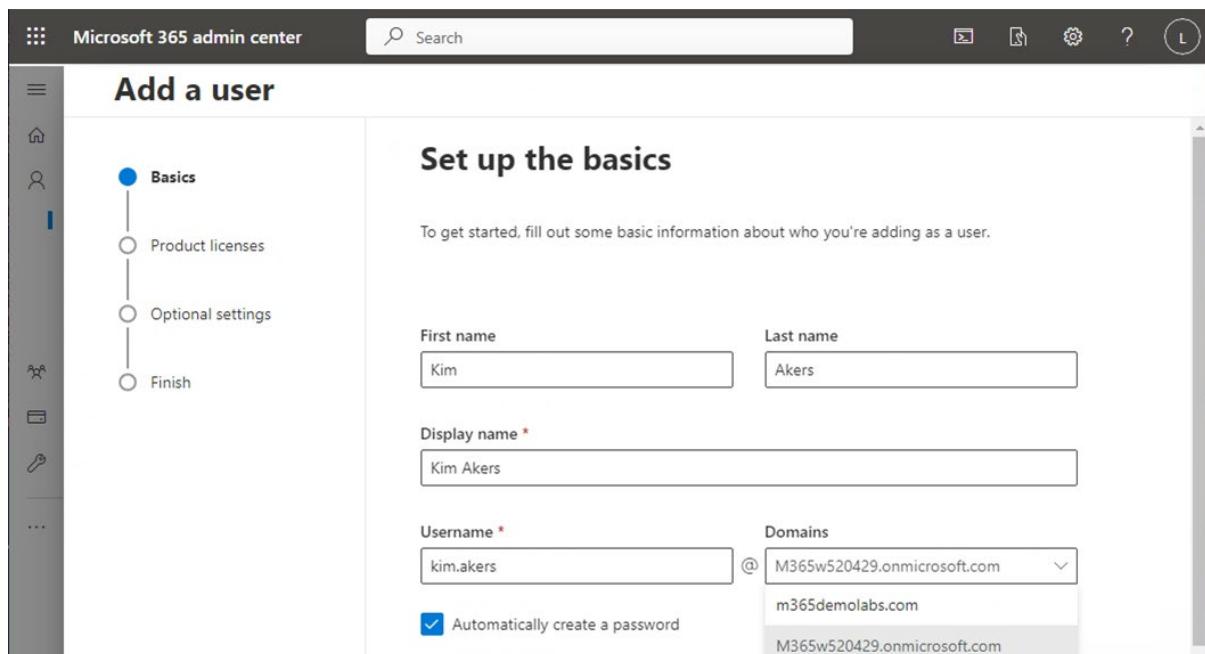


Figure 2.1 – Adding a new cloud user

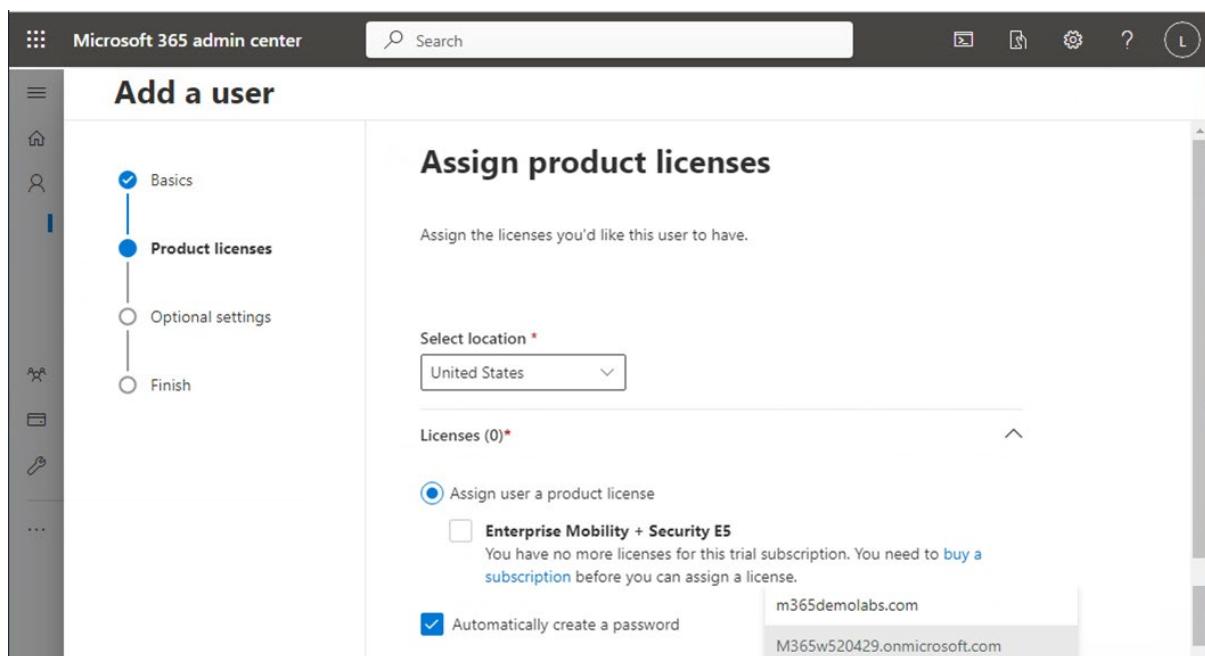


Figure 2.2 – Assign product licenses page

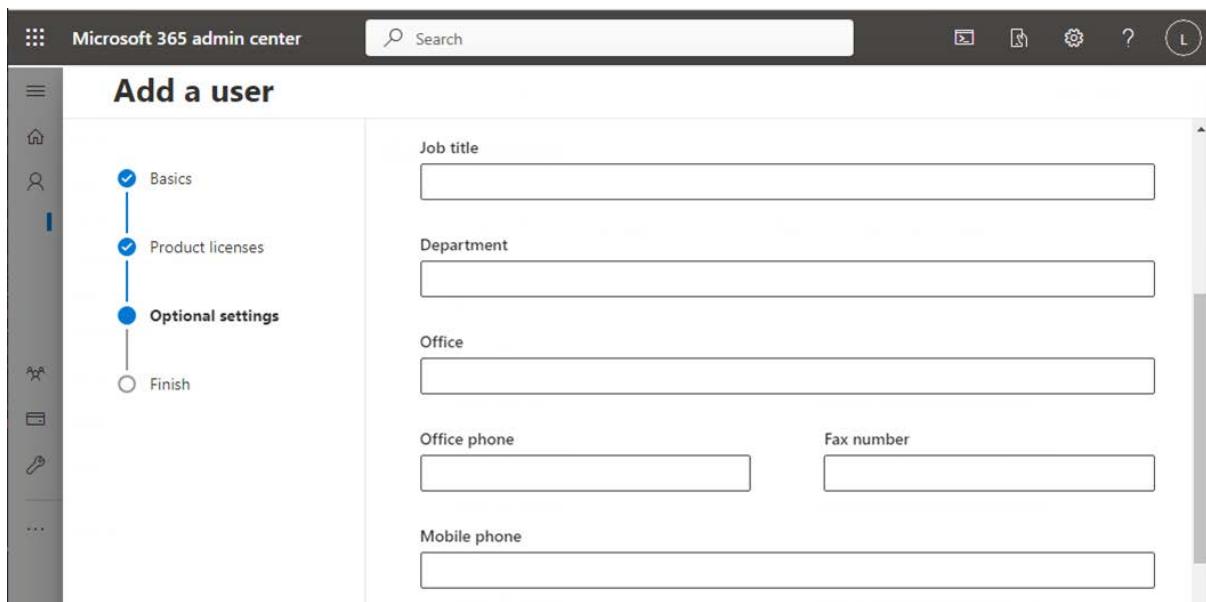


Figure 2.3 – Add a user profile information

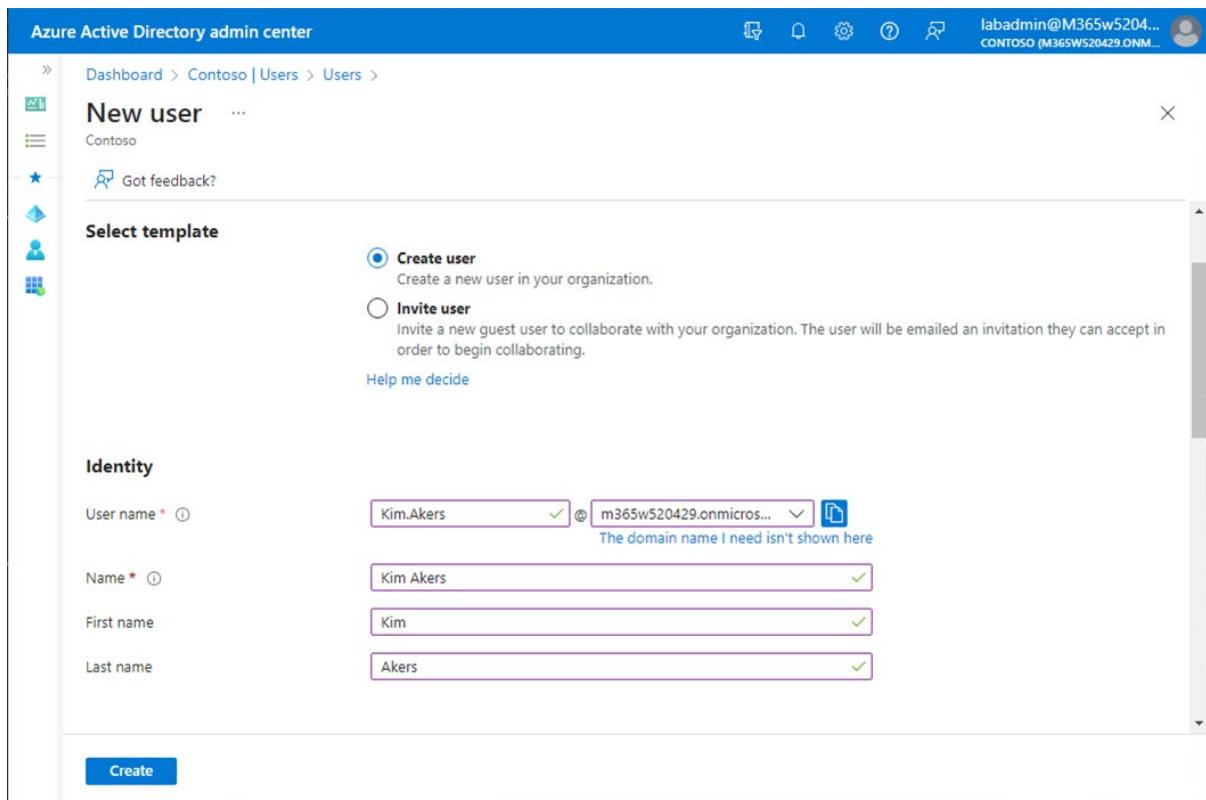


Figure 2.4 – Creating a user through the Azure AD portal

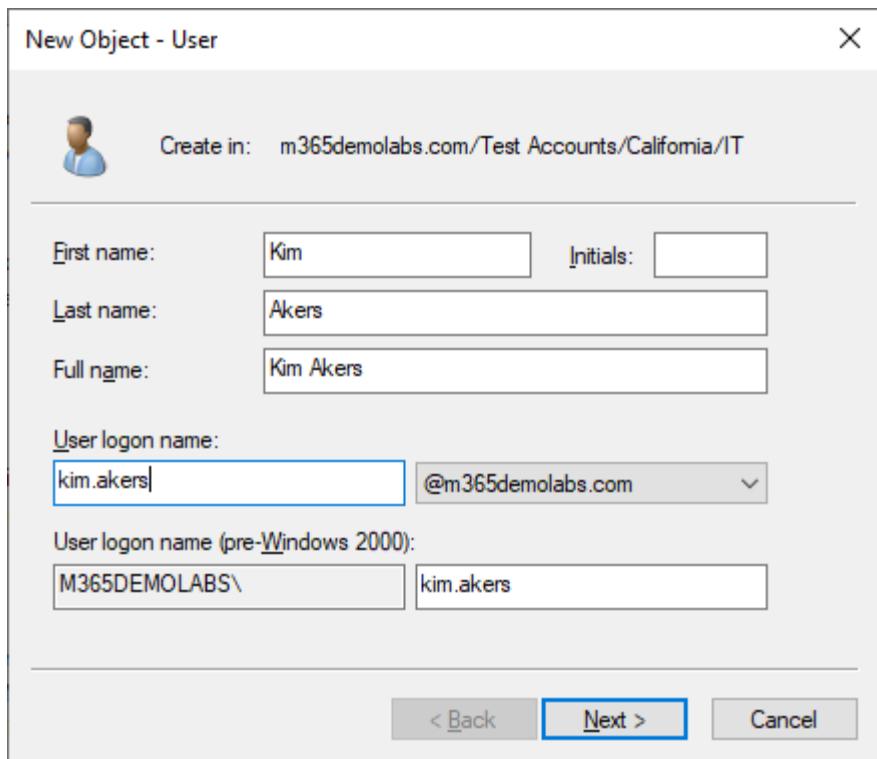


Figure 2.5 – Creating a new user through Active Directory Users and Computers

Display name	Username	Sync status	Action
Kim Akers	kim.akers@m365demolabs.com		
Kim Akerson	kim.akerson@m365demolabs.com		

Figure 2.6 – Displaying cloud and synchronized users

Figure 2.7 – Guest users administration in Microsoft 365 admin center

The screenshot shows the Microsoft Azure portal's 'Users' page for the 'Contoso' tenant. In the top navigation bar, there is a search bar with placeholder text 'Search resources, services, and docs (G+/-)'. To the right of the search bar are several icons: a magnifying glass, a gear, a question mark, a refresh symbol, and a person icon. The top right corner displays the email 'labadmin@M365w5204...' and the tenant name 'CONTOSO (M365W520429.ONM...)'.

The main content area is titled 'Users' with a sub-section 'All users (preview)'. On the left, there is a sidebar with links: 'Audit logs', 'Sign-in logs', 'Diagnose and solve problems', 'Manage', 'Deleted users (preview)', 'Password reset', and 'User settings'. A context menu is open over the 'Create new user' option in the top navigation bar. The menu items are 'Create new user' (selected) and 'Invite external user'. Below the menu, a table lists three users: 'Aamir B Doss', 'Aamir E Cupp', and 'Aamir G Waldron', each with a small profile picture, their email addresses, user type (Member), and whether they are 'On-premises sync' (Yes). The table has columns for 'User principal name', 'User type', 'On-premises sync...', and 'Identifier'.

Figure 2.8 – Inviting a new guest user

This screenshot shows the 'New user' configuration page in the Microsoft Azure portal. The top navigation bar includes a search bar and the same account information as Figure 2.8.

The main title is 'New user' under the 'Contoso' tenant. There is a 'Got feedback?' link. The first section is 'Select template', which contains two options: 'Create user' (unselected) and 'Invite user' (selected). A tooltip for 'Invite user' states: 'Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.' Below this is a 'Help me decide' link.

The next section is 'Identity', which includes fields for 'Name' (with placeholder 'Example: "Chris Green"'), 'Email address *' (with placeholder 'Example: chris@contoso.com'), 'First name', and 'Last name'. All these fields are currently empty.

The final section is 'Personal message', which contains a large text input field for a personal message to the invitee, followed by a 'Send' button at the bottom.

Figure 2.9 – Configuring the guest invitation

Microsoft Azure ... labadmin@M365w5204...
CONTOSO (M365W520429.ONM... ...

Home > Users > aaronguilmette >

aaronguilmette

Properties

Refresh Got feedback?

All Identity Job Information Contact Information Parental controls Settings On-premises

Search

Showing 13 results

Display name	aaronguilmette
First name	
Last name	
User principal name	aaronguilmette_gmail.com#EXT# @ M365w520429.onmicro...
Object ID	bb2b50b8-58e1-4575-8d07-e89530768571
User type	Guest
Creation type	Invitation
Created date time	2023-03-13T19:06:55Z
Last password change date time	2023-03-13T19:06:55Z
Invitation state	PendingAcceptance

Save Cancel

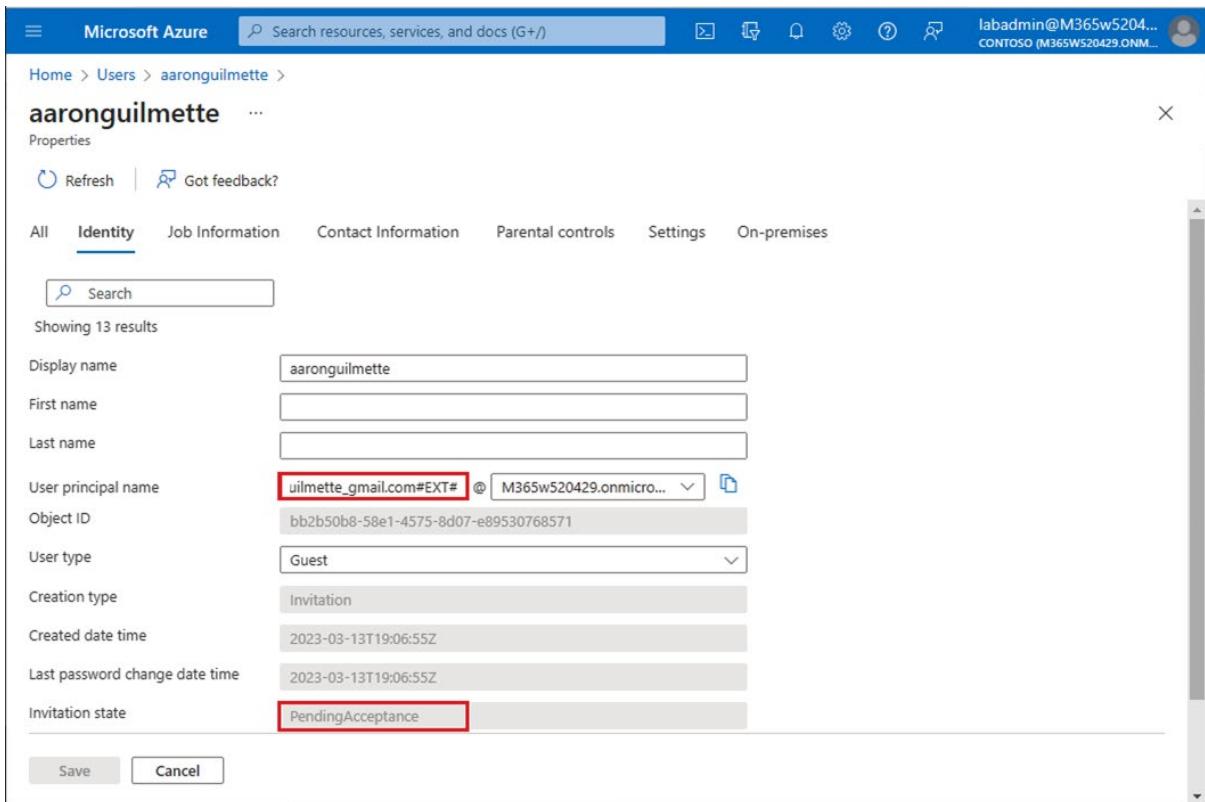


Figure 2.10 – Newly invited guest user



atguilmette@hotmail.com

Permission requested by:

 Contoso
M365w520429.onmicrosoft.com

By accepting, you allow this organization to:

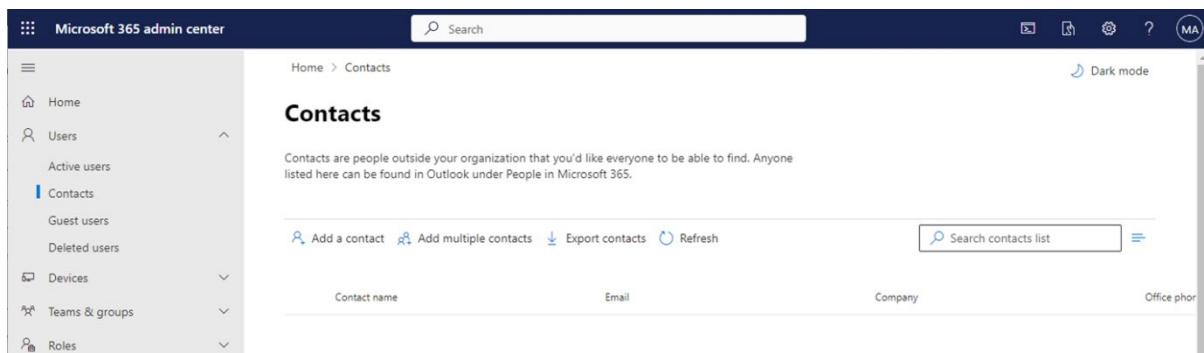
- ✓ Receive your profile data
Your profile data means your name, email address, and photo
- ✓ Collect and log your activity
Your activity data means your access, usage, and content associated with their apps and resources
- ✓ Use your profile data and activity data
This data may be used with your access and use of their apps and resources, as well as to create, control, and administer an account according to their policies

You should only accept if you trust Contoso. **Contoso has not provided a link to their privacy statement for you to review.**
You can update these permissions at <https://myaccount.microsoft.com/organizations>
[Learn More](#)

This resource is not shared by Microsoft.

[Cancel](#) [Accept](#)

Figure 2.11 – Invitation redemption consent



The screenshot shows the Microsoft 365 admin center interface. The left sidebar has a 'Users' section with 'Active users', 'Contacts' (which is selected), 'Guest users', and 'Deleted users'. Below that are sections for 'Devices', 'Teams & groups', and 'Roles'. The main content area is titled 'Contacts' and includes a sub-instruction: 'Contacts are people outside your organization that you'd like everyone to be able to find. Anyone listed here can be found in Outlook under People in Microsoft 365.' It features a search bar, buttons for 'Add a contact', 'Add multiple contacts', 'Export contacts', and 'Refresh', and a 'Search contacts list' input field. A table header with columns for 'Contact name', 'Email', 'Company', and 'Office phor' is visible.

Figure 2.12 – Contacts page in Microsoft 365 admin center

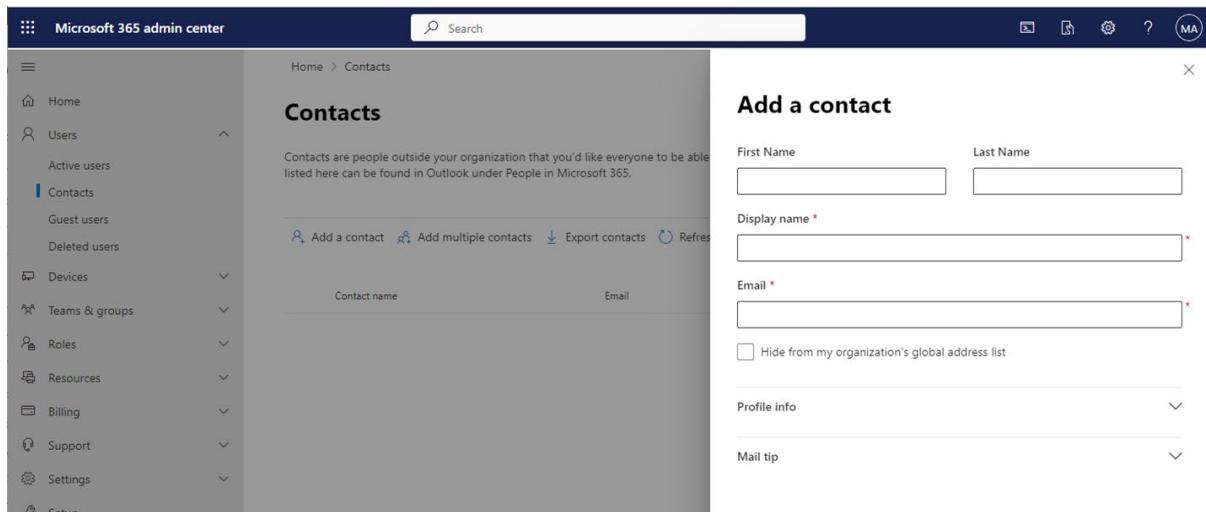


Figure 2.13 – Populating a contact

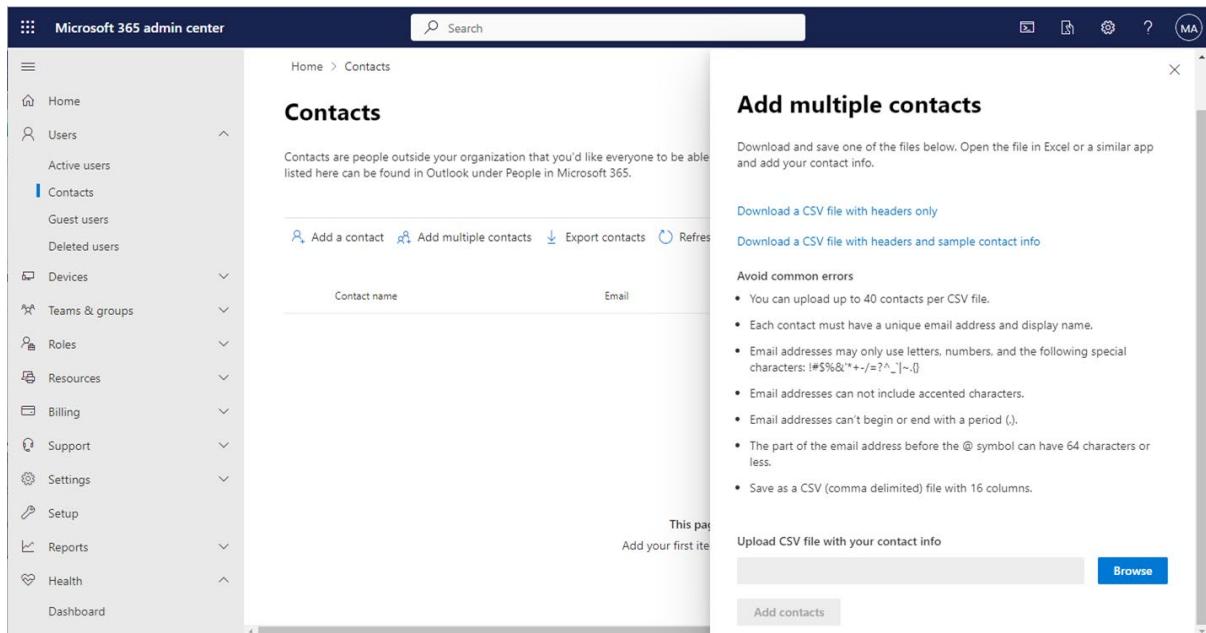


Figure 2.14 – Add multiple contacts flyout

This screenshot shows a Microsoft Excel spreadsheet titled 'Import_Contact_Sample'. The spreadsheet has a header row with columns for Contact number, First name, Last name, Email, Company, Office ph, Mobile ph, Fax numb, Title, Web site, Street, Street, City, State or Pr, Zip or pos, Country or region. Below the header, there is one data row: 'Chris Green, Chris Green, chris@contoso.com, Contoso, 123-555-123-555-6, 123-555-9, IT Manager, www.contoso.com, 1 Microsoft Suite 1, Redmond, Wa, 98052, United States'. The Excel ribbon at the top shows various tabs like File, Home, Insert, etc., and the formula bar shows 'Contact name'.

Contact number	First name	Last name	Email	Company	Office ph	Mobile ph	Fax numb	Title	Web site	Street	Street	City	State or Pr	Zip or pos	Country or region
2	Chris Green	Chris Green	chris@contoso.com	Contoso	123-555-123-555-6	123-555-9	IT Manager	www.contoso.com	1 Microsoft Suite 1	Redmond	Wa	98052	United States		
3															
4															
5															
6															

Figure 2.15 – Bulk contact import template

The screenshot shows the Exchange admin center's Contacts page. The left sidebar has a 'Contacts' section selected. The main area displays a list of contacts with columns for 'Display name', 'Email address', and 'Contact type'. At the top, there are buttons for 'Add a mail contact', 'Add a mail user', 'Export contacts', and 'Refresh'. A search bar and a filter button are also present.

Figure 2.16 – Exchange admin center contact administration

The screenshot shows the 'New Mail Contact' wizard, Step 1: Set up the basic information. It has three tabs: 'Basic information' (selected), 'Mail contact information (Optional)', and 'Review mail contact'. On the right, there are fields for First name, Last name, Initials, Display name, Alias, and External email address. A 'Next' button is at the bottom right.

Figure 2.17 – New Mail Contact wizard in Exchange admin center

The screenshot shows the Microsoft 365 admin center's Active teams & groups page. The left sidebar has a 'Teams & groups' section with 'Active teams & groups' selected. The main area displays a list of active teams and groups with columns for 'Name', 'Email', and 'Sync status'. Buttons for 'Add a group', 'Export', and 'Refresh' are at the top, along with a search bar and filter options.

Figure 2.18 – Active teams and groups

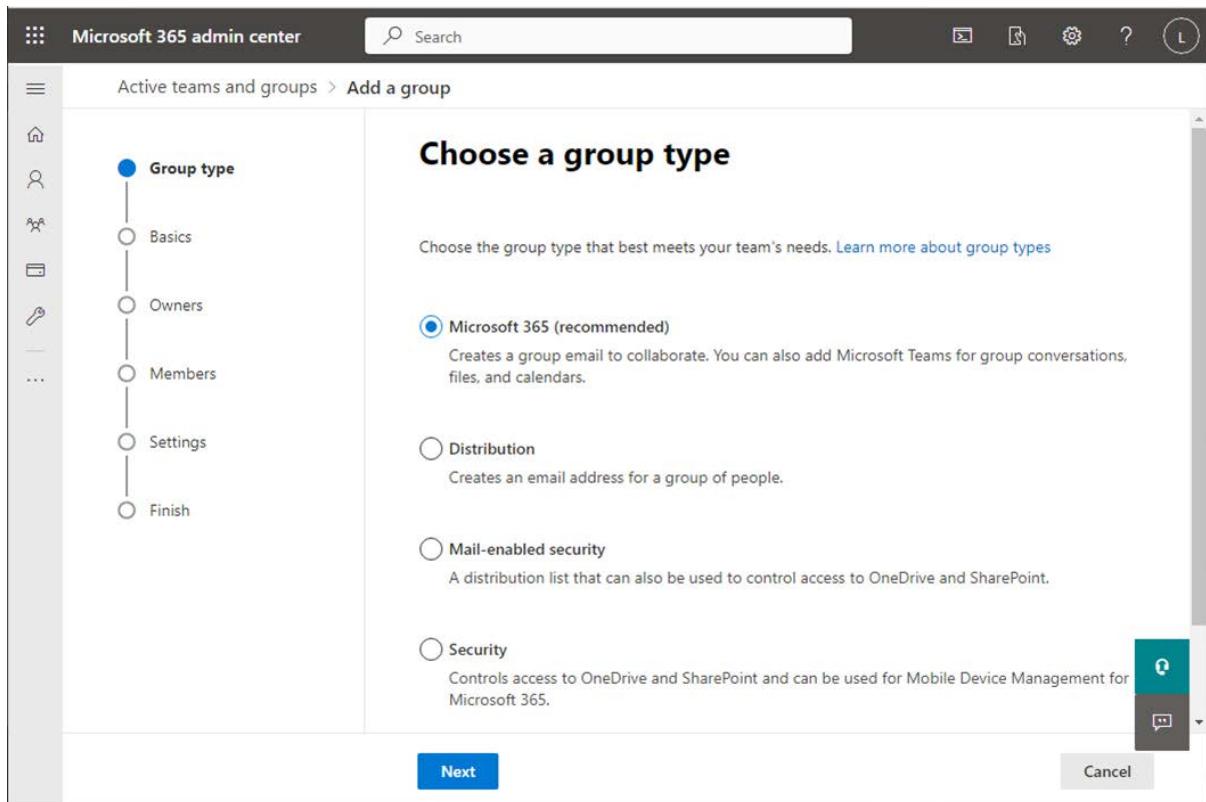


Figure 2.19 – Choose a group type

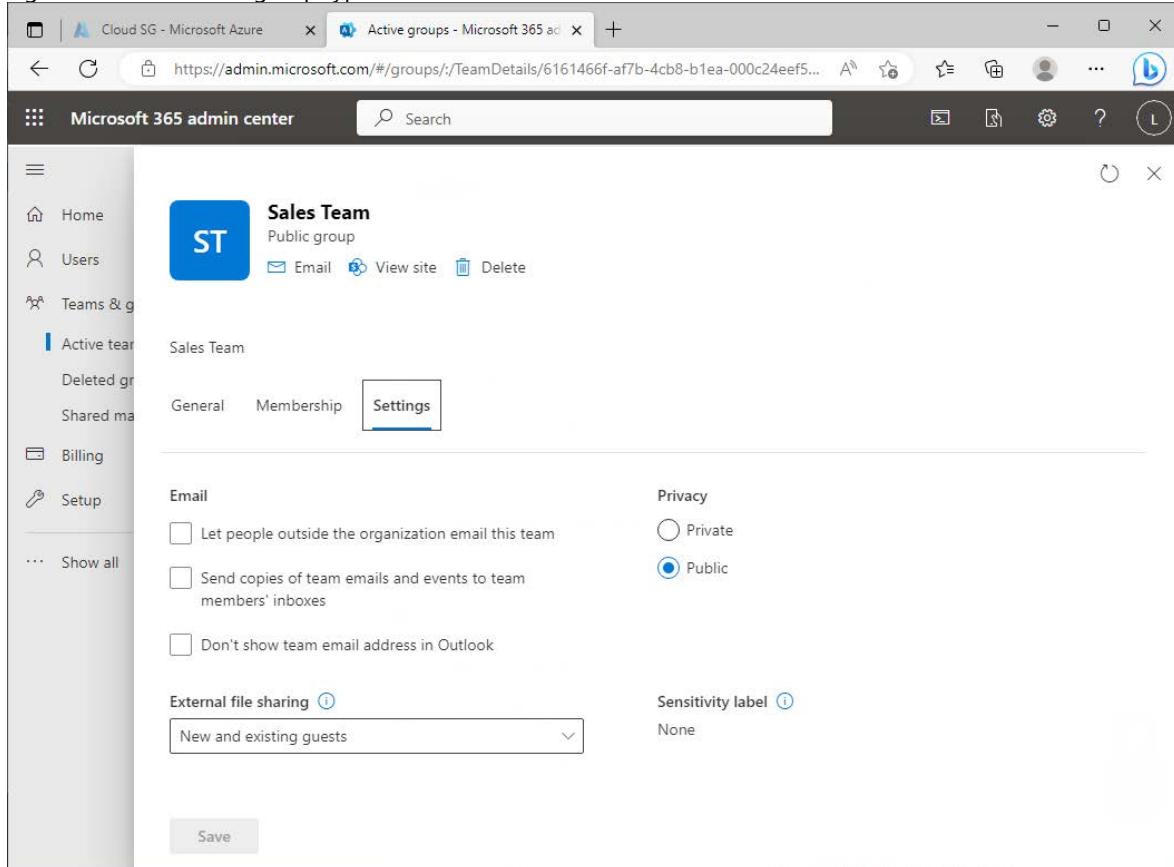


Figure 2.20 – Modifying settings of a Microsoft 365 group

The screenshot shows the 'Groups | All groups' page in the Azure Active Directory admin center. The left sidebar includes links for 'All groups', 'Deleted groups', 'Diagnose and solve problems', 'Settings' (General, Expiration, Naming policy), and 'Activity'. The main area features a search bar, a 'Search mode' toggle set to 'Contains', and a table listing 475 groups. The table columns are 'Name ↑' (sorted by name), 'Object Id', and 'Category'. Two entries are visible: 'ADSyncAdmins' (Object ID: 029a46f3-d2b9-4598-8dfa-f6d515dca150) and 'ADSyncBrowse' (Object ID: 0f31055c-23e2-424f-bde3-3ec49c13868a). A blue 'New group' button is located at the top left of the main content area.

Figure 2.21 – Azure AD all groups

The screenshot shows the 'New Group' page. The left sidebar has a 'Got feedback?' link. The main form fields include: 'Group type *' (Security selected), 'Group name *' (input field 'Enter the name of the group'), 'Group description' (input field 'Enter a description for the group'), 'Azure AD roles can be assigned to the group' (radio buttons 'Yes' (selected) and 'No'), and 'Membership type *' (dropdown 'Assigned'). A 'Owners' section is partially visible below these fields.

Figure 2.22 – New Group page

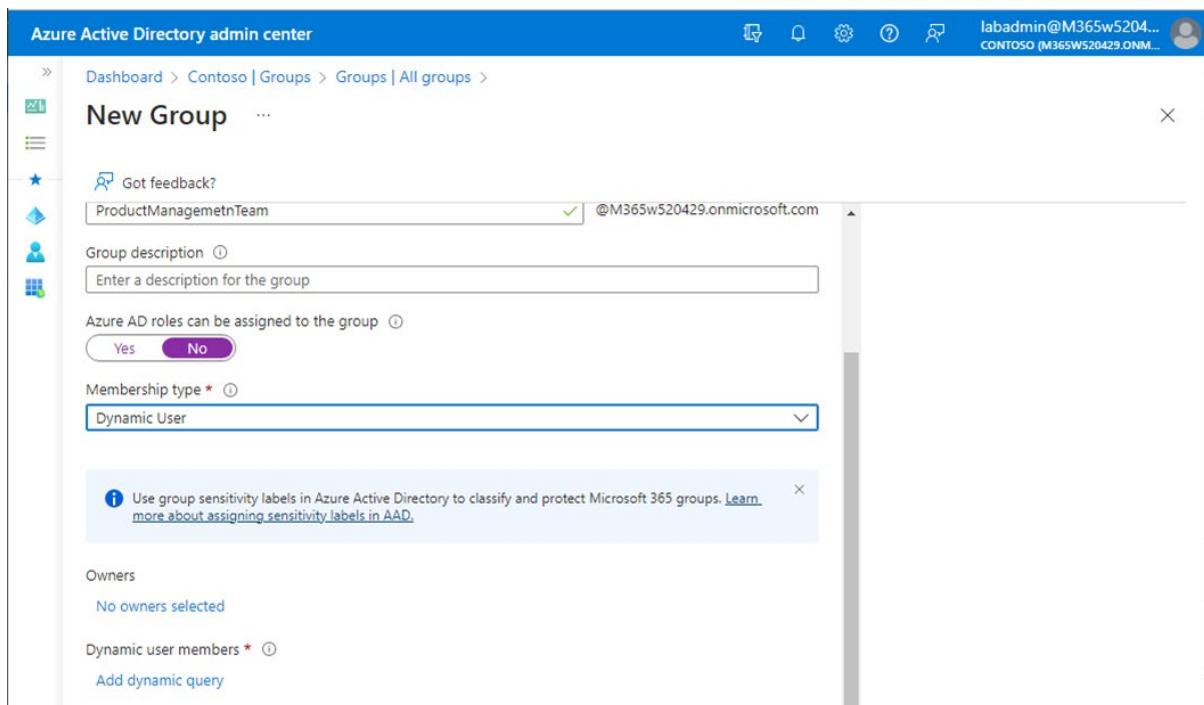


Figure 2.23 – Creating a new dynamic group

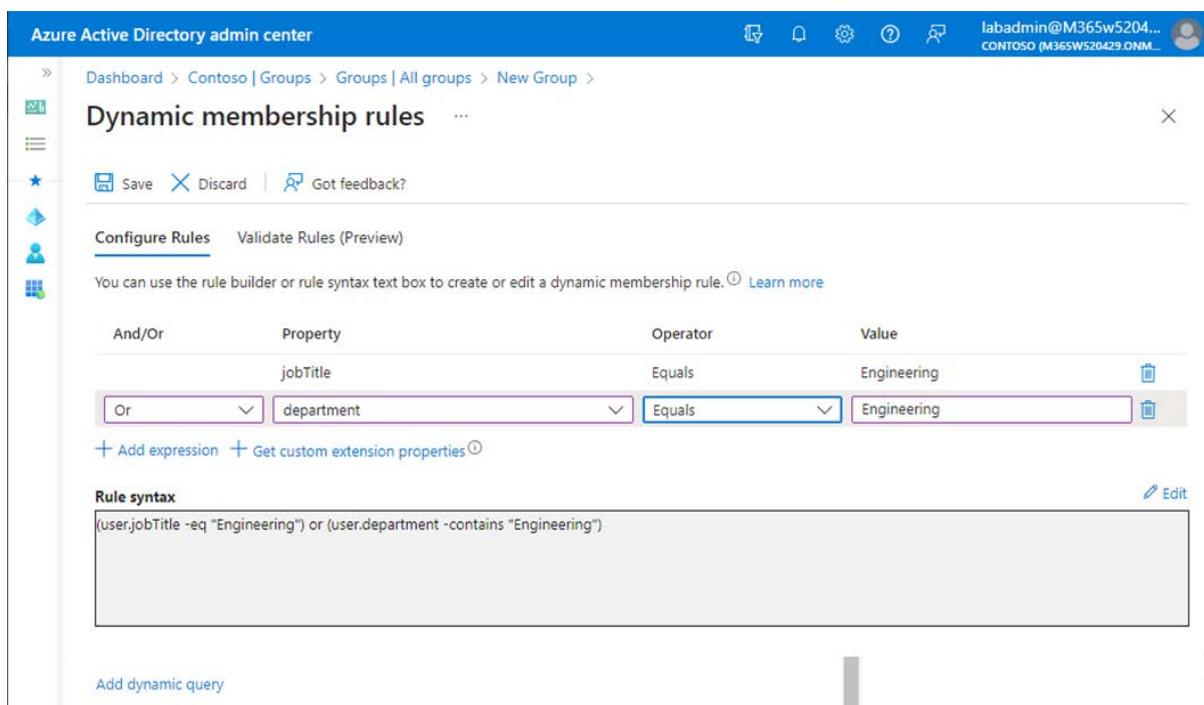


Figure 2.24 – Creating a dynamic membership rule

The screenshot shows the 'Dynamic membership rules' page in the Azure Active Directory admin center. At the top, there's a navigation bar with 'Dashboard > Contoso | Groups > Groups | All groups > New Group > Dynamic membership rules'. Below the navigation is a toolbar with 'Save', 'Discard', and 'Got feedback?' buttons. A sidebar on the left has icons for Home, Groups, Users, and Applications. The main area is titled 'Dynamic membership rules' with a 'Configure Rules' tab selected and a 'Validate Rules (Preview)' tab highlighted. Under 'Rule syntax', the expression '(user.jobTitle -eq "Engineering") or (user.department -eq "Engineering")' is shown. Below this, a note says 'Add users to validate against this rule.' followed by 'Learn more'. There are 'Add users' and 'Validate' buttons. A status bar at the bottom shows 'In group' (green checkmark), 'Not in group' (red X), and 'Unknown' (grey question mark). A table lists two users: Aamir E Cupp (AE) and Abaqael R Rauch (AR). The table has columns 'Name' and 'Status'. AE is marked as 'Not in group' (red X) and AR is marked as 'In group' (green checkmark).

Figure 2.25 – Validating the dynamic membership rule

The screenshot shows the 'Community Leadership | Properties' page in the Azure Active Directory admin center. The navigation bar is identical to Figure 2.25. The main area is titled 'Community Leadership | Properties' with a 'Group' icon. On the left, a sidebar under 'Manage' has 'Properties' selected, along with other options like 'Members', 'Owners', 'Roles and administrators', etc. The properties section includes fields for 'Group name' (Community Leadership), 'Group description' (This is the primary group for the Community Leadership Team), 'Group type' (Microsoft 365), 'Membership type' (Assigned), 'Object Id' (960f4582-c2dc-480e-9506-74e1553806b3), 'Azure AD roles can be assigned to the group' (Yes/No), and 'Group writeback state' (No writeback).

Figure 2.26 – Editing a group

The screenshot shows the Microsoft Entra admin center interface. The left sidebar includes sections for Favorites, Azure Active Directory (Overview, Users, Groups, Learn & support), and other services like Audit logs, Sign-in logs, and Diagnose and solve problems. The main content area is titled "Users" and displays a list of users with columns for Display name, User principal name, and User type. There are four users listed: Aaron Guilmette (Member), Alan Nicholls (Member), Brian Smith (Member), and Yura Lee (Member). A search bar and filter options are also present.

Figure 2.27 – Entra admin center

The screenshot shows the Microsoft 365 admin center interface. The left sidebar includes sections for Home, Users, Teams & groups, Billing (Purchase services, Your products, Licenses, Bills & payments, Billing accounts, Payment methods, Billing notifications), Setup, and Show all. The main content area is titled "Licenses" and shows the "Subscriptions" tab selected. It displays a list of products with their available and assigned license counts. The products listed are Enterprise Mobility + Security E5 (0 available, 20/20 assigned), Microsoft Teams Exploratory (99 available, 1/100 assigned), and Office 365 E5 (0 available, 20/20 assigned).

Name	Available licenses	Assigned licenses
Enterprise Mobility + Security E5	0	20/20
Microsoft Teams Exploratory	99	1/100
Office 365 E5	0	20/20

Figure 2.28 – License details in the Microsoft 365 admin center

The screenshot shows the Microsoft 365 admin center interface. On the left, there's a navigation sidebar with icons for Home, Active users, Add a user, Multi-factor authentication, Refresh, and more. The main area is titled "Active users" and shows a list of users. A specific user, "Karen Berg", is selected. Her profile picture, name, and email (karenb@M365w520429.OnMicrosoft.com) are displayed. Below her profile, there are options to Reset password, Block sign-in, or Delete user. A "Change photo" link is also present. Under "Office 365 E5", it says "0 of 20 licenses available". On the right, there's a section titled "Apps (63)" with a dropdown menu set to "Office 365 E5". It lists several apps assigned to this license: Common Data Service (Office 365 E5), Common Data Service for Teams (Office 365 E5), and Customer Lockbox. A "Save changes" button is at the bottom.

Figure 2.29 – User license management

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes "Microsoft Azure", a search bar, and user information (labadmin@M365w5204... and CONTOSO (M365WS20429.ON...)). The main area shows the "Licenses | All products" page for Contoso - Azure Active Directory. On the left, there's a sidebar with "Overview", "Diagnose and solve problems", "Manage" (which is expanded to show "Licensed features", "All products", and "Self-service sign up products"), and "Try / Buy", "Assign", "Bills", "Columns", and "Got feedback?" buttons. The "All products" section displays a table of available licenses:

Name	Total	Assigned	Available	Expiring soon
Enterprise Mobility + Security E5	20	20	0	0
Microsoft Teams Explorer	100	1	99	0
Office 365 E5	20	20	0	0

Figure 2.30 – Assign selected licenses to a group

The screenshot shows the Microsoft Azure 'Assign license' interface. At the top, there's a navigation bar with 'Microsoft Azure', a search bar, and user information ('labadmin@M365w5204...'). Below the navigation is a breadcrumb trail: 'Home > Contoso | Licenses > Licenses | All products > Assign license'. A 'Got feedback?' link is also present.

The main area is titled 'Assignment options' and contains two sections:

- Enterprise Mobility + Security E5**:
 - Azure Active Directory Premium P1: Off → On
 - Azure Active Directory Premium P2: Off → On
 - Azure Information Protection Premium P1: Off → On
 - Azure Information Protection Premium P2: Off → On
 - Azure Rights Management: Off → On
 - Microsoft Azure Multi-Factor Authentication: Off → On
 - Microsoft Defender for Cloud Apps: Off → On
 - Microsoft Defender for Identity: Off → On
 - Microsoft Intune Plan 1: Off → On
- Office 365 E5**:
 - Review + assign
 - < Previous
 - Next : Review + assign >

Figure 2.31 – Configuring assignment options

The screenshot shows the Microsoft 365 admin center 'Active users' page. The top navigation bar includes 'Microsoft 365 admin center', a search bar, and a 'Dark mode' toggle. The breadcrumb trail shows 'Home > Active users'. The main title is 'Active users'.

The page features a toolbar with actions like 'Add a user', 'User templates', 'Add multiple users', 'Multi-factor authentication', and a 'Filter' button. A search bar is also present.

The user list table has columns: 'Display name ↑', 'Username', 'Sync status', and 'Licenses'. One user is listed:

Display name ↑	Username	Sync status	Licenses
Aamir B Doss	Aamir.B.Doss@m365demolabs.com	Unlicensed	

Figure 2.32 – Active users page

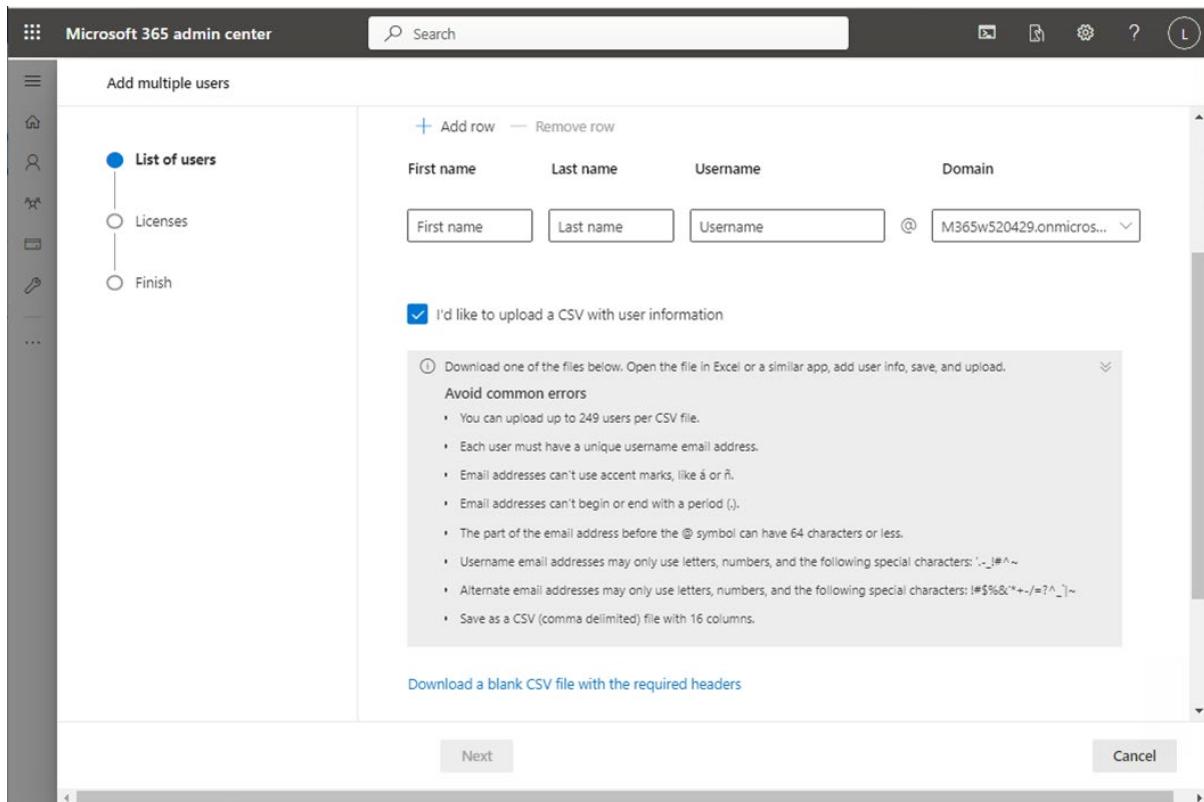


Figure 2.33 – Configuring the bulk user upload

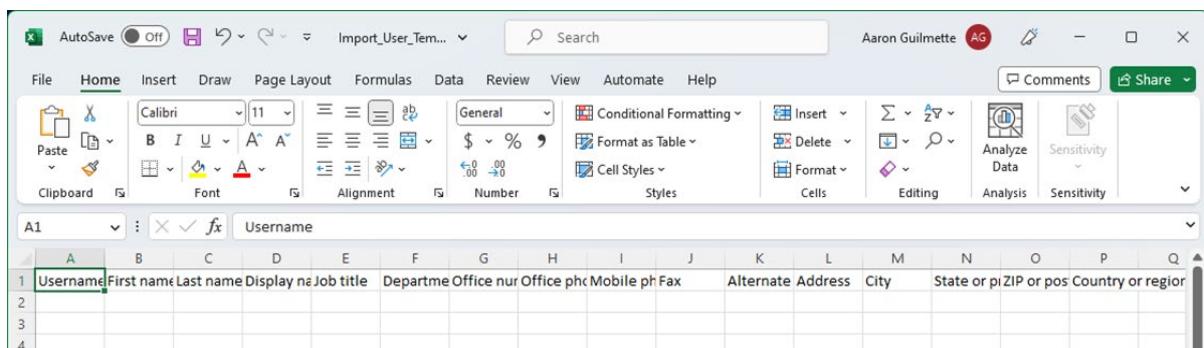


Figure 2.34 – Microsoft 365 admin center bulk user template

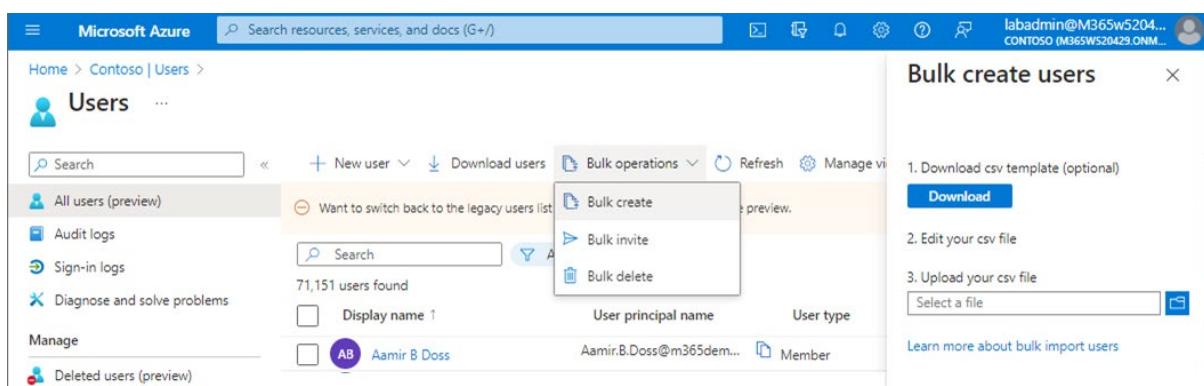


Figure 2.35 – Bulk operations menu in the Azure AD portal

A	B	C	D
1	version:v1.0		
2	Name [displayName] Required	User principal name [userPrincipalName] Required	Initial password [passwordProfile] Required
3	Example: Chris Green	chris@contoso.com	Block sign in (Yes/No) [accountEnabled] Required
4		myPassword1234	No
5			
6			

Figure 2.36 – Azure AD bulk user create template

DisplayName	UserPrincipalName	Department
Terrianne E Briscoe	Terrianne.E.Briscoe@m365demolabs.com	Project Management
Micky L Gillette	Micky.L.Gillette@m365demolabs.com	Project Management
Gordie E Laughlin	Gordie.E.Laughlin@m365demolabs.com	Project Management
Nealson D Christianson	Nealson.D.Christianson@m365demolabs.com	Project Management
Jude W Chavez	Jude.W.Chavez@m365demolabs.com	Project Management
Florie N Church	Florie.N.Church@m365demolabs.com	Project Management
Darelle A Hite	Darelle.A.Hite@m365demolabs.com	Project Management
Liliane N Bourgeois	Liliane.N.Bourgeois@m365demolabs.com	Project Management
Jean-Pierre Y Sawyers	Jean-Pierre.Y.Sawyers@m365demolabs.com	Project Management
Monica R Conyers	Monica.R.Conyers@m365demolabs.com	Project Management

Figure 2.37 – Get-MsolvUser cmdlet

DisplayName	UserPrincipalName	Department
Terrianne E Briscoe	Terrianne.E.Briscoe@m365demolabs.com	Project Management
Micky L Gillette	Micky.L.Gillette@m365demolabs.com	Project Management
Gordie E Laughlin	Gordie.E.Laughlin@m365demolabs.com	Project Management
Nealson D Christianson	Nealson.D.Christianson@m365demolabs.com	Project Management
Jude W Chavez	Jude.W.Chavez@m365demolabs.com	Project Management
Florie N Church	Florie.N.Church@m365demolabs.com	Project Management
Darelle A Hite	Darelle.A.Hite@m365demolabs.com	Project Management
Liliane N Bourgeois	Liliane.N.Bourgeois@m365demolabs.com	Project Management
Jean-Pierre Y Sawyers	Jean-Pierre.Y.Sawyers@m365demolabs.com	Project Management
Monica R Conyers	Monica.R.Conyers@m365demolabs.com	Project Management

Figure 2.38 – Get-AzureADUser cmdlet

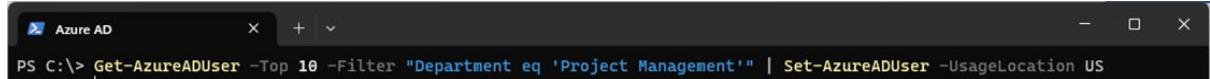
DisplayName	UserPrincipalName	Department
Terrianne E Briscoe	Terrianne.E.Briscoe@m365demolabs.com	Project Management
Micky L Gillette	Micky.L.Gillette@m365demolabs.com	Project Management
Gordie E Laughlin	Gordie.E.Laughlin@m365demolabs.com	Project Management
Nealson D Christianson	Nealson.D.Christianson@m365demolabs.com	Project Management
Jude W Chavez	Jude.W.Chavez@m365demolabs.com	Project Management
Florie N Church	Florie.N.Church@m365demolabs.com	Project Management
Darelle A Hite	Darelle.A.Hite@m365demolabs.com	Project Management
Liliane N Bourgeois	Liliane.N.Bourgeois@m365demolabs.com	Project Management
Jean-Pierre Y Sawyers	Jean-Pierre.Y.Sawyers@m365demolabs.com	Project Management
Monica R Conyers	Monica.R.Conyers@m365demolabs.com	Project Management

Figure 2.39 – Get-MgUser cmdlet



```
PS C:\> Get-MsolUser -MaxResults 10 -Department "Project Management" | Set-MsolUser -UsageLocation US
```

Figure 2.40 – Updating the UsageLocation with Set-MsolvUser



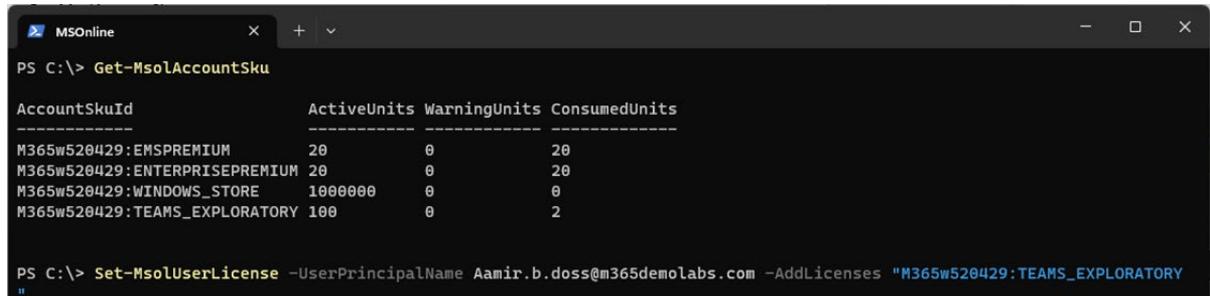
```
PS C:\> Get-AzureADUser -Top 10 -Filter "Department eq 'Project Management'" | Set-AzureADUser -UsageLocation US
```

Figure 2.41 – Updating the UsageLocation with Set-AzureADUser



```
PS C:\> Get-MgUser -Filter "Department eq 'Project Management'" -Top 5 -ConsistencyLevel Eventual -Property * | Foreach { Update-MgUser -UserId $_.id -UsageLocation US }
```

Figure 2.42 – Updating the UsageLocation with Update-MgUser

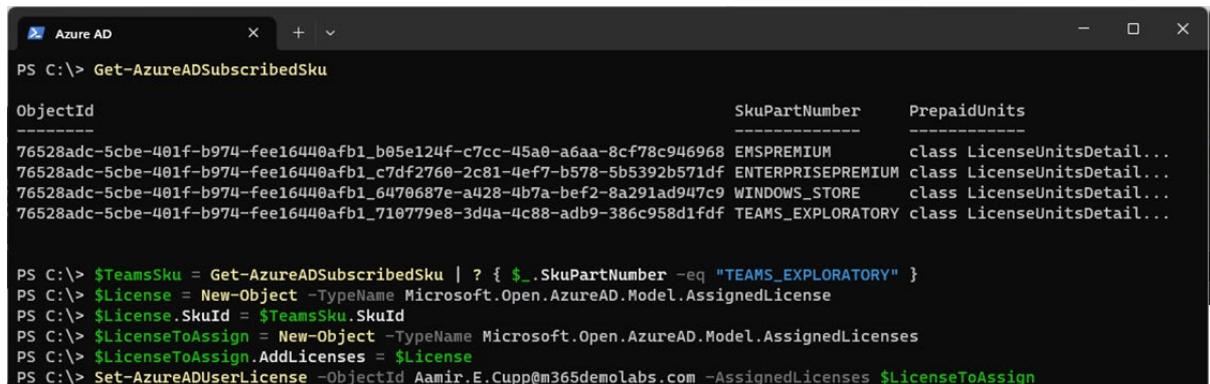


```
PS C:\> Get-MsolAccountSku

AccountSkuId          ActiveUnits WarningUnits ConsumedUnits
-----              -----
M365w520429:EMSPREMIUM    20        0            20
M365w520429:ENTERPRISEPREMIUM 20        0            20
M365w520429:WINDOWS_STORE 1000000    0            0
M365w520429:TEAMS_EXPLORATORY 100        0            2

PS C:\> Set-MsolUserLicense -UserPrincipalName Aamir.b.doss@m365demolabs.com -AddLicenses "M365w520429:TEAMS_EXPLORATORY"
```

Figure 2.43 – Adding a license to a user with the MSOnline module

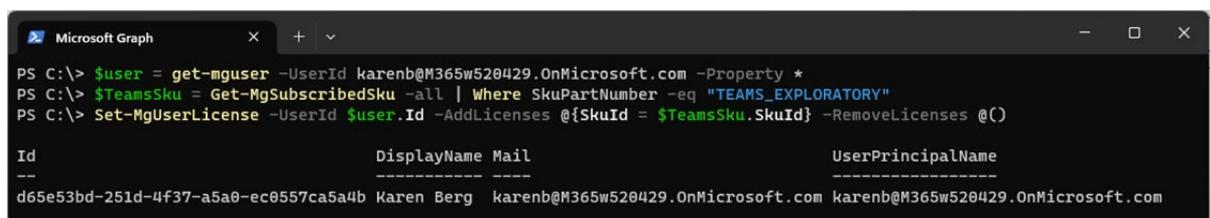


```
PS C:\> Get-AzureADSubscribedSku

ObjectId                           SkuPartNumber     PrepaidUnits
-----                           -----
76528adc-5cbe-401f-b974-fee16440afb1_b05e124f-c7cc-45a0-a6aa-8cf78c946968 EMSPREMIUM      class LicenseUnitsDetail...
76528adc-5cbe-401f-b974-fee16440afb1_c7df2760-2c81-4ef7-b578-5b5392b571df ENTERPRISEPREMIUM class LicenseUnitsDetail...
76528adc-5cbe-401f-b974-fee16440afb1_6470687e-a428-4b7a-bef2-8a291ad947c9 WINDOWS_STORE   class LicenseUnitsDetail...
76528adc-5cbe-401f-b974-fee16440afb1_710779e8-3d4a-4c88-adb9-386c958d1fdf TEAMS_EXPLORATORY class LicenseUnitsDetail...

PS C:\> $TeamSku = Get-AzureADSubscribedSku | ? { $_.SkuPartNumber -eq "TEAMS_EXPLORATORY" }
PS C:\> $License = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicense
PS C:\> $License.SkuId = $TeamSku.SkuId
PS C:\> $LicenseToAssign = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicenses
PS C:\> $LicenseToAssign.AddLicenses = $License
PS C:\> Set-AzureADUserLicense -ObjectId Aamir.E.Cupp@m365demolabs.com -AssignedLicenses $LicenseToAssign
```

Figure 2.44 – Adding a license with the Set-AzureADUserLicense cmdlet



```
PS C:\> $user = get-mguser -UserId karenb@M365w520429.OnMicrosoft.com -Property *
PS C:\> $TeamSku = Get-MgSubscribedSku -all | Where SkuPartNumber -eq "TEAMS_EXPLORATORY"
PS C:\> Set-MgUserLicense -UserId $user.Id -AddLicenses @{$skuId = $TeamSku.SkuId} -RemoveLicenses @()

Id           DisplayName Mail           UserPrincipalName
--           -----
d65e53bd-251d-4f37-a5a0-ec0557ca5a4b Karen Berg  karenb@M365w520429.OnMicrosoft.com karenb@M365w520429.OnMicrosoft.com
```

Figure 2.45 – Adding a license with the Set-MgUserLicense cmdlet

A	B	C	D	E	F	G	H	I	J	K
UserPrincipalName	FirstName	LastName	DisplayName	JobTitle	Department	UsageLocation				
robert.smith@m365demolabs.com	Robert	Smith	Robert Smith	Pre-sales Specialist	Sales	US				
grant.roberts@m365demolabs.com	Grant	Roberts	Grant Roberts	HR Generalist	Human Resources	US				

Figure 2.46 – Bulk user template

```

PS C:\> $Users = Import-Csv -Path C:\temp\ImportUsers.csv
PS C:\> Foreach ($User in $Users) { New-MsolUser -UserPrincipalName $User.UserPrincipalName -FirstName $User.FirstName -LastName $User.LastName -DisplayName $User.DisplayName -Title $User.JobTitle -Department $User.Department -UsageLocation $User.UsageLocation -Country US }

Password UserPrincipalName          DisplayName     isLicensed
----- -----
Kad74447 robert.smith@m365demolabs.com Robert Smith False
Vac19974 grant.roberts@m365demolabs.com Grant Roberts False

```

Figure 2.47 – Bulk creating users with New-MsolUser

```

PS C:\> $Users = Import-Csv C:\temp\ImportUsers.csv
PS C:\> $PasswordProfile = New-Object -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile
PS C:\> $PasswordProfile.Password = "P@ssw0rd123"
PS C:\> Foreach ($User in $Users) { New-AzureADUser -UserPrincipalName $User.UserPrincipalName -GivenName $User.FirstName -Surname $User.LastName -DisplayName $User.DisplayName -JobTitle $User.JobTitle -Department $User.Department -UsageLocation $User.UsageLocation -Country $User.Country -AccountEnabled $True -MailNickname $User.UserPrincipalName.Split("@")[-1] -PasswordProfile $PasswordProfile }

ObjectId          DisplayName   UserPrincipalName      UserType
---- -----
fb2754d2-605d-4e0f-bb0a-18d9c8912bf9 Robert Smith  robert.smith@m365demolabs.com Member
7848058c-df77-4e46-a4b0-b60759164fbf Grant Roberts  grant.roberts@m365demolabs.com Member

```

Figure 2.48 – Creating new users with New-AzureADUser

```

PS C:\> $Users = Import-Csv C:\Temp\ImportUsers.csv
PS C:\> $PasswordProfile = @{ Password = "P@ssw0rd123" }
PS C:\> Foreach ($User in $Users) { New-MgUser -UserPrincipalName $User.UserPrincipalName -GivenName $User.FirstName -Surname $User.LastName -DisplayName $User.DisplayName -JobTitle $User.JobTitle -Department $User.Department -UsageLocation $User.UsageLocation -Country $User.UsageLocation -AccountEnabled -MailNickname $User.UserPrincipalName.Split("@")[-1] -PasswordProfile $PasswordProfile }

Id          DisplayName   Mail UserPrincipalName      UserType
-- -----
fb0618c1-6972-4f2d-bdee-5e25eafec28a Robert Smith  robert.smith@m365demolabs.com Member
f73211cd-446d-4e49-9c60-685164ad4066 Grant Roberts  grant.roberts@m365demolabs.com Member

```

Figure 2.49 – Creating new users with the New-MgUser cmdlet

DASHBOARD > CHAPTER 2

Managing Users and Groups

Summary

In this chapter, you learned some of the basics of administering objects on the Microsoft 365 platform, whether those objects were on-premises or cloud only. Managing identity is a large part of the Microsoft 365 administration experience, so it's important to have a firm grasp on the variety of tools and methods for provisioning, licensing, and updating objects.

In the next chapter, you'll learn how to manage roles in Microsoft 365.

Chapter Review Questions

The Microsoft 365 Administrator MS-102 Exam Guide
by Aaron Guilmette

Select Quiz

Quiz 1

[SHOW QUIZ DETAILS](#) ▾

START

Figure 2.50 – Chapter Review Questions for Chapter 2

Chapter 3: Managing Roles in Microsoft 365

New Group

Got feedback?

Group type * ①

Security

Group name * ①

Service Desk Team

Group description ①

Enter a description for the group

Azure AD roles can be assigned to the group ①

Yes No

Membership type * ①

Assigned

Owners

No owners selected

Members

Create

Figure 3.1 – Configuring the `isAssignableToRole` property on a new group

The screenshot shows the Microsoft 365 Admin Center homepage. The left sidebar has a 'Home' icon and the text 'Home'. Below it are sections for 'Users', 'Teams & groups', and 'Roles'. Under 'Roles', 'Role assignments' is highlighted. Other items in this section include 'Administrative units', 'Resources', and 'Billing'. The main content area has a search bar at the top. It displays '4 global admins' and a warning about having too many global admins. It also shows a chart titled 'Assigned admin roles' with one entry: 'Global Admins' (represented by a purple bar). There are also 'What's new?' and 'Dark mode' buttons.

Figure 3.2 – Role assignments

The screenshot shows the Microsoft 365 admin center interface. The top navigation bar includes links for 'Role assignments', 'Micro...', and a search bar. Below the navigation is a header for 'Microsoft 365 admin center' with a 'Search' field and various icons. The main content area is titled 'Role assignments' and has tabs for 'Azure AD', 'Exchange', 'Intune', and 'Billing'. A sub-section for 'Azure AD' provides information about assigning built-in roles to users. It includes a link to 'Learn more about roles in Microsoft 365'. Below this is a table with role details:

<input type="checkbox"/>	Name ↑	<input type="checkbox"/> Description
<input type="checkbox"/>	Exchange Administrator	Full access to Exchange Online, creates and manages groups, manages service requests, and monitors service health.
<input type="checkbox"/>	Global Administrator	Has unlimited access to all management features and most data in Azure Active Directory.
<input type="checkbox"/>	Global Reader	Can view all administrative features and settings in all admin centers.
<input type="checkbox"/>	Helpdesk Administrator	Resets passwords and re-authenticates for all non-admins and some admin roles, manages service requests.

On the right side of the table, there are two buttons: a teal 'Help & support' button and a dark grey 'Give feedback' button.

Figure 3.3 – Role assignments page

This screenshot shows the 'Role assignments' page for the 'Exchange Administrator' role. The left sidebar has a tree view with 'Home', 'Users', 'Teams & groups', 'Roles' (selected), 'Resources', 'Billing', 'Support', 'Settings', 'Setup', 'Reports', 'Health', and 'Admin centers'. The main content area is titled 'Exchange Administrator' and includes a 'Run As' button. Below it are tabs for 'General', 'Assigned' (which is selected), and 'Permissions'. A link to 'Learn more about assigning admin roles' is present. Under the 'Assigned' tab, there are buttons for 'Add users' and 'Add groups'. A table lists the assigned role:

<input type="checkbox"/>	Name ↑	<input type="checkbox"/> Admin name	Last sign-in	Scope <i>(i)</i>
<input checked="" type="checkbox"/>	Exchange Administrator			
<input type="checkbox"/>	Global Administrator			
<input type="checkbox"/>	Global Reader			
<input type="checkbox"/>	Helpdesk Administrator			

A message at the bottom states 'Nobody has been assigned to this role yet.' and 'Select 'Add users' or 'Add groups' to get started.'

Figure 3.4 – Making role assignments

The screenshot shows the Microsoft 365 Defender interface. On the left, there's a navigation sidebar with sections like Cloud apps, Reports, Audit, Health, Permissions, Settings, More resources, and Customize navigation. The main content area is titled 'Permissions & roles > Microsoft 365 Defender'. It includes a 'Learn more' link and a 'Workload settings' button. Below this is a 'Permissions and roles' section with a sub-section titled 'Get started with roles in Microsoft 365 Defender'. A 'Create your first role' button is visible. The central part of the screen displays a table for managing roles, with columns for Role name, Description, Data source, Last upd..., and Assigned... (with a value of 0 items). There are buttons for '+ Create custom role', 'Edit', and 'Delete roles'.

Figure 3.5 – Microsoft 365 Defender permissions

This screenshot shows the 'Create your first role' wizard. The left sidebar has sections like Partners and APIs, Evaluation & tutorials, Configuration management, Email & collaboration, Investigations, Explorer, Review, Campaigns, Exchange message trace, Attack simulation training, Policies & rules, Cloud apps, Cloud discovery, Cloud app catalog, OAuth apps, and Files. The main area is titled 'Set up the basics'. It has a 'Basics' tab selected, which contains fields for 'Role name *' (set to 'Defender Security Reader') and 'Description' (a placeholder text area). There are also 'Permissions' and 'Assignments' tabs. At the bottom are 'Next' and 'Cancel' buttons.

Figure 3.6 – Creating a new custom role

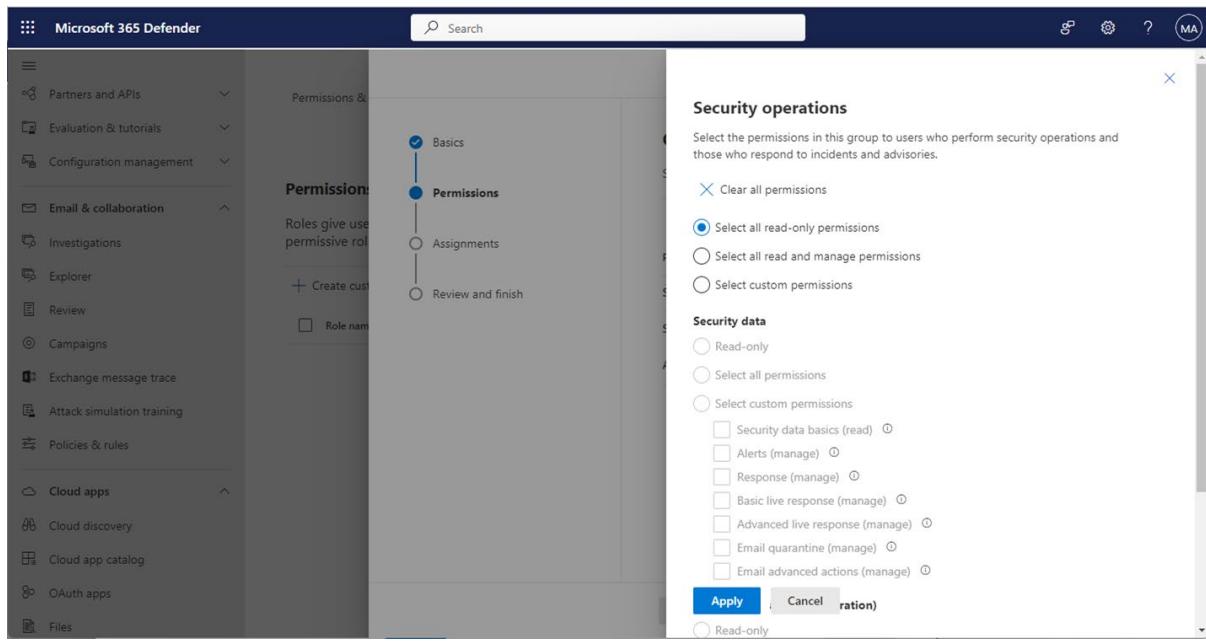


Figure 3.7 – Selecting permissions

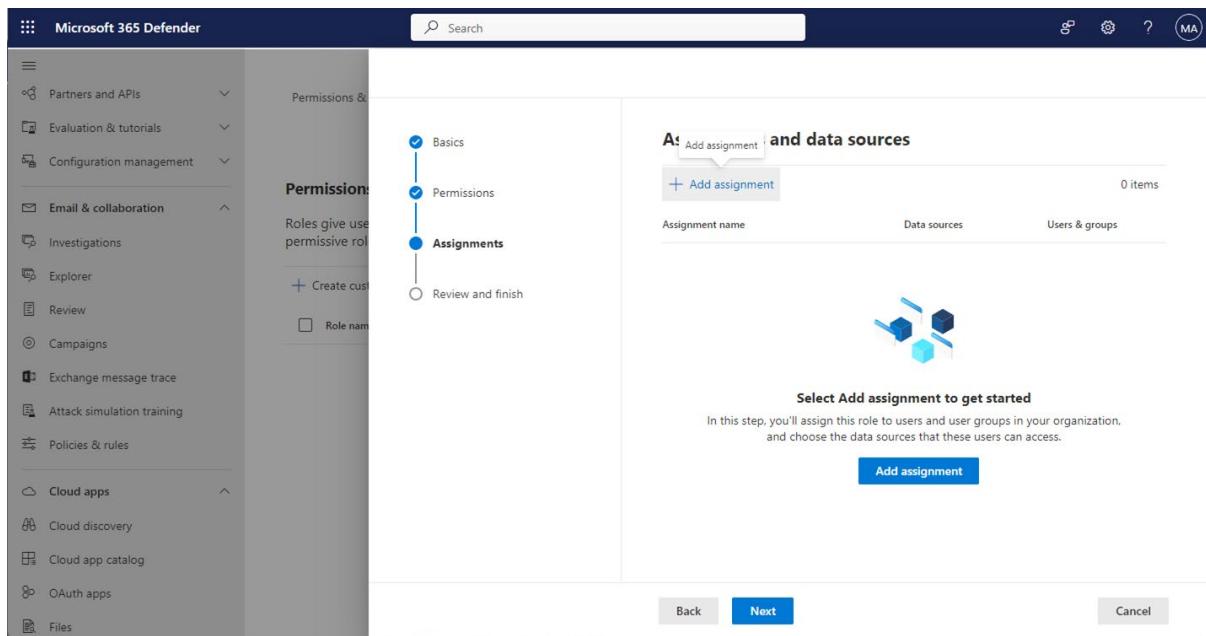


Figure 3.8 – Adding user and data assignments

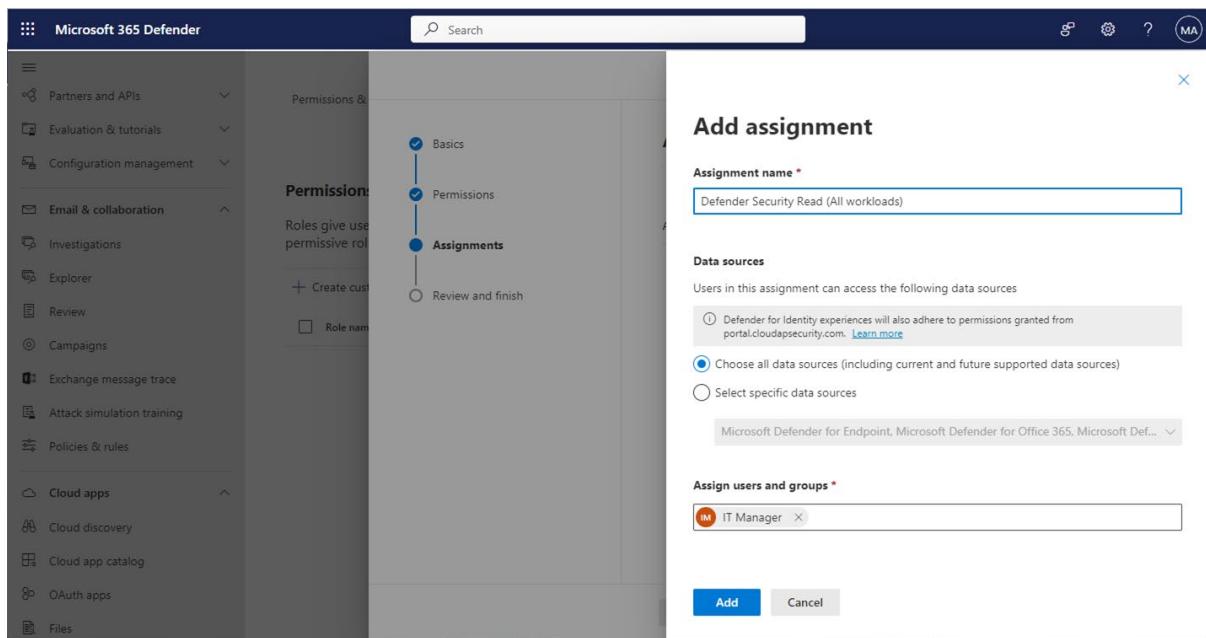


Figure 3.9 – Selecting assignment options

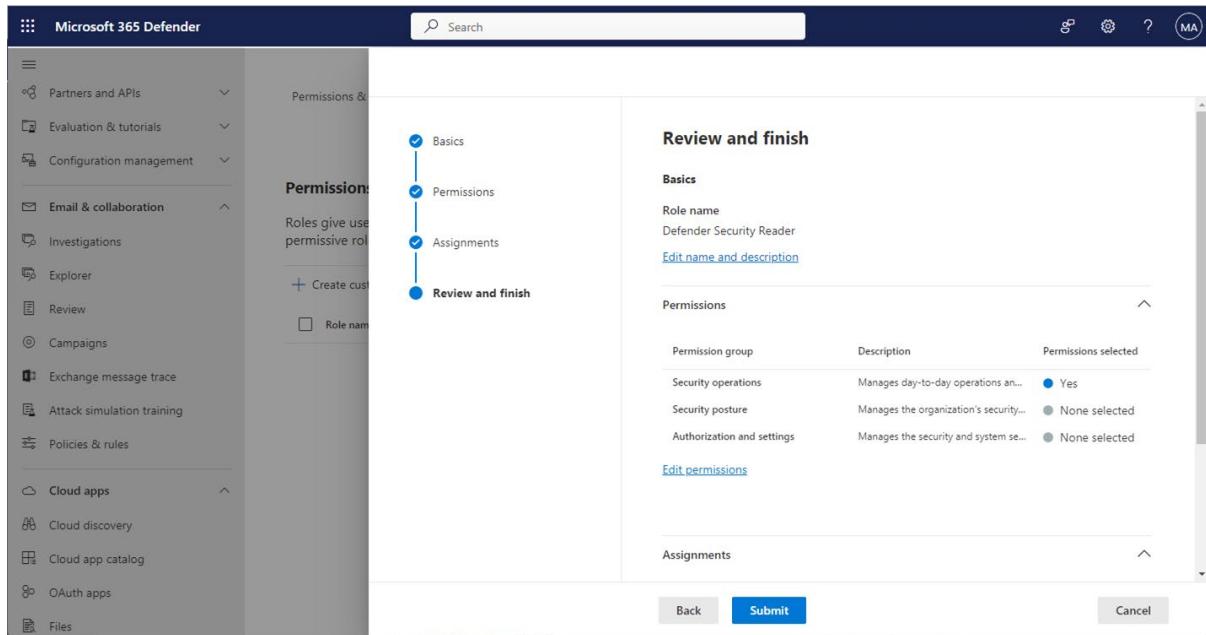


Figure 3.10 – Confirming configuration

The screenshot shows the Microsoft Purview admin center interface. The left sidebar includes sections for Home, Compliance Manager, Data classification, Data connectors, Alerts, Policies, Roles & scopes (which is expanded to show Permissions, Adaptive scopes, and Trials), Solutions (Catalog, Audit, Content search, Communication compliance), and a bottom section for Solutions (Catalog, Audit, Content search, Communication compliance). The main content area is titled "Permissions > Azure AD roles". It displays a list of Azure AD roles with columns for Admin role, Users, and Description. The roles listed are Global administrator, Compliance data administrator, Compliance administrator, Security operator, Security reader, Security administrator, Global reader, and Attack simulation administrator. A note at the top states: "These Azure AD roles are used to perform various tasks in the compliance portal. Select a role for more detail and to view current members. You can manage these roles from [Azure AD](#). To manage role groups for performing solution-specific tasks, go to [Role groups for Microsoft Purview solutions](#)". A footer indicates there are 9 items.

Admin role	Users	Description
Global administrator	4	Can manage all aspects of Azure AD and Microsoft services that use Azure A...
Compliance data administrator	0	Creates and manages compliance content.
Compliance administrator	0	Can read and manage compliance configuration and reports in Azure AD an...
Security operator	0	Creates and manages security events.
Security reader	0	Can read security information and reports in Azure AD and Office 365.
Security administrator	0	Security Administrator allows ability to read and manage security configurat...
Global reader	0	Can read everything that a global admin can read but not update anything.
Attack simulation administrator	0	Can create and manage all aspects of attack simulation campaigns.

Figure 3.11 – Viewing the Azure AD roles in the Microsoft 365 admin center

The screenshot shows the Microsoft Purview admin center interface. The left sidebar includes sections for Home, Compliance Manager, Data classification, Data connectors, Alerts, Policies, Roles & scopes (which is expanded to show Permissions, Adaptive scopes, and Trials), Solutions (Catalog, Audit, Content search, Communication compliance), and a bottom section for Solutions (Catalog, Audit, Content search, Communication compliance). The main content area is titled "Permissions > Role groups for Microsoft Purview solutions". It displays a list of role groups with columns for Name, Type, Description, and Last modified. The role groups listed are Attack Simulator Administrators, Attack Simulator Payload Authors, Organization Management, Security Administrator, Billing Administrator, eDiscovery Manager, and Compliance Administrator. A note at the top states: "Admin roles give users permission to view data and complete tasks in the Microsoft Purview compliance portal. Give users only the access they need by assigning the least-permissive role. [Learn more about role groups](#)". A footer indicates there are 53 items.

Name	Type	Description	Last modified
Attack Simulator Administrators	Built-in	-	-
Attack Simulator Payload Authors	Built-in	-	-
Organization Management	Built-in	-	-
Security Administrator	Built-in	-	-
Billing Administrator	Built-in	-	-
eDiscovery Manager	Built-in	-	-
Compliance Administrator	Built-in	-	-

Figure 3.12 – Microsoft Purview solutions roles

The screenshot shows the Microsoft 365 admin center interface. The left sidebar has a navigation menu with sections like Devices, Teams & groups, Roles, Resources, Billing, Support, Settings, Setup, Reports, and Health. Under Admin centers, there are Security, Compliance, Endpoint Manager, and Azure Active Directory. The main content area is titled "Azure AD" and shows a list of built-in roles. At the top of this list is "Application Administrator". A tooltip for this role states: "Full access to enterprise applications, application registrations, and application proxy settings." The list also includes "Application Developer", "Attack Payload Author", "Attack Simulation Administrator", "Attribute Assignment Administrator", "Attribute Assignment Reader", and "Attribute Definition Administrator". The "Help & support" and "Give feedback" buttons are visible in the bottom right corner of the main content area.

Figure 3.13 – Microsoft 365 workload roles

The screenshot shows the Microsoft 365 admin center interface. The left sidebar has a navigation menu with sections like Home, Users, Teams & groups, Roles, Resources, Billing, and Support. The "Administrative units" section is currently selected. The main content area is titled "Administrative units". It contains a brief description: "Units let you sub-divide your organization into any unit that you want, and then assign specific administrators that can only manage that unit. For example, you can assign the Helpdesk Administrator role to a regional support specialist, so they can manage users only in that region." Below this is a table with columns: "Unit ↑", "Description", and "Membership type". There is a "Search this list" input field and a "Refresh" button at the top of the table area. The "Dark mode" toggle is located in the top right corner.

Figure 3.14 – Administrative units page

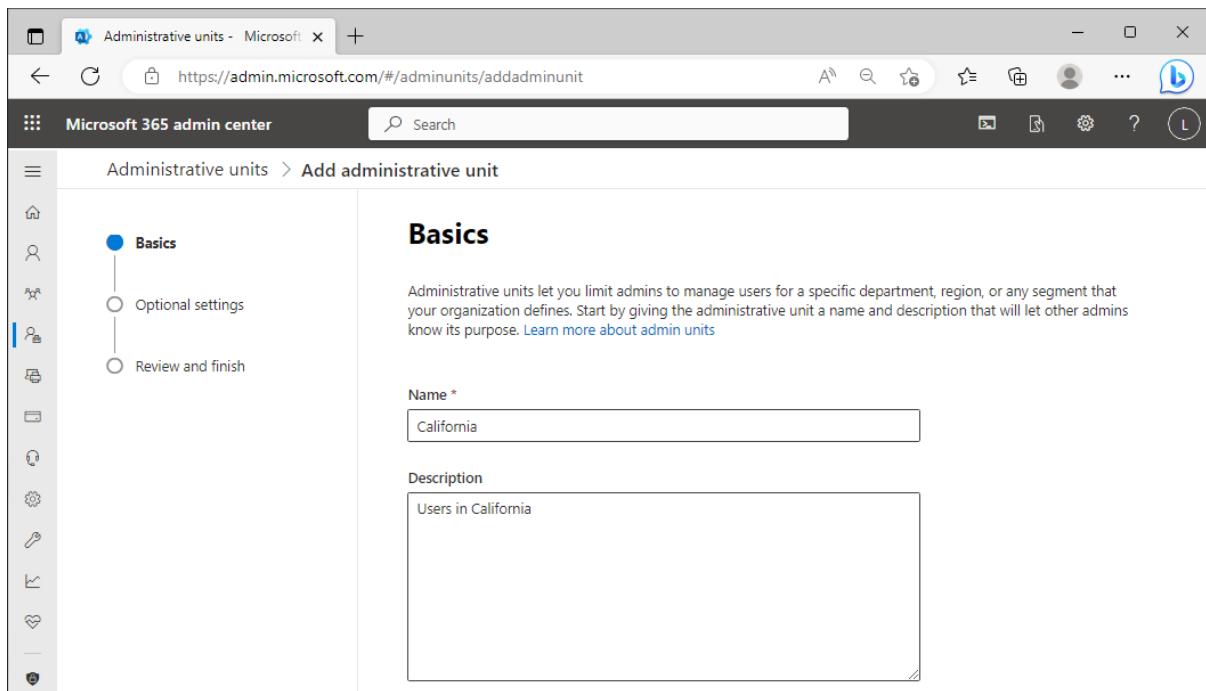


Figure 3.15 – Basics page

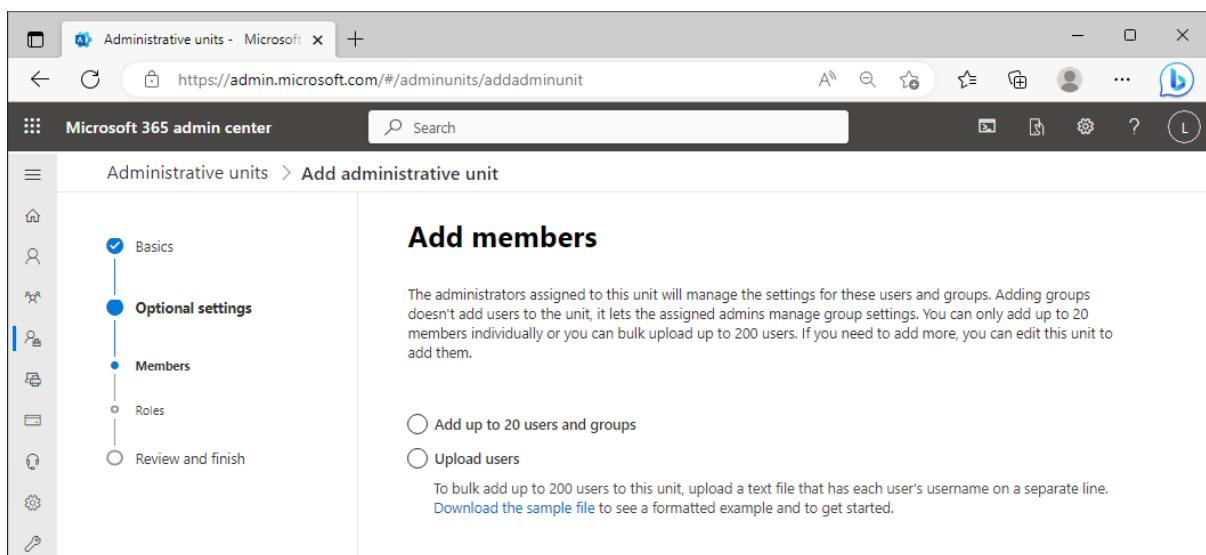


Figure 3.16 – Add members page

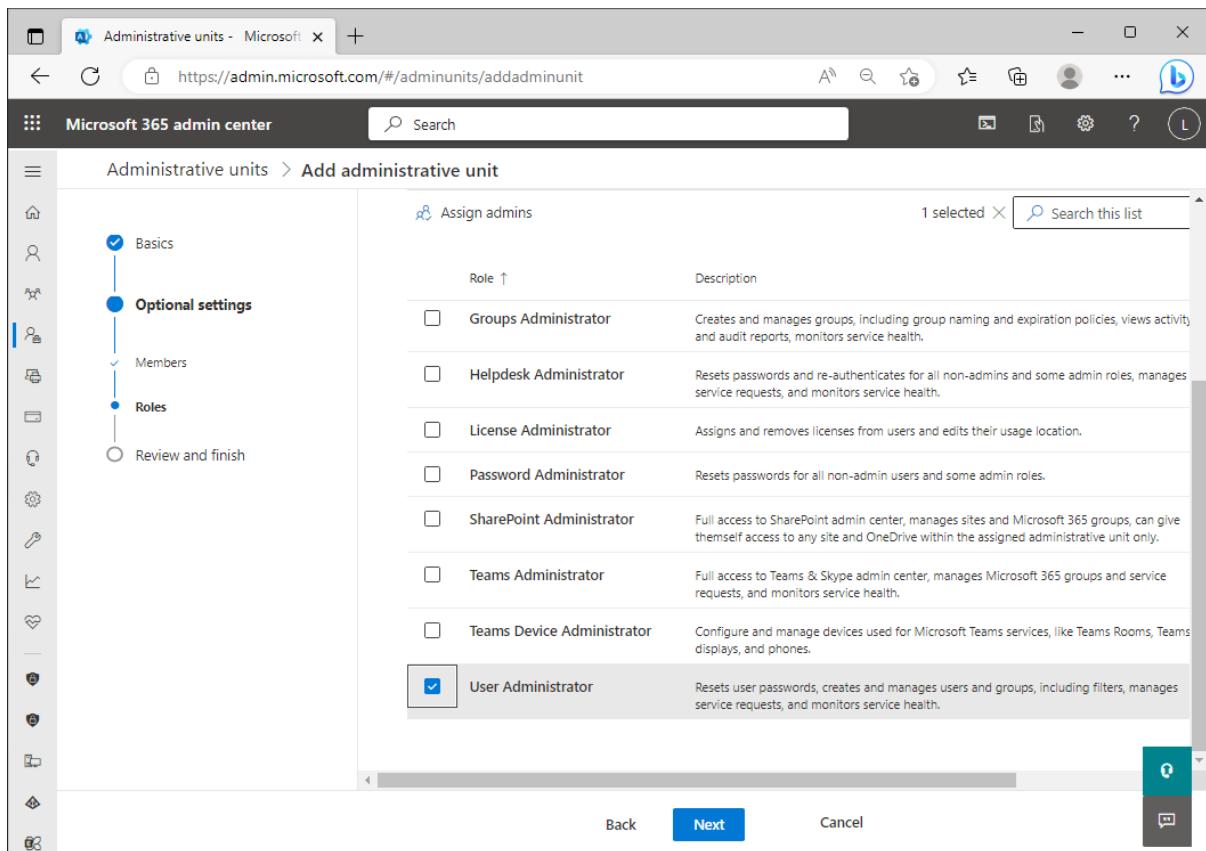


Figure 3.17 – Adding roles

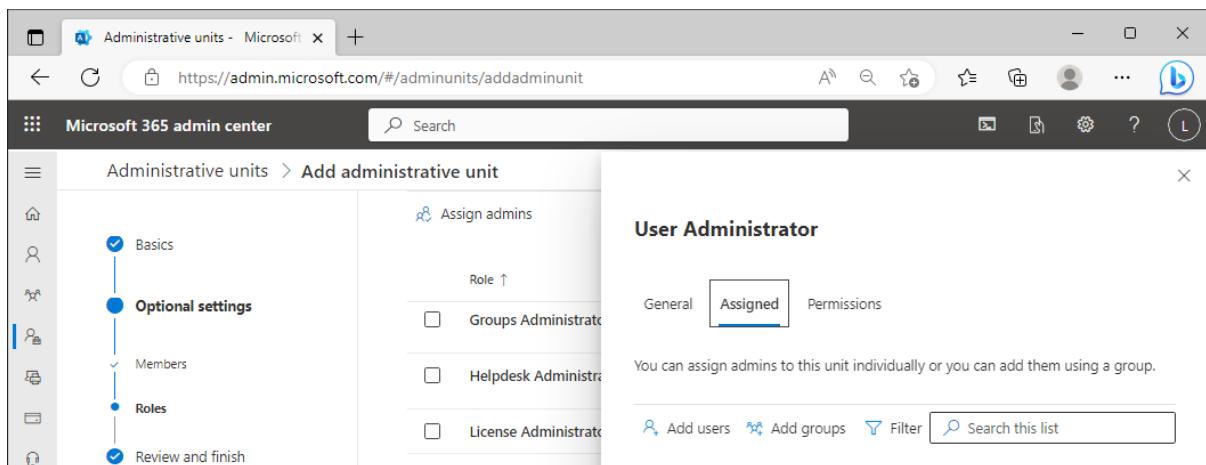


Figure 3.18 – User Administrator flyout

The screenshot shows the Microsoft 365 Admin Center interface for adding an administrative unit. The left sidebar has a 'Roles' icon selected. The main pane shows a flow: Basics, Optional settings (selected), Members, Roles, and Review and finish. On the right, under 'Assign admins', the 'User Administrator' role is listed. A green success message box says 'Abbey M Mcfall was added to this role.' Below it is a search bar and a list of users with their names, last sign-in dates, and email addresses.

Figure 3.19 – Adding users to role

The screenshot shows the Microsoft 365 Admin Center 'Administrative units' page. The left sidebar has a 'Roles' icon selected. The main pane shows the title 'Administrative units' and a brief description about what they are used for. Below is a table with columns: Unit, Description, and Membership type. One entry is visible: 'California' with the description 'Users in California' and 'Assigned' membership type.

Unit	Description	Membership type
California	Users in California	Assigned

Figure 3.20 – Viewing administrative units

The screenshot shows the Microsoft Azure Identity Governance dashboard. On the left, there's a sidebar with links like 'Lifecycle workflows', 'Access reviews', and 'Privileged Identity Management'. The 'Privileged Identity Management' section is highlighted with a red box. It contains two sub-links: 'Azure AD roles' and 'Azure resources'. The main content area has a heading 'Get started with Identity Governance' and a sub-section titled 'Control your external user lifecycle' with a circular diagram showing users and a central gear.

Figure 3.21 – Privileged Identity Management

The screenshot shows the 'Contoso | Roles' page under 'Identity Governance | Azure AD roles'. The left sidebar lists 'My roles', 'Pending requests', 'Approve requests', 'Review access', 'Manage', 'Roles' (which is selected), 'Assignments', and 'Alerts'. The main content area displays a table of Azure AD roles:

Role	Description	Active	Eligible
Application Administrator	Users with this role can create and manage all aspects ...	0	0
Application Developer	Users with this role can create application registrations...	0	0
Attack Payload Author	Can create attack payloads that an administrator can in...	0	0
Attack Simulation Administrator	Can create and manage all aspects of attack simulation...	0	0
Attribute Assignment Administrat...	Assigns attribute keys and values to Azure AD objects.	0	0
Attribute Assignment Reader	Reads attribute keys and values to Azure AD objects.	0	0
Attribute Definition Administrat...	Defines and manages the definition of security attribut...	0	0
Attribute Definition Reader	Read the definition of security attributes for the tenant.	0	0
Authentication Administrator	Can access to view, set and reset authentication metho...	0	0

Figure 3.22 – Role assignments

The screenshot shows the 'Select a member' dialog box from the Microsoft Azure portal. The URL is https://portal.azure.com/#view/Microsoft_Azure_PIMCommon/RoleAssignmentBl... . The dialog title is 'Select a member' under 'Privileged Identity Management | Azure AD roles'. It displays a search bar and a list of users: Aamir B Doss (Selected), Aamir E Cupp (Selected), and Aamir G Waldron (Selected). Below the list is a 'Selected items' section containing the same three users with 'Remove' buttons. On the left, there's a sidebar with 'Membership' and 'Setting' tabs, and sections for 'Resource' (Contoso) and 'Resource type' (Directory). Under 'Select role', 'Exchange Administrator' is selected. Under 'Scope type', 'Directory' is selected. At the bottom, it says 'Select member(s)' with 'No member selected'.

Figure 3.23 – Selecting members

The screenshot shows the 'Add assignments' configuration dialog box from the Microsoft Azure portal. The URL is https://portal.azure.com/#view/Microsoft_Azure_PIMCommon/RoleAssignmentBl... . The title is 'Add assignments' under 'Privileged Identity Management | Azure AD roles'. It has 'Membership' and 'Setting' tabs, with 'Setting' selected. Under 'Assignment type', 'Eligible' is selected (radio button checked). Below it, it says 'Maximum allowed eligible duration is permanent.' and 'Permanently eligible' is checked. There are two date pickers: 'Assignment starts' set to 03/20/2023 at 3:38:25 AM, and 'Assignment ends' set to 03/19/2024 at 3:38:25 AM.

Figure 3.24 – Configuring assignment type and eligibility duration

The screenshot shows the Microsoft Azure portal interface for Contoso. The left sidebar includes 'Quick start', 'Overview', 'Tasks' (with 'My roles', 'Pending requests', 'Approve requests', 'Review access'), 'Manage' (with 'Roles', 'Assignments', 'Alerts'), and 'Activity'. The main content area is titled 'Contoso | Assignments' under 'Privileged Identity Management | Azure AD roles'. It has tabs for 'Eligible assignments', 'Active assignments' (which is selected), and 'Expired assignments'. A search bar allows searching by member name or principal name. Below is a table listing assignments:

Name	Principal name	Type	Scope	Membership	Start time
Exchange Administrator					
Aamir B Doss	Aamir.B.Doss@m365de	User	Directory	Direct	3/20/2023, 3:17:18 AM
Aamir G Waldron	Aamir.G.Waldron@m365de	User	Directory	Direct	3/20/2023, 3:42:44 AM
Aamir E Cupp	Aamir.E.Cupp@m365de	User	Directory	Direct	3/20/2023, 3:42:42 AM
Helpdesk Administrator					
Abagail A Robertson	Abagail.A.Robertson@m365de	User	Directory	Direct	3/20/2023, 3:47:37 AM
Charles F Sparks	Charles.F.Sparks@m365de	User	Directory	Direct	3/20/2023, 3:47:40 AM

Figure 3.25 – Viewing role assignments

The screenshot shows the Microsoft Azure portal interface for Contoso, similar to Figure 3.25 but with the 'Active assignments' tab selected. The main content area is titled 'Contoso | Assignments' under 'Privileged Identity Management | Azure AD roles'. It has tabs for 'Eligible assignments', 'Active assignments' (selected), and 'Expired assignments'. A search bar allows searching by member name or principal name. Below is a table listing assignments:

Name	Principal name	Type	Scope	Membership	State
Directory Readers					
Microsoft.Azure.Syn	00000014-0000-0000-c	Service principal	Directory	Direct	Assigned
MicrosoftAzureActiv	0000001a-0000-0000-c	Service principal	Directory	Direct	Assigned
Exchange Administrator					
Aamir B Doss	Aamir.B.Doss@m365de	User	Directory	Direct	Assigned
EXO_App2	74919118-4de8-428d-e	Service principal	Directory	Direct	Assigned
Global Administrator					
labadmin	labadmin@m365w5204...	User	Directory	Direct	Assigned
Microsoft Service Ac	ms-serviceaccount@M...	User	Directory	Direct	Assigned
MOD Administrator	admin@m365w520429	User	Directory	Direct	Assigned
Hybrid Identity Administrator					
labadmin	labadmin@m365w5204...	User	Directory	Direct	Assigned

Figure 3.26 – Viewing active assignments

The screenshot shows the 'Edit alert setting' page in Microsoft Azure. The URL is https://portal.azure.com/#view/Microsoft_Azure_PIMCommon/EditAlertSettings/p... . The top navigation bar includes 'Microsoft Azure' and a search bar. The main content area is titled 'Edit alert setting' under 'Privileged Identity Management | Azure AD roles'. It features two configuration sections: 'Number of Global Administrators' (set to 3) and 'Percentage of Global Administrators' (set to 10). On the left, there's a list of alert types:

- The organization doesn't have Azure AD Premium P2
- Roles don't require multi-factor authentication for activation
- Eligible administrators aren't activating their privileged role
- Roles are being assigned outside of Privileged Identity Management
- Roles are being activated too frequently
- There are too many global administrators
- Potential stale accounts in a privileged role

Figure 3.27 – Viewing PIM Alert settings

The screenshot shows the 'Practice Resources' section for Chapter 3. The title is 'Managing Roles in Microsoft 365'. The 'Summary' section contains the following text:

In this chapter, you learned about what it means to manage Azure AD from a least-privilege perspective. Reducing the scope and privileges used to administer an environment can greatly reduce the possible impacts of administrative actions—whether they are unintentional or targeted attacks by malicious users.

The next chapter will explore authentication options and configurations in the Microsoft 365 platform.

To the right, there is a 'Chapter Review Questions' section for 'The Microsoft 365 Administrator MS-102 Exam Guide' by Aaron Guilmette. It features a 'Select Quiz' button and a 'Quiz 1' section with a 'START' button and a 'SHOW QUIZ DETAILS' dropdown.

Figure 3.28 – Chapter Review Questions for Chapter 3

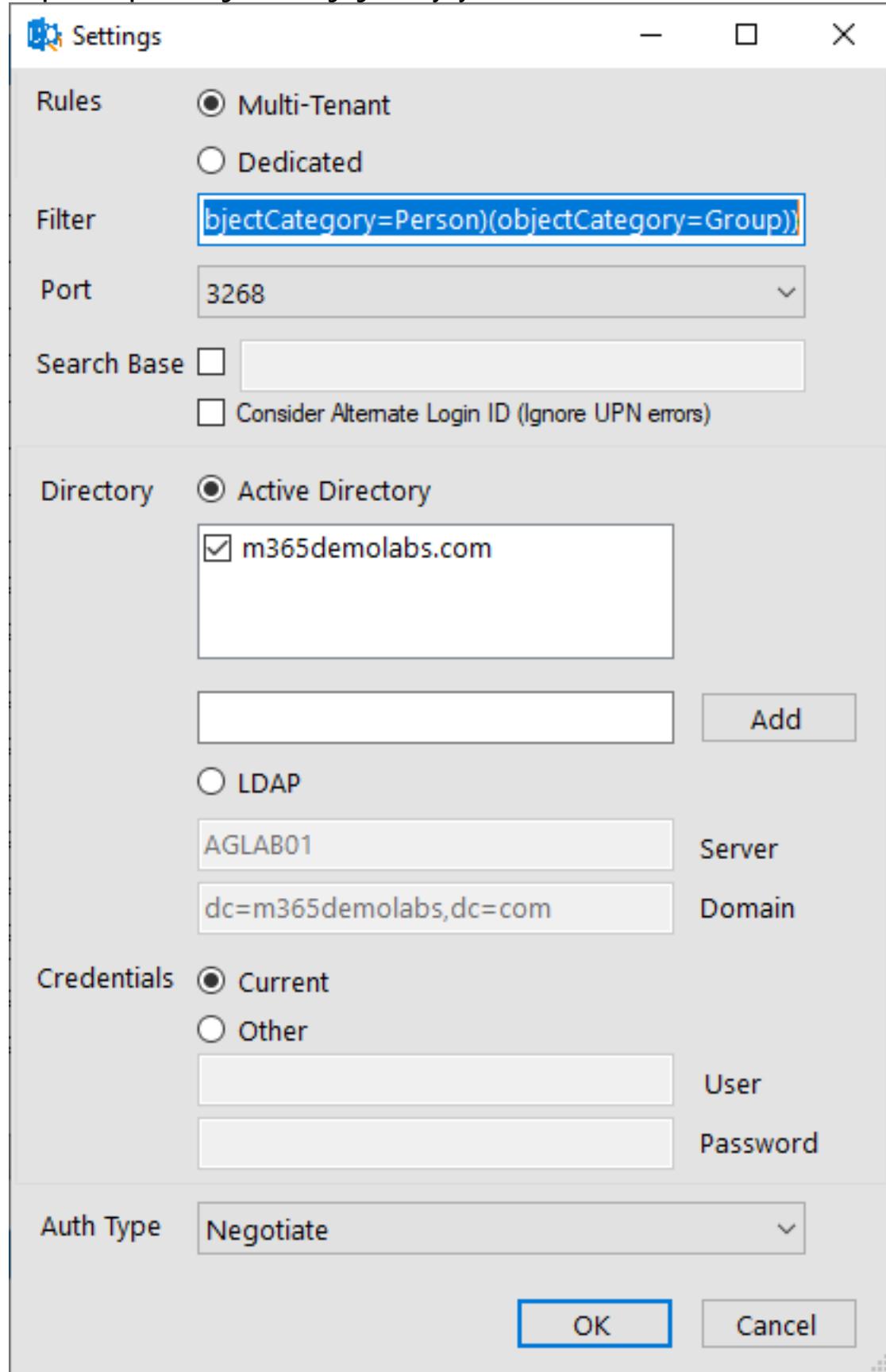


Figure 4.1 – IdFix Settings

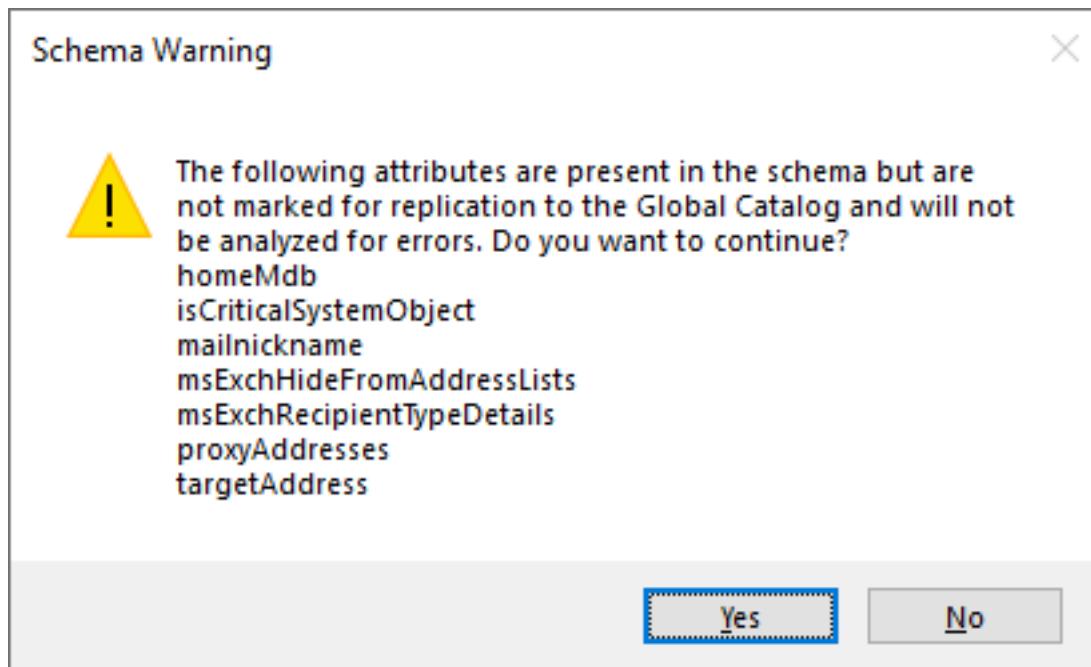


Figure 4.2 – IdFix schema warning

Office 365		Query	Cancel	Accept	Apply	Export	Import	Undo	More
DISTINGUISHEDNAME	COMMONNAME	OBJECTCLASS	ATTRIBUTE	ERROR	VALUE	UPDATE	ACTION		
CN=ELane A Emanuel...	ELane A Emanuel	user	userPrincipalName	Character	E\Lane.A.Emanuel...	E\Lane.A.Emanuel@...	EDIT	▼	
CN=ELane C Baer,...	ELane C Baer	user	userPrincipalName	Character	E\Lane.C.Baer@m3...	E\Lane.C.Baer@m3...	▼	▼	
CN=ELane H Lovell,...	ELane H Lovell	user	userPrincipalName	Character	E\Lane.H.Lovell@m...	E\Lane.H.Lovell@m3...	▼	▼	
CN=ELane J Montemay...	ELane J Montemayor	user	userPrincipalName	Character	E\Lane.J.Montemayo...	E\Lane.J.Montemayo...	▼	▼	
CN=ELane K Hamon...	ELane K Hamon	user	userPrincipalName	Character	E\Lane.K.Hamon@m...	E\Lane.K.Hamon@m...	▼	▼	
CN=ELane M Holiday...	ELane M Holiday	user	userPrincipalName	Character	E\Lane.M.Holiday@m...	E\Lane.M.Holiday@m...	▼	▼	
CN=ELane P Beaty....	ELane P Beaty	user	userPrincipalName	Character	E\Lane.P.Beaty@m3...	E\Lane.P.Beaty@m3...	▼	▼	
CN=ELane T Cutler...	ELane T Cutler	user	userPrincipalName	Character	E\Lane.T.Cutler@m...	E\Lane.T.Cutler@m3...	▼	▼	
CN=ELane T Francis...	ELane T Francis	user	userPrincipalName	Character	E\Lane.T.Francis@m...	E\Lane.T.Francis@m...	▼	▼	
CN=ELane V Popp....	ELane V Popp	user	userPrincipalName	Character	E\Lane.V.Popp@m3...	E\Lane.V.Popp@m3...	▼	▼	
CN=Engineering Eng...	Engineering Engineer...	group	sAMAccountName	Duplicate	Engineering Engine...	Engineering Engine...	▼	▼	
CN=Engineering Eng...	Engineering Engineer...	group	sAMAccountName	Duplicate	Engineering Engine...	Engineering Engine...	▼	▼	
CN=Engineering Eng...	Engineering Engineer...	group	sAMAccountName	Duplicate	Engineering Engine...	Engineering Engine...	▼	▼	
CN=Engineering Eng...	Engineering Engineer...	group	sAMAccountName	Duplicate	Engineering Engine...	Engineering Engine...	▼	▼	
CN=Engineering Eng...	Engineering Engineer...	group	sAMAccountName	Duplicate	Engineering Engine...	Engineering Engine...	▼	▼	
CN=Engineering Eng...	Engineering Engineer...	group	sAMAccountName	Duplicate	Engineering Engine...	Engineering Engine...	▼	▼	
CN=Engineering Eng...	Engineering Engineer...	group	sAMAccountName	Duplicate	Engineering Engine...	Engineering Engine...	▼	▼	
CN=Engineering Eng...	Engineering Engineer...	group	sAMAccountName	Duplicate	Engineering Engine...	Engineering Engine...	▼	▼	
CN=Engineering Ma...	Engineering Manager...	group	sAMAccountName	Duplicate	Engineering Manag...	Engineering Manager...	▼	▼	
CN=Engineering Ma...	Engineering Manager...	group	sAMAccountName	Duplicate	Engineering Manag...	Engineering Manager...	▼	▼	
CN=Engineering Ma...	Engineering Manager	group	sAMAccountName	Duplicate	Engineering Manager	Engineering Manager	▼	▼	
CN=Engineering Ma...	Engineering Manager	group	sAMAccountName	Duplicate	Engineering Manager	Engineering Manager	▼	▼	
CN=Engineering Res...	Engineering Resear...	group	sAMAccountName	Duplicate	Engineering Resear...	Engineering Research...	▼	▼	

Figure 4.3 – IdFix data grid

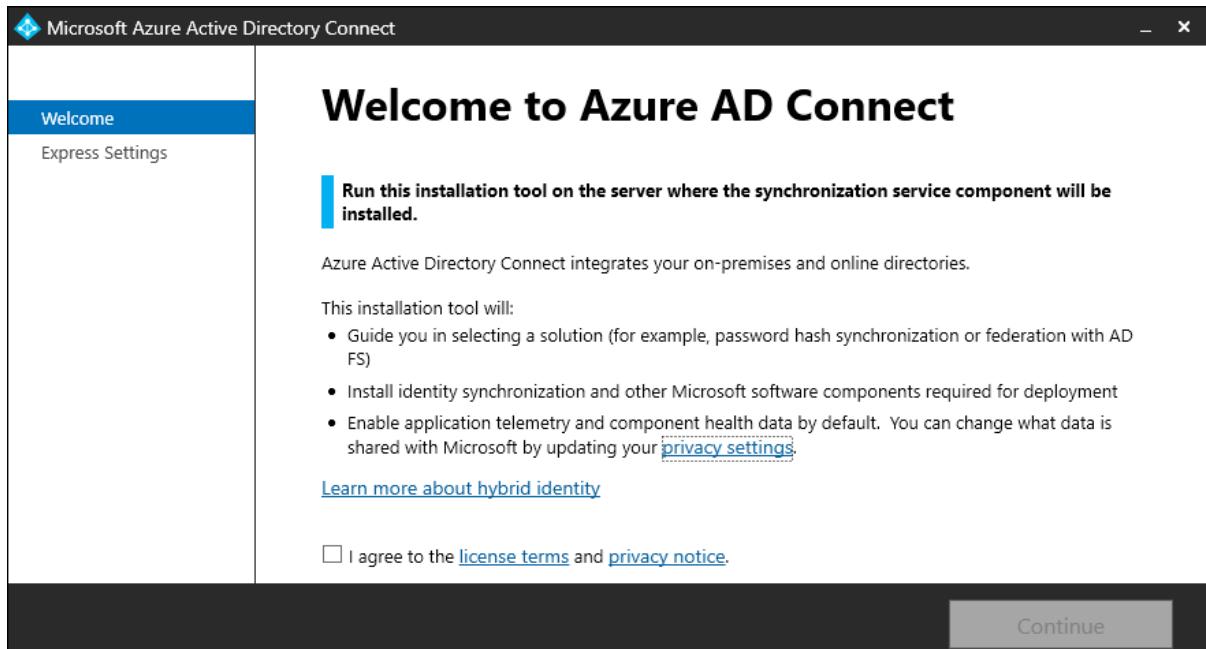


Figure 4.4 – Azure AD Connect welcome page

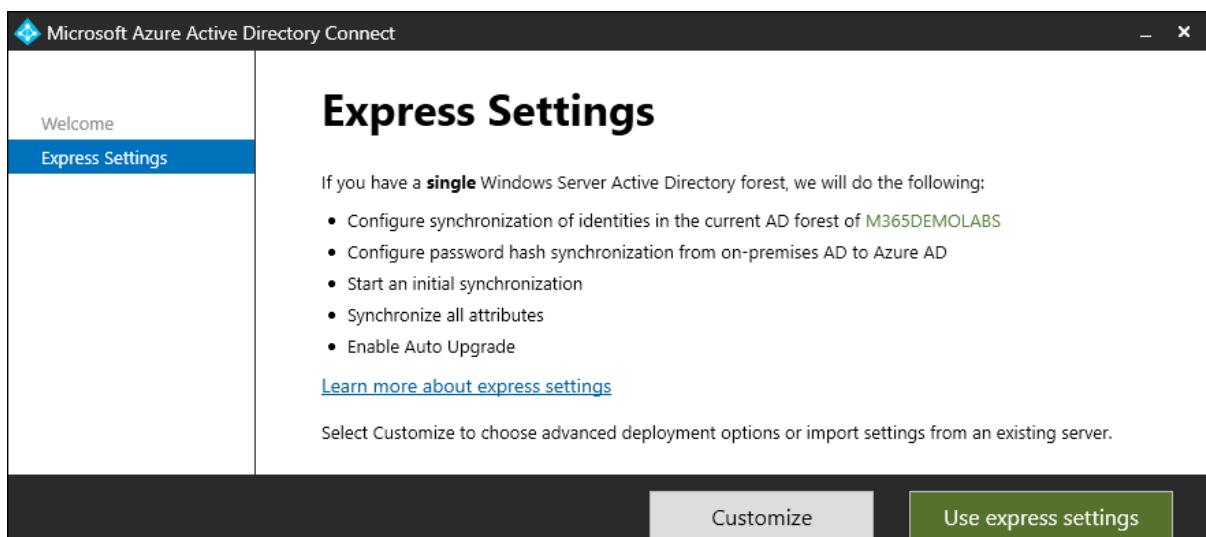


Figure 4.5 – Azure AD Connect Express Settings page

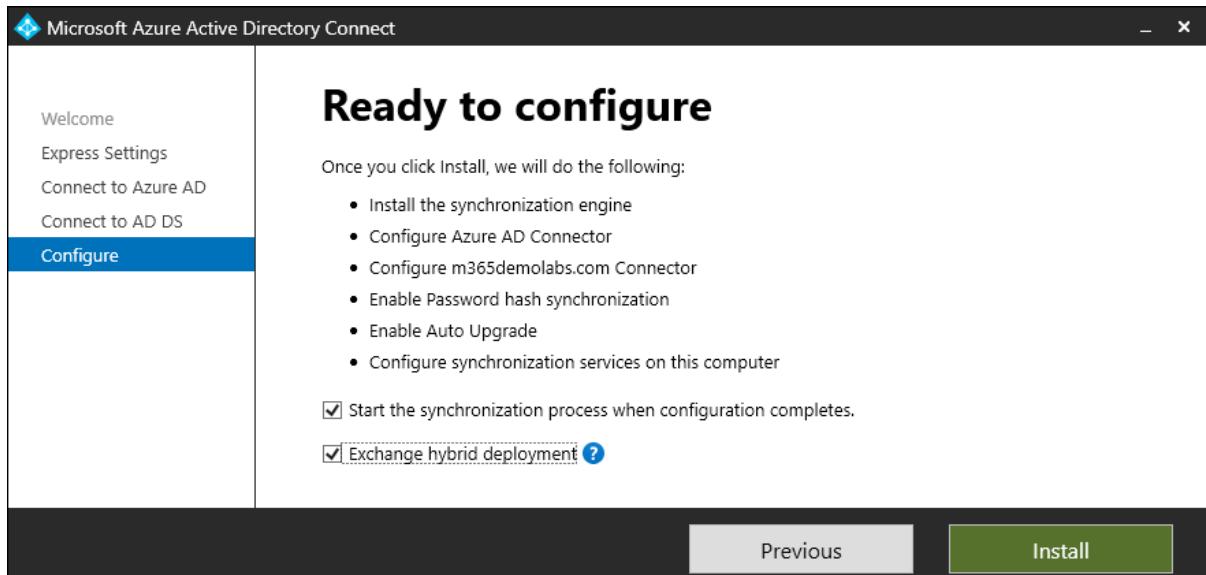


Figure 4.6 – Azure AD Connect Ready to configure page

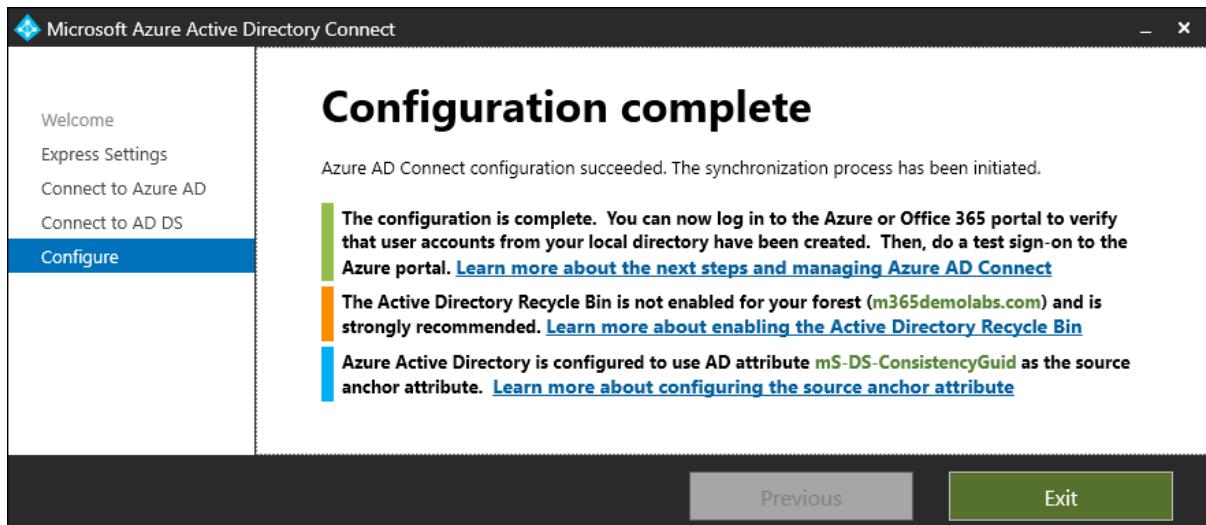


Figure 4.7 – Azure AD Connect Configuration complete page

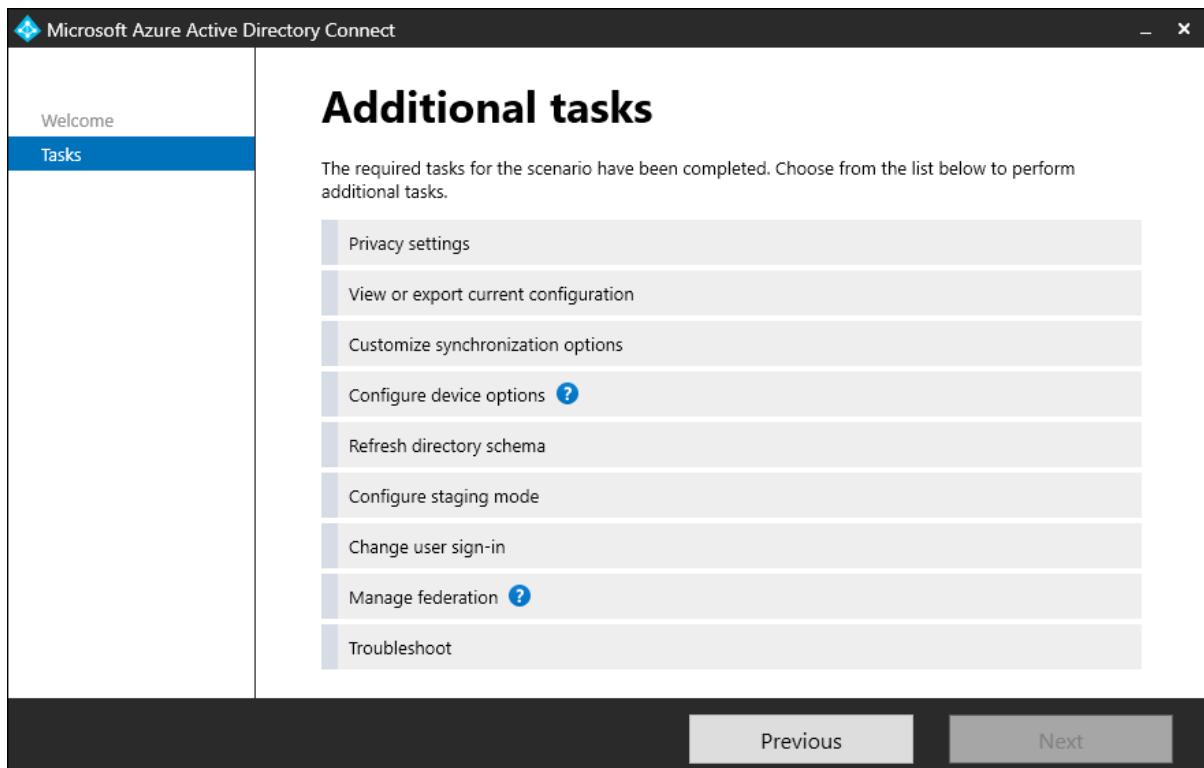


Figure 4.8 – Additional tasks page

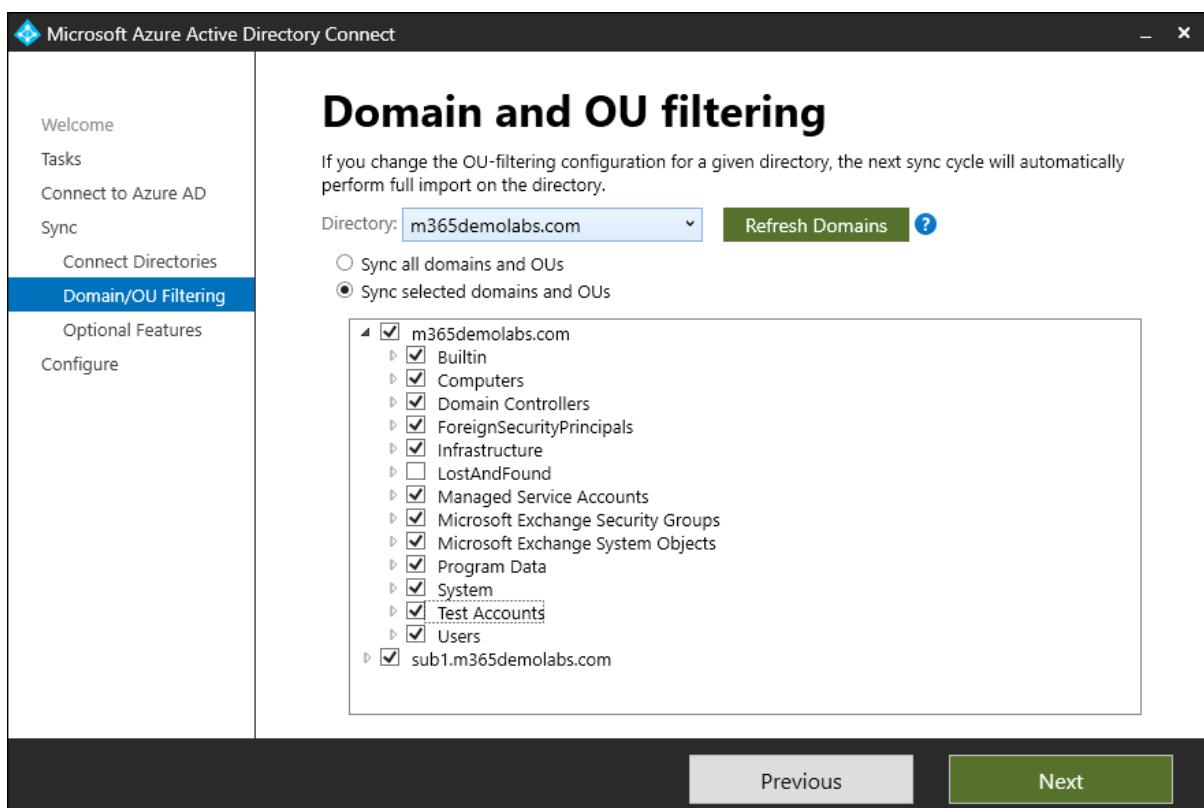


Figure 4.9 – Azure AD Connect Domain and OU filtering page

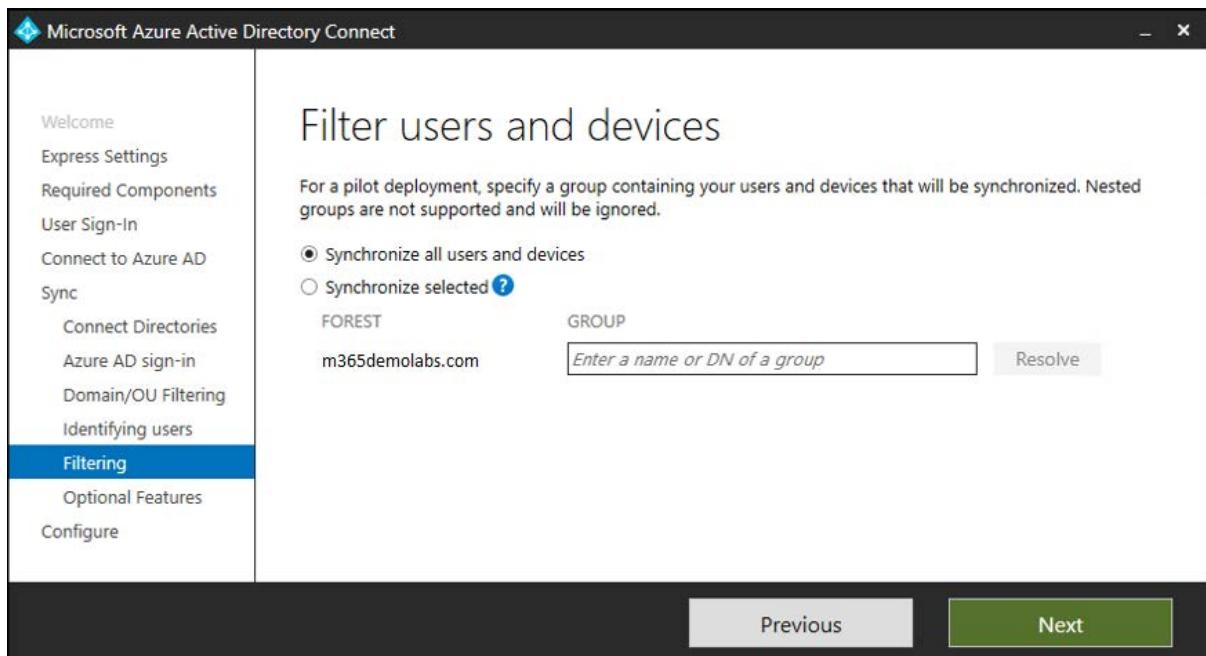


Figure 4.10 – Filter users and devices page

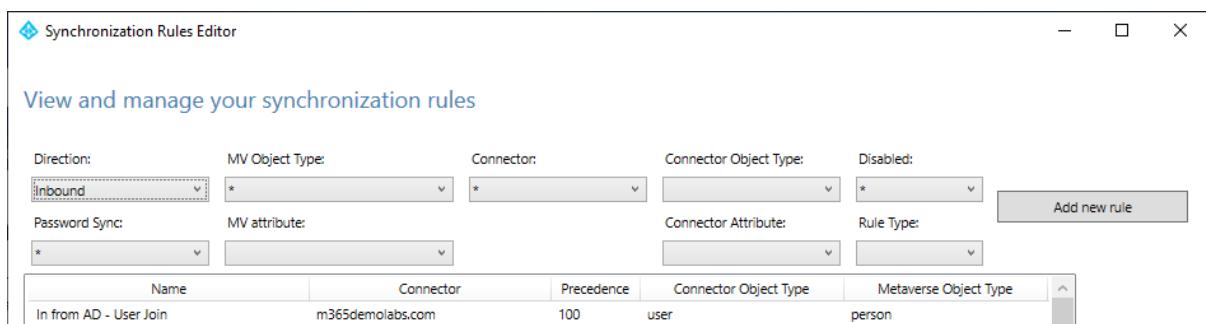


Figure 4.11 – Synchronization rules editor

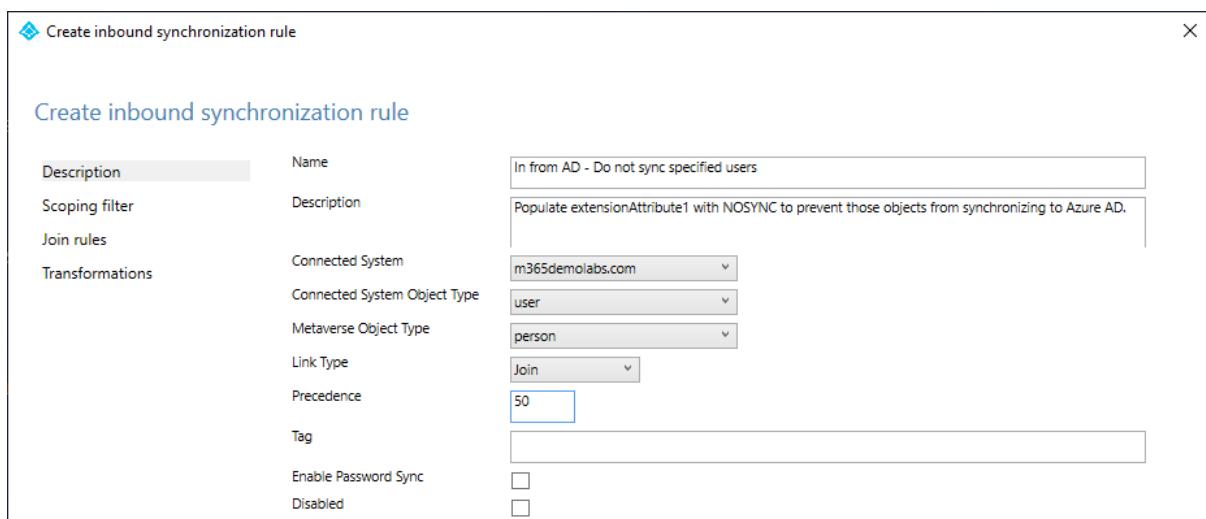


Figure 4.12 – Creating a new inbound synchronization rule

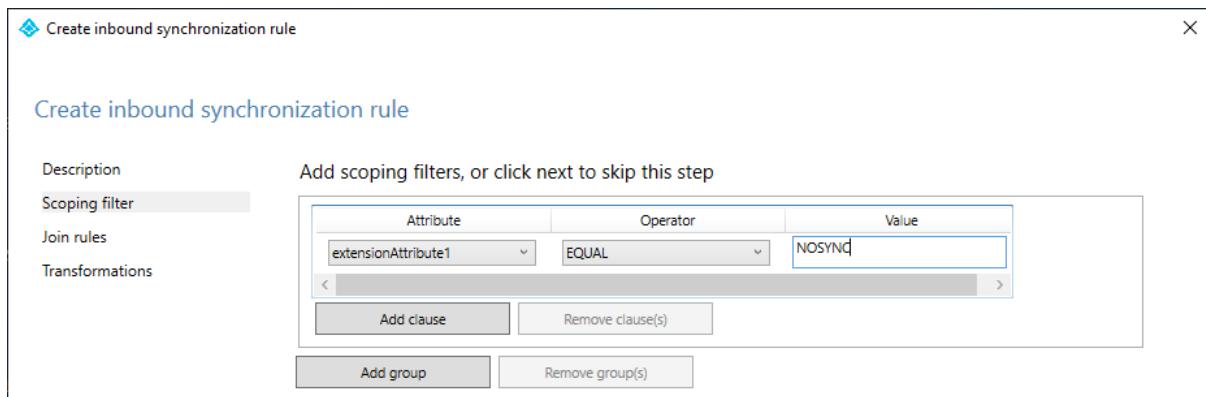


Figure 4.13 – Configuring a scoping filter for extensionAttribute1

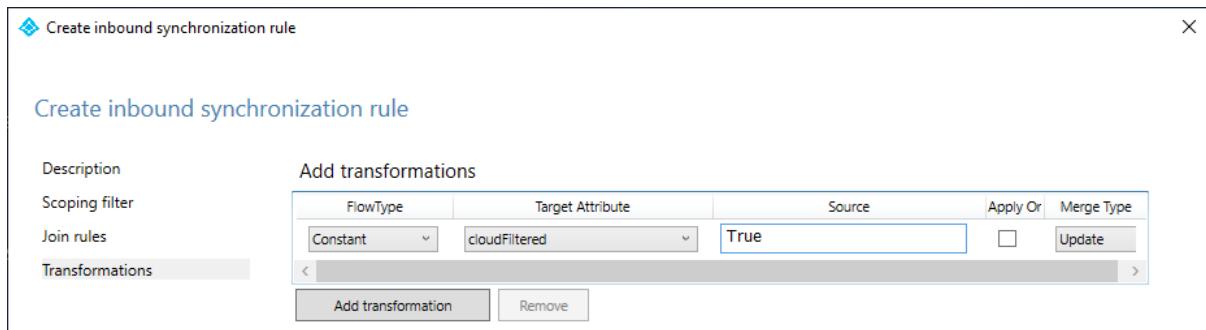


Figure 4.14 – Adding a transformation for the cloudFiltered attribute

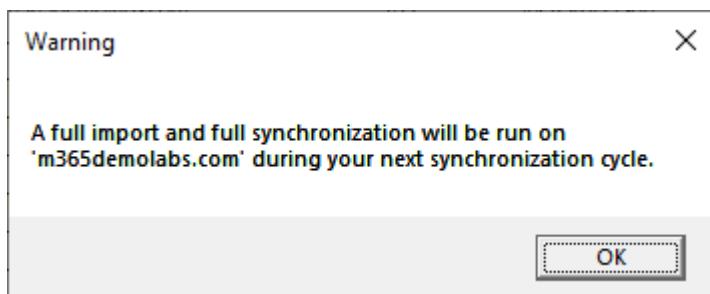


Figure 4.15 – Warning for full import and synchronization

The screenshot shows the Azure Active Directory Connect Health Quick start page. The left sidebar includes links for Sync errors, Sync services, AD FS services, AD DS services, Settings, IAM, Troubleshoot, and New support request. The main content area features a 'What's new' section about Azure AD Connect Health for Sync, a 'Get tools' section with download links for agents, a 'Provide feedback' section, and a 'Learn more' section with documentation and FAQs.

Figure 4.16 – Azure Active Directory Connect Health

The screenshot shows the Azure AD Connect Health Sync errors page. The left sidebar is identical to Figure 4.16. The main content area displays a table titled 'Sync Error by Type' with four categories: Duplicate Attribute (2 errors), Data Mismatch (0 errors), Data Validation Failure (7 errors), and Large Attribute (0 errors). Below this table is another table showing Federated Domain C... (0 errors), Existing Admin Role ... (0 errors), and Other (2 errors).

Duplicate Attribute	Data Mismatch	Data Validation Failure	Large Attribute
AadSyncService-M365w520429... 2	AadSyncService-M365w520429... 0	AadSyncService-M365w520429... 7	AadSyncService-M365w520429... 0

Federated Domain C...	Existing Admin Role ...	Other
AadSyncService-M365w520429... 0	AadSyncService-M365w520429... 0	AadSyncService-M365w520429... 2

Figure 4.17 – Azure AD Connect Health Sync errors

The screenshot shows a Microsoft Azure AD Connect Health error details page. The title is "Duplicate Attribute Error". The error type is "AttributeValueMustBeUnique" for the attribute "ProxyAddresses". The message states: "Unable to update this object because the ProxyAddresses value SMTP:HumanResourcesManager-California@sub1.m365demolabs.com associated with this object may already be associated with another object in your local directory services. To resolve this conflict, first determine which object should be using the conflicting value. Then, update or remove the conflicting value from the other object(s).". A table provides detailed information about the conflicting object:

Attribute	Object With Conflicting Attribute	Existing Object
Display Name	Human Resources Manager - California	Human Resources Manager - California
Object Type	group	group
User Principal Name		N/A
Licenses		View assigned licenses
Distinguished Name	CN=Human Resources Manager - California,OU=Groups,OU=Test Accounts,DC=sub1,DC=m365demolabs,DC=com	N/A
Mail	HumanResourcesManager-California@sub1.m365demolabs.com	HumanResourcesManager-California@sub1.m365demolabs.com
Object GUID	248076a3-1bd6-4ae3-877e-d08a40d6b964	77b6714f-4983-4d28-a4dc-596c134c0f5b

Figure 4.18 – Azure AD Connect Health error details

The screenshot shows the "Azure Active Directory Connect Health | AD DS services" section. It includes a "Quick start" sidebar with "Sync errors" and "Sync services" options. The main area displays a table of AD DS services:

Service Name	Active Alerts	Last Updated	Status
m365demolabs.com	0	3/13/2023, 12:52:47 AM	Healthy

Figure 4.19 – Azure AD Connect Health AD DS services

The screenshot shows the Azure AD Connect Health interface for Domain Services (DS) for the domain **m365demolabs.com**. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information (admin@M365w520429... and CONTOSO (M365W520429.ONM...)). Below the header, the breadcrumb navigation shows Home > Azure Active Directory Connect Health | AD DS services > **m365demolabs.com**.

The main content area displays the following details:

- Essentials**:
 - Forest name: **m365demolabs.com**
 - Functional Level: **Windows2016Forest**
 - Domain naming master FSMO role: **AGLAB01.m365demolabs.com**
- Domain Controllers, Domains and Sites**:
 - m365demolabs.com** (1 of 2 DCs monitored)
 - Domains**: 2 DOMAINS
 - Sites**
- Replication Status**:
 - m365demolabs.com**
 - 0** DCs with errors

Figure 4.20 – Azure AD Connect Health for DS detail page

The screenshot shows the Azure AD Connect Health interface for Active Directory Federation Services (AD FS) for the service **www.m365demolabs.com**. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information (admin@M365w520429... and CONTOSO (M365W520429.ONM...)). Below the header, the breadcrumb navigation shows Home > Azure Active Directory Connect Health > **Azure Active Directory Connect Health | AD FS services**.

The main content area displays the following details:

- Quick start**:
 - Sync errors**
 - Sync services**
- Active Directory Federation Services**:
 - AD FS services**
- Find ...** search bar
- Table** showing service status:

Service Name	Active Alerts	Last Updated	Status
www.m365demolabs.com	0	1/1/1, 12:00:00 AM	Healthy

Figure 4.21 – Azure AD Connect Health for AD FS

The screenshot shows the Microsoft Azure interface for Azure Active Directory Connect Health. At the top, there's a search bar and a user profile for 'admin@M365w520429...' and 'CONTOSO (M365WS520429.DNM...)'. Below the header, the URL 'www.m365demolabs.com' is displayed. The main content area is titled 'Overview' and contains a summary of service instances:

- Federation Server: 1 INSTANCE
- Federation Server Proxy: 1 INSTANCE

At the bottom of the overview section are two buttons: 'Quick Start' and 'Properties'. Below this is the 'Operations' section, which includes an 'Alerts' tab showing one alert for 'AdFederationService-www.m365demolabs.com'.

Figure 4.22 – Azure AD Connect Health for AD FS overview

The screenshot shows the Microsoft Azure Active Directory Connect Troubleshooting interface. On the left, a sidebar lists 'Welcome', 'Tasks', and 'Troubleshooting', with 'Troubleshooting' being the active tab. The main area has a title 'Welcome to AADConnect Troubleshooting' and a subtitle 'AZURE AD CONNECT TROUBLESHOOTING TOOL'. A large green 'Launch' button is centered at the bottom of this area.

Figure 4.23 – Launching the AADConnect Troubleshooting tool

The screenshot shows a Windows PowerShell window titled 'Administrator: Windows PowerShell'. The title bar also includes 'Microsoft Azure Active Directory Connect'. The main content is a menu for 'AADConnect Troubleshooting' with the following options:

```
Enter '1' - Troubleshoot Object Synchronization
Enter '2' - Troubleshoot Password Hash Synchronization
Enter '3' - Collect General Diagnostics
Enter '4' - Configure AD DS Connector Account Permissions
Enter '5' - Test Azure Active Directory Connectivity
Enter '6' - Test Active Directory Connectivity
Enter 'Q' - Quit
```

Below the menu, a prompt says 'Please make a selection: -'

Figure 4.24 – AADConnect Troubleshooting menu

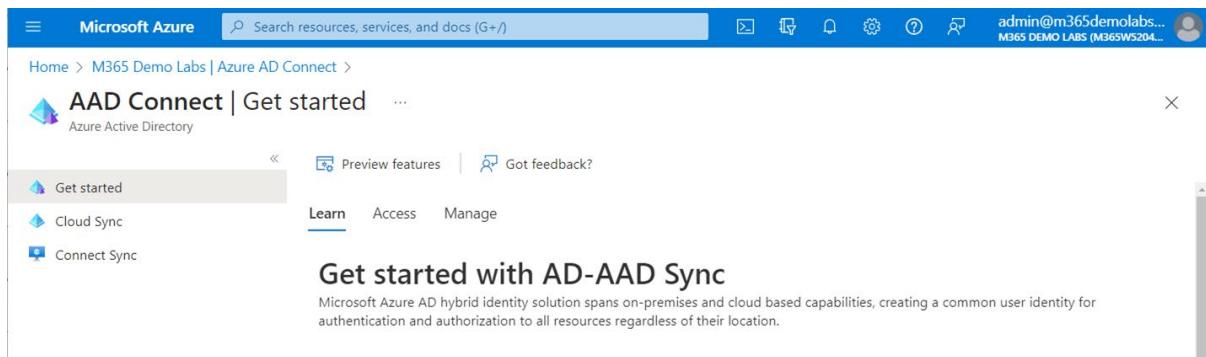


Figure 4.25 – Azure AD Connect in the Azure portal

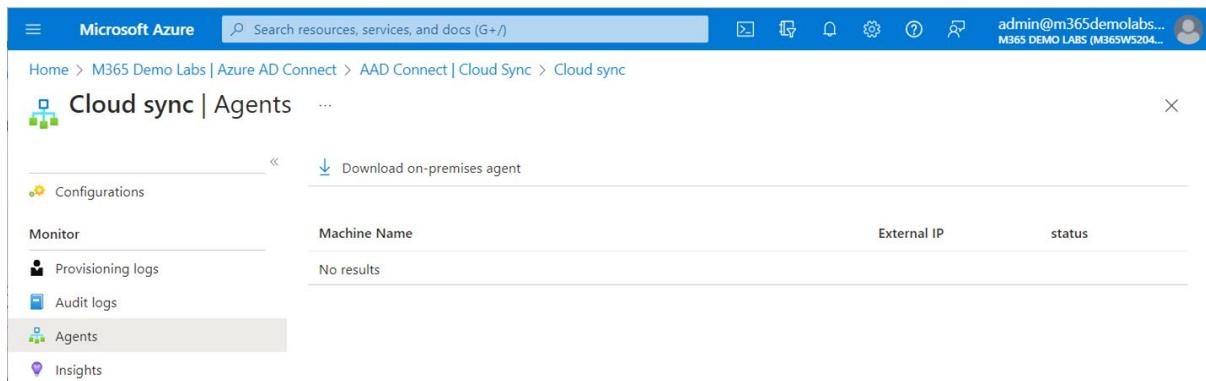


Figure 4.26 – Download on-premises agent for Azure AD Connect Cloud Sync

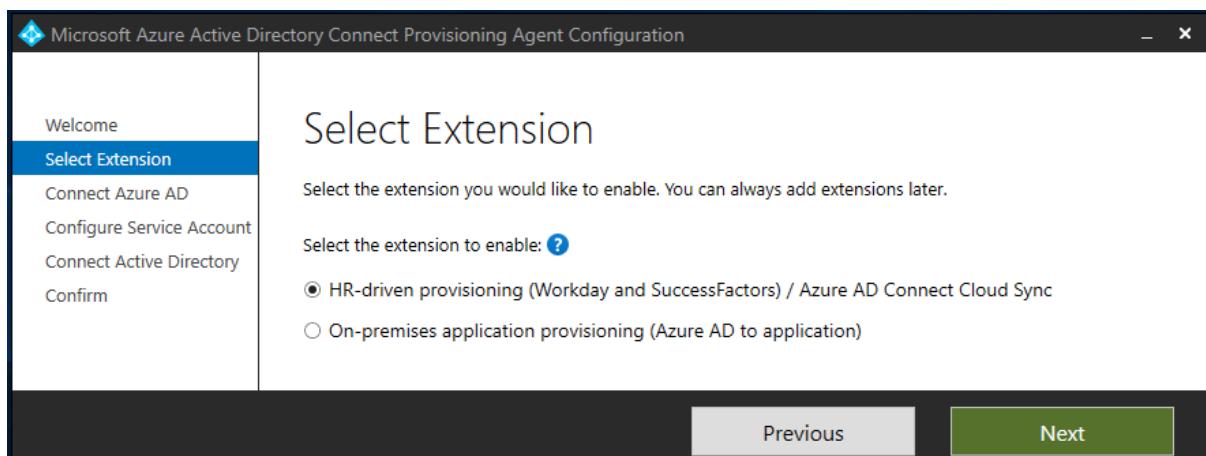


Figure 4.27 – Azure AD Connect Cloud Sync Select Extension page

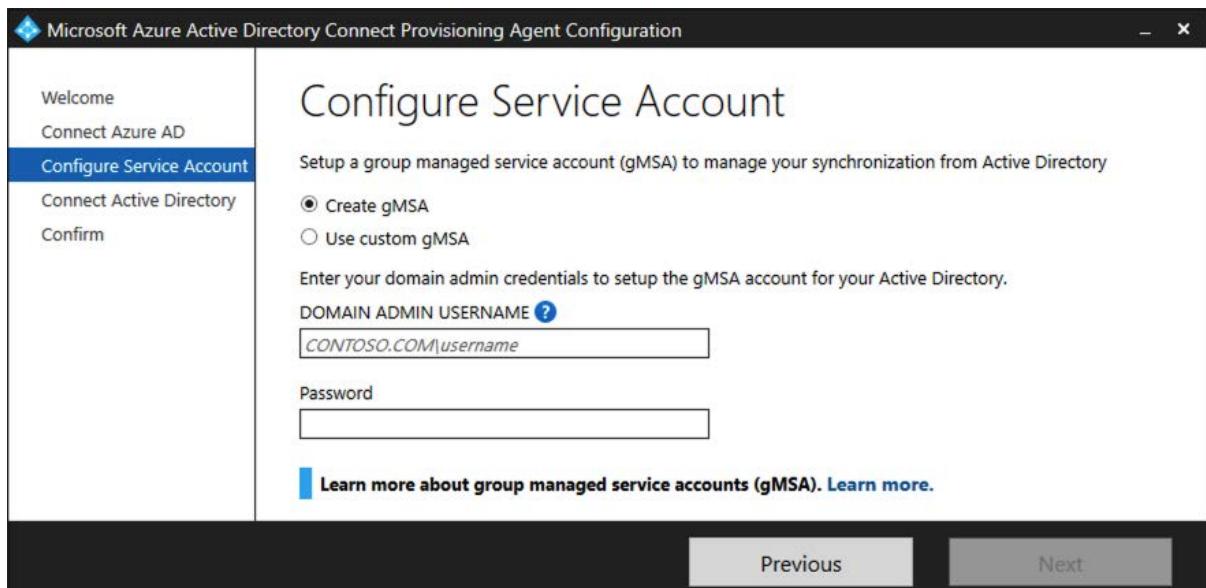


Figure 4.28 – Configure Azure AD Connect Cloud Sync service account

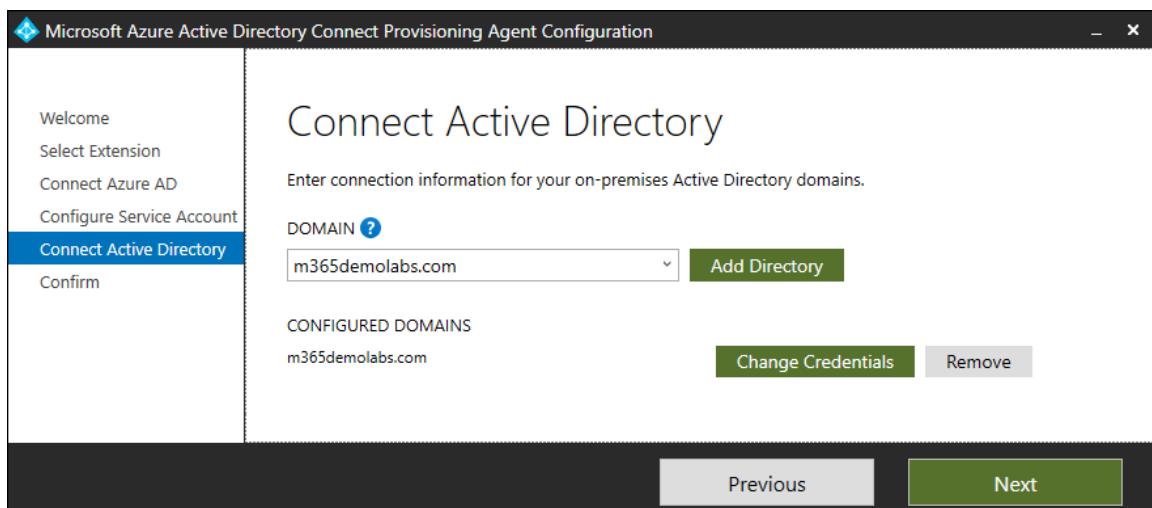


Figure 4.29 – Adding a directory to Azure AD Connect Cloud Sync

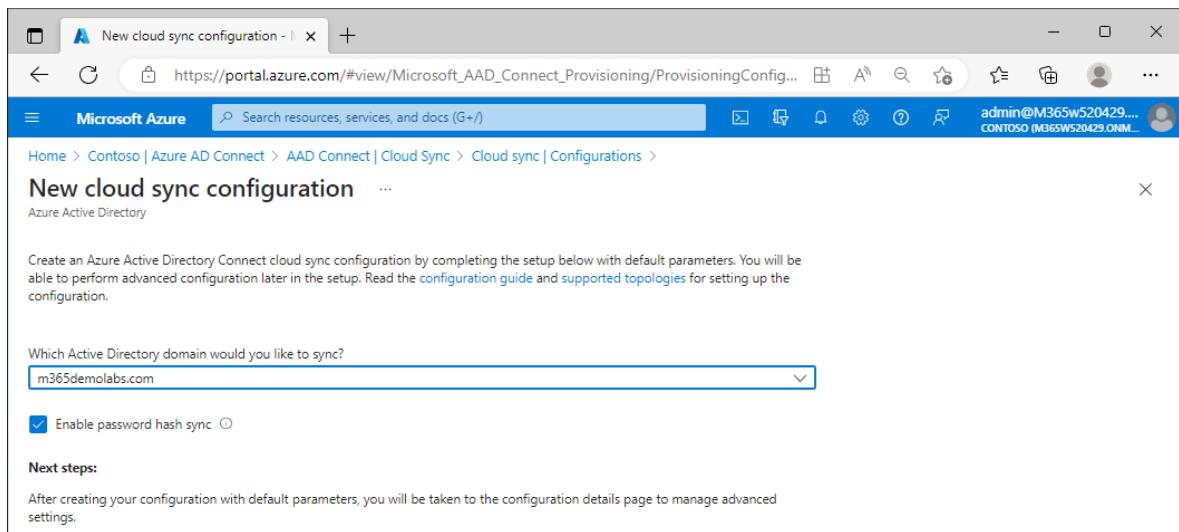


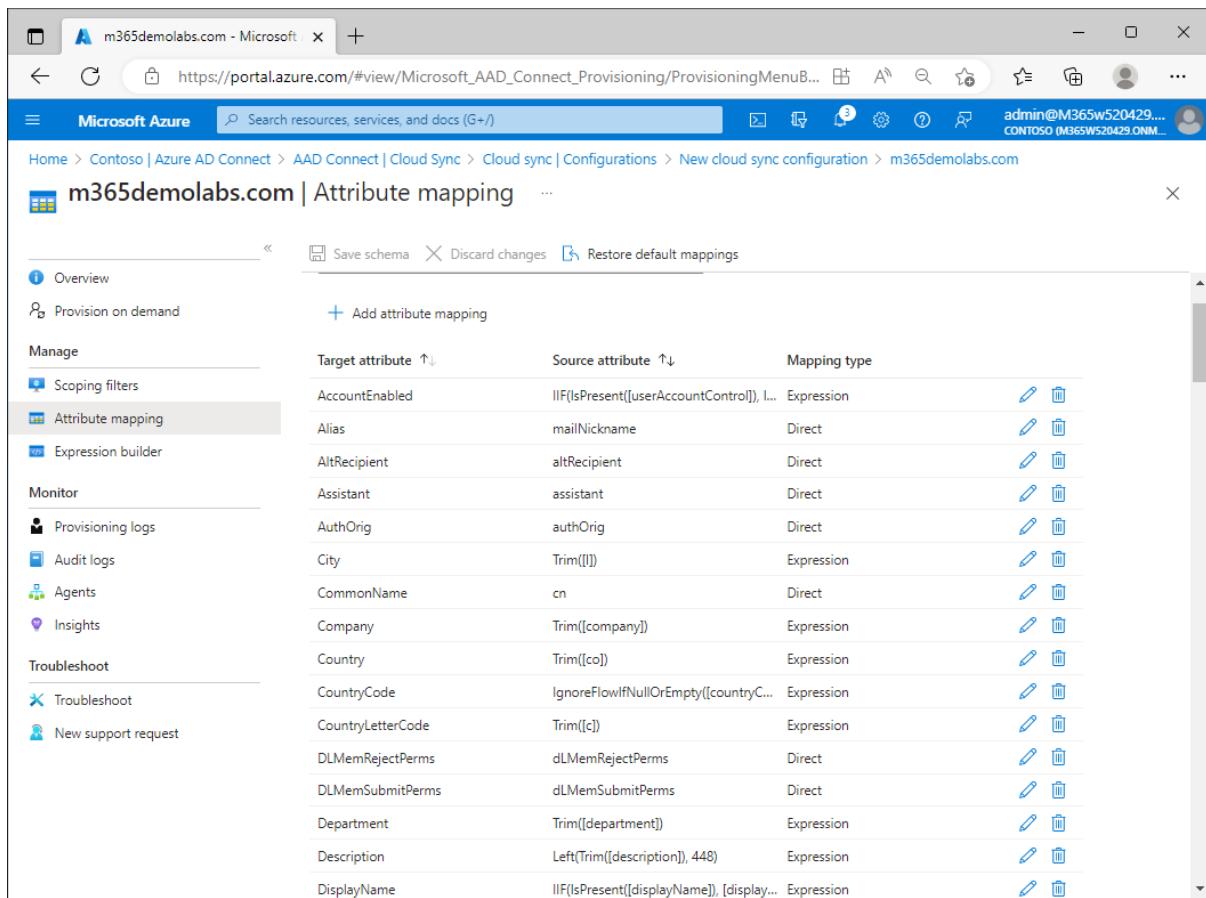
Figure 4.30 – Creating a new Azure AD Connect Cloud Sync configuration

The screenshot shows the Microsoft Azure portal interface. The URL in the address bar is https://portal.azure.com/#view/Microsoft_AAD_Connect_Provisioning/ProvisioningMenuBl.... The top navigation bar includes links for Home, Contoso | Azure AD Connect, AAD Connect | Cloud Sync, Cloud sync | Configurations, and New cloud sync configuration. The main title is "m365demolabs.com | Overview". On the left, there's a sidebar with sections like Overview, Provision on demand, Manage (Scoping filters, Attribute mapping, Expression builder), Monitor (Provisioning logs, Audit logs, Agents, Insights), and Troubleshoot (Troubleshoot). The main content area has tabs for Get started, Overview, Properties, and Tutorials. Under "Get started", there's a section titled "Get started provisioning your agent" with a sub-section "How do I configure with Cloud Sync?". It features two icons: one for "Add scoping filters" (showing laboratory glassware) and another for "Edit attributes" (showing a person icon). Below these are two numbered steps: "1. Add scoping filters (optional)" and "2. Map attributes (optional)". Step 1 has a link "Add scoping filters" and a note about filtering objects from on-premises directories. Step 2 has a link "Edit attributes".

Figure 4.31 – Provisioning agent overview page

The screenshot shows the Microsoft Azure portal interface. The URL in the address bar is https://portal.azure.com/#view/Microsoft_AAD_Connect_Provisioning/ProvisioningMenuBl.... The top navigation bar includes links for Home, Contoso | Azure AD Connect, AAD Connect | Cloud Sync, Cloud sync | Configurations, and m365demolabs.com. The main title is "m365demolabs.com | Scoping filters". The left sidebar is identical to Figure 4.31. The main content area shows the "Scoping filters" configuration page. It has a "Save" button at the top right. Under "Manage", the "Scoping filters" option is selected. To its right, there are three radio buttons: "All users" (selected), "Selected security groups", and "Selected organizational units". Below these is a text input field labeled "Distinguished name of object" with a placeholder "No Results". There is also a "Add" button.

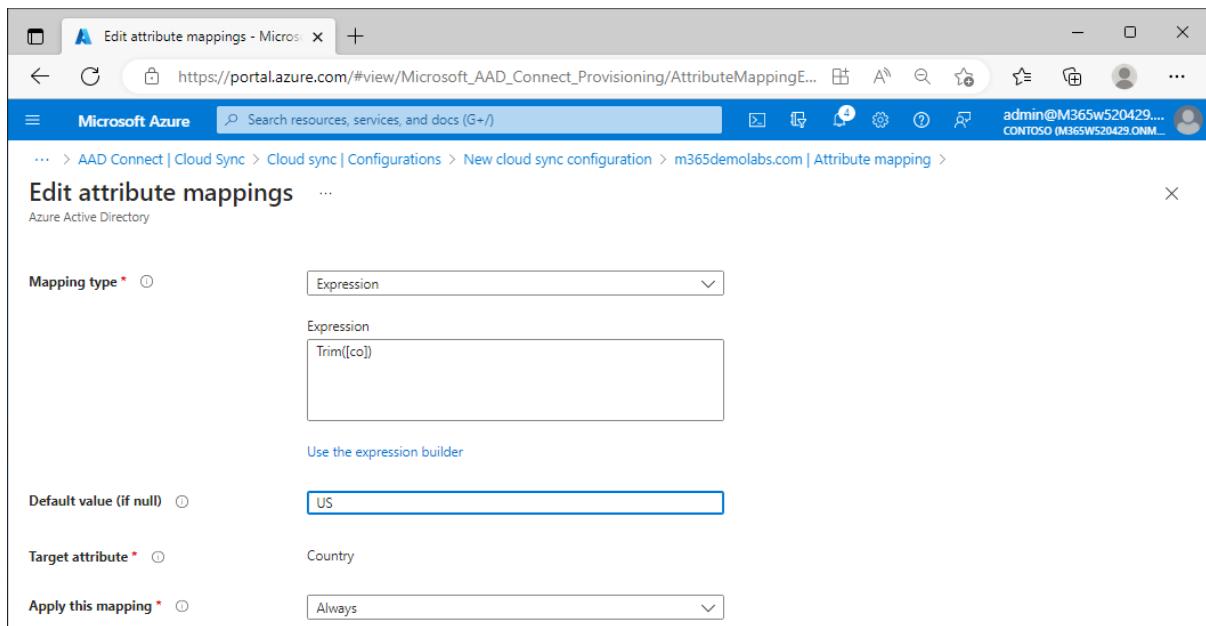
Figure 4.32 – Azure AD Connect Cloud Sync scoping filters



The screenshot shows the 'Attribute mapping' section of the Azure AD Connect Cloud Sync configuration. On the left, there's a sidebar with 'Overview', 'Provision on demand', 'Manage' (Scoping filters, Attribute mapping selected), 'Expression builder', 'Monitor' (Provisioning logs, Audit logs, Agents, Insights), and 'Troubleshoot' (Troubleshoot, New support request). The main area has tabs for 'Save schema', 'Discard changes', and 'Restore default mappings'. A large table lists attribute mappings:

Target attribute ↑↓	Source attribute ↑↓	Mapping type
AccountEnabled	IIF(IsPresent([userAccountControl]), I...	Expression
Alias	mailNickname	Direct
AltRecipient	altRecipient	Direct
Assistant	assistant	Direct
AuthOrig	authOrig	Direct
City	Trim([l])	Expression
CommonName	cn	Direct
Company	Trim([company])	Expression
Country	Trim([co])	Expression
CountryCode	IgnoreFlowIfNullOrEmpty([countryC...)	Expression
CountryLetterCode	Trim([c])	Expression
DLMemRejectPerms	dLMemRejectPerms	Direct
DLMemSubmitPerms	dLMemSubmitPerms	Direct
Department	Trim([department])	Expression
Description	Left(Trim([description]), 448)	Expression
DisplayName	IIF(IsPresent([displayName]), [display...)	Expression

Figure 4.33 – Azure AD Connect Cloud Sync attribute mappings



The screenshot shows the 'Edit attribute mappings' page. The URL is https://portal.azure.com/#view/Microsoft_AAD_Connect_Provisioning/AttributeMappingE... . It shows a form for editing a specific mapping:

Mapping type *: Expression
Expression:
Trim([co])
[Use the expression builder](#)

Default value (if null) *: US

Target attribute *: Country

Apply this mapping *: Always

Figure 4.34 – Edit attribute mappings in Azure AD Connect Cloud Sync

DASHBOARD > CHAPTER 4

Implementing and Managing Identity Synchronization with Azure AD

Summary

In this chapter, you learned how to deploy identity synchronization and authentication solutions. You learned how to configure filtering for both Azure AD Connect and Azure AD Connect Cloud Sync, as well as deploying and managing the health agents for diagnostic and troubleshooting.

The next chapter will discuss methods to manage authentication.

Chapter Review Questions

The Microsoft 365 Administrator MS-102 Exam Guide
by Aaron Guilmette

Select Quiz

Quiz 1

[SHOW QUIZ DETAILS](#) ▾

START

Figure 4.35 – Chapter Review Questions for Chapter 4

Chapter 5: Implementing and Managing Authentication

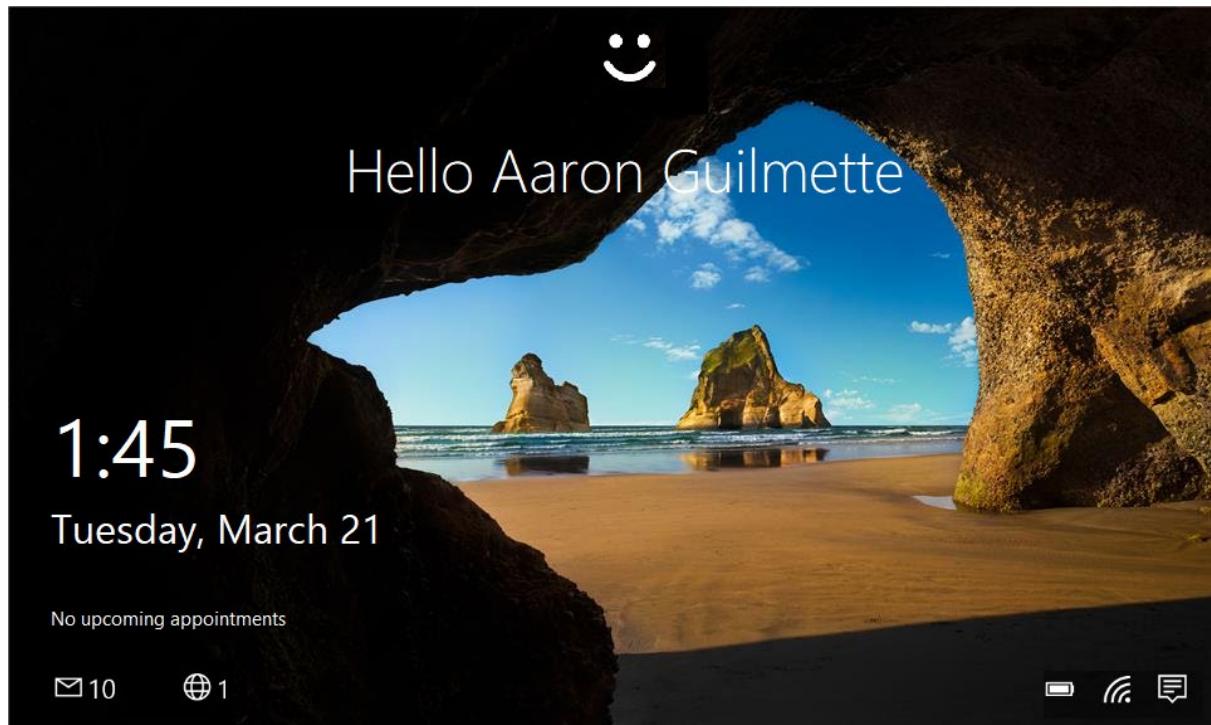


Figure 5.1 – Windows Hello for Business sign-on screen

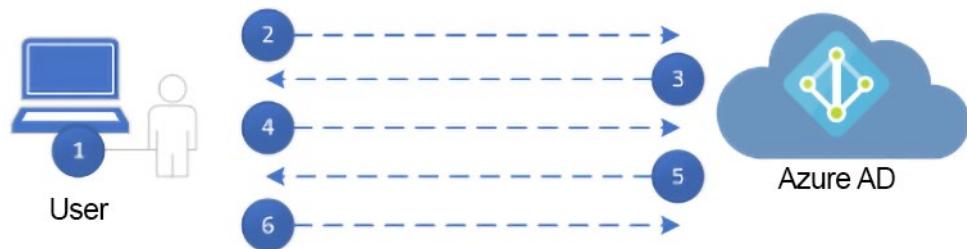


Figure 5.2 – Windows Hello authentication sequence

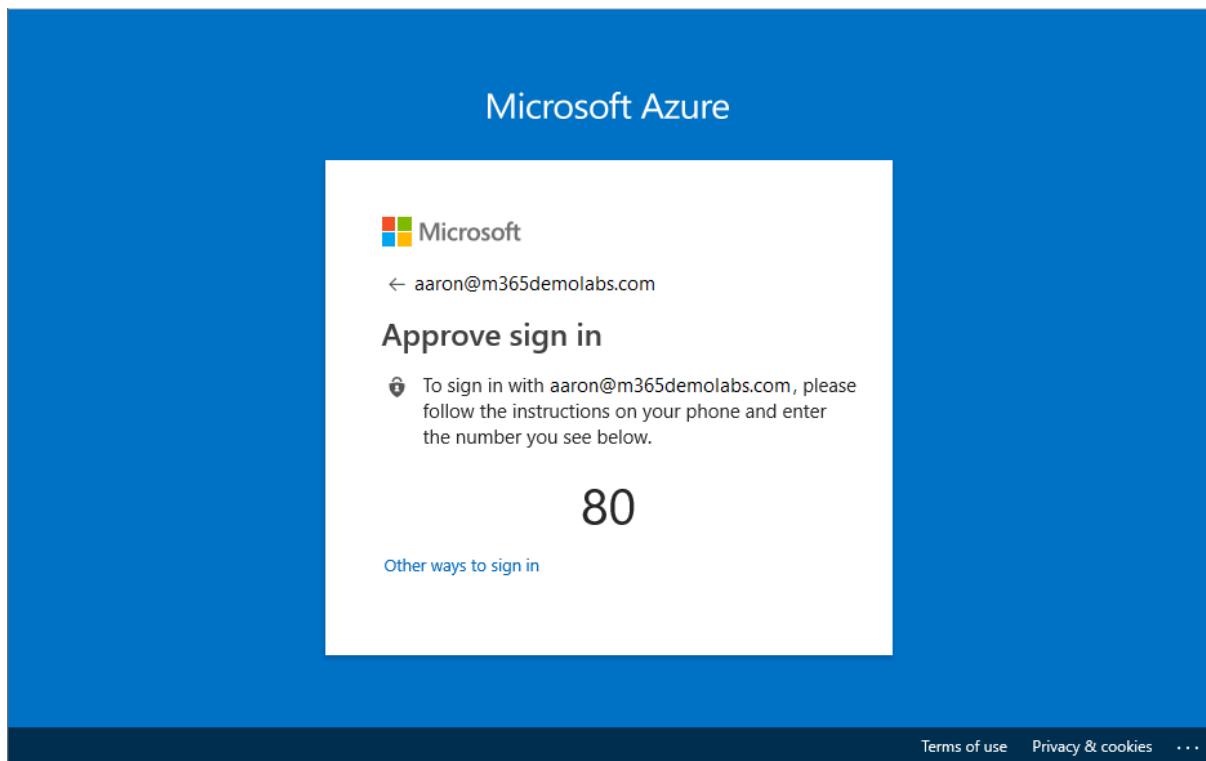


Figure 5.3 – Passwordless authentication dialog with Microsoft Authenticator

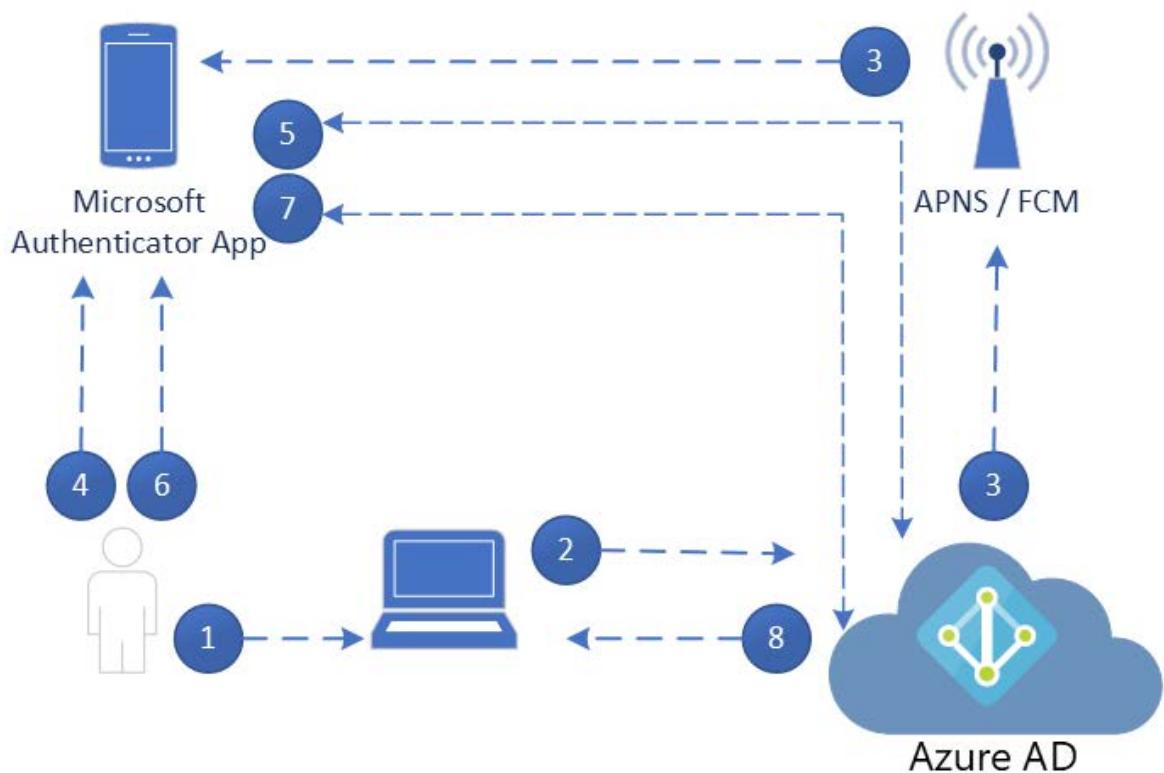


Figure 5.4 – Microsoft Authenticator authentication sequence

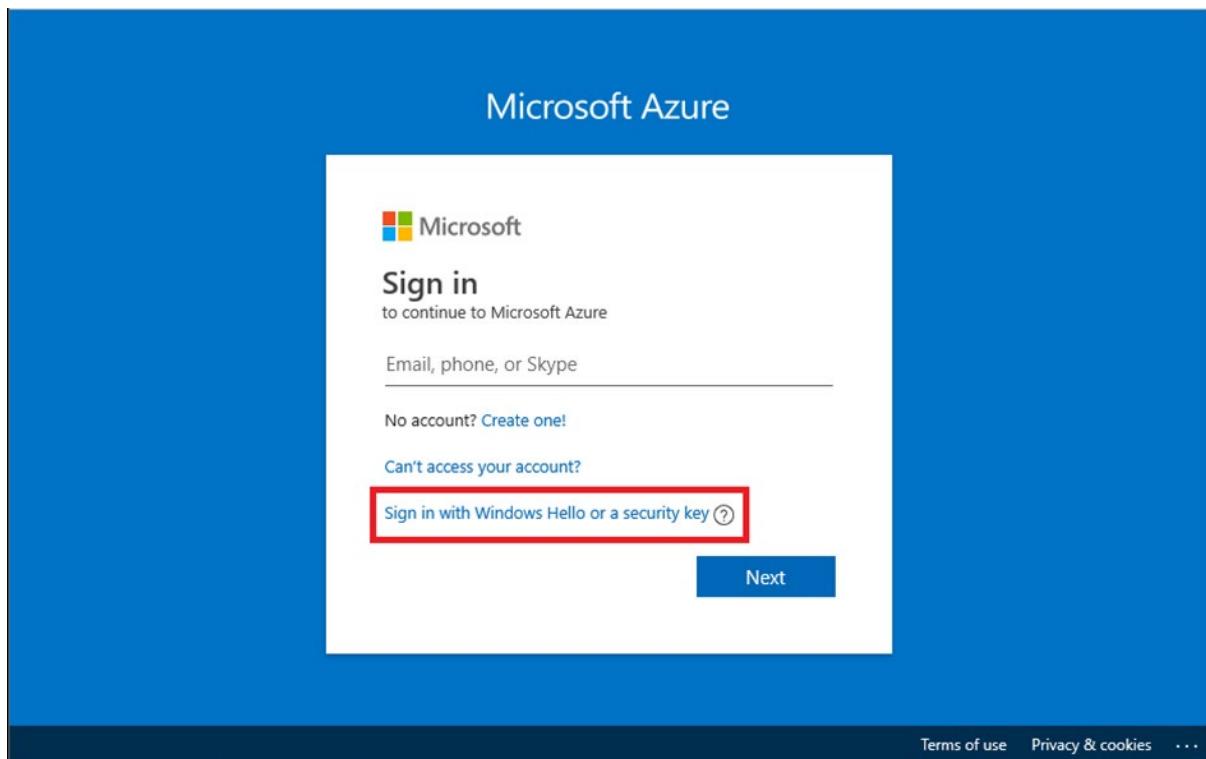


Figure 5.5 – Passwordless authentication dialog with a FIDO2 security token

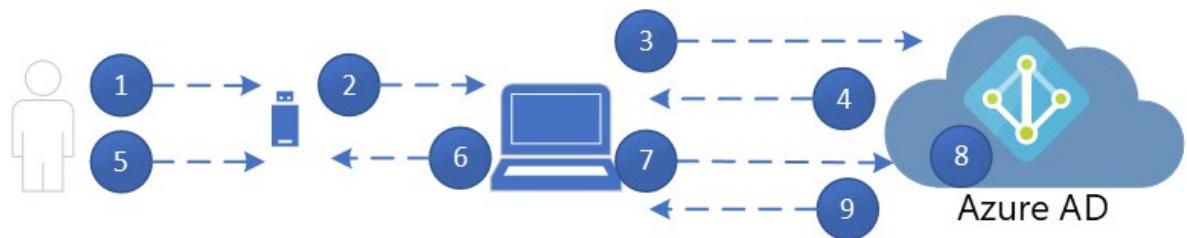


Figure 5.6 – FIDO2 authentication sequence

A screenshot of the Microsoft Intune admin center. The top navigation bar shows 'Microsoft Intune admin center' and the user 'labadmin@M365w5204...'. The main page title is 'Devices | Overview'. On the left, there's a sidebar with links like Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, and Users. The main content area has a search bar and tabs for 'Enrollment status', 'Enrollment alerts', and 'Compliance status'. A section titled 'Intune enrolled devices' shows a table with one entry: Platform 'Linux' and Devices '0'. The table was last updated on 3/24/23 at 8:22 PM.

Figure 5.7 – Enroll devices

The screenshot shows the Microsoft Intune admin center interface. The left sidebar includes options like Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled "Enroll devices | Windows enrollment". A search bar is at the top. Below it, a list of enrollment methods is shown: Windows enrollment (selected), Apple enrollment, Android enrollment, Enrollment device limit restrictions, Enrollment device platform restrictions, Corporate device identifiers, and Device enrollment managers. To the right, a "General" section highlights "Automatic Enrollment" (Configure Windows devices to enroll when they join or register with Azure Active Directory) and "Windows Hello for Business" (Replace passwords with strong two-factor authentication).

Figure 5.8 – Windows Hello for Business

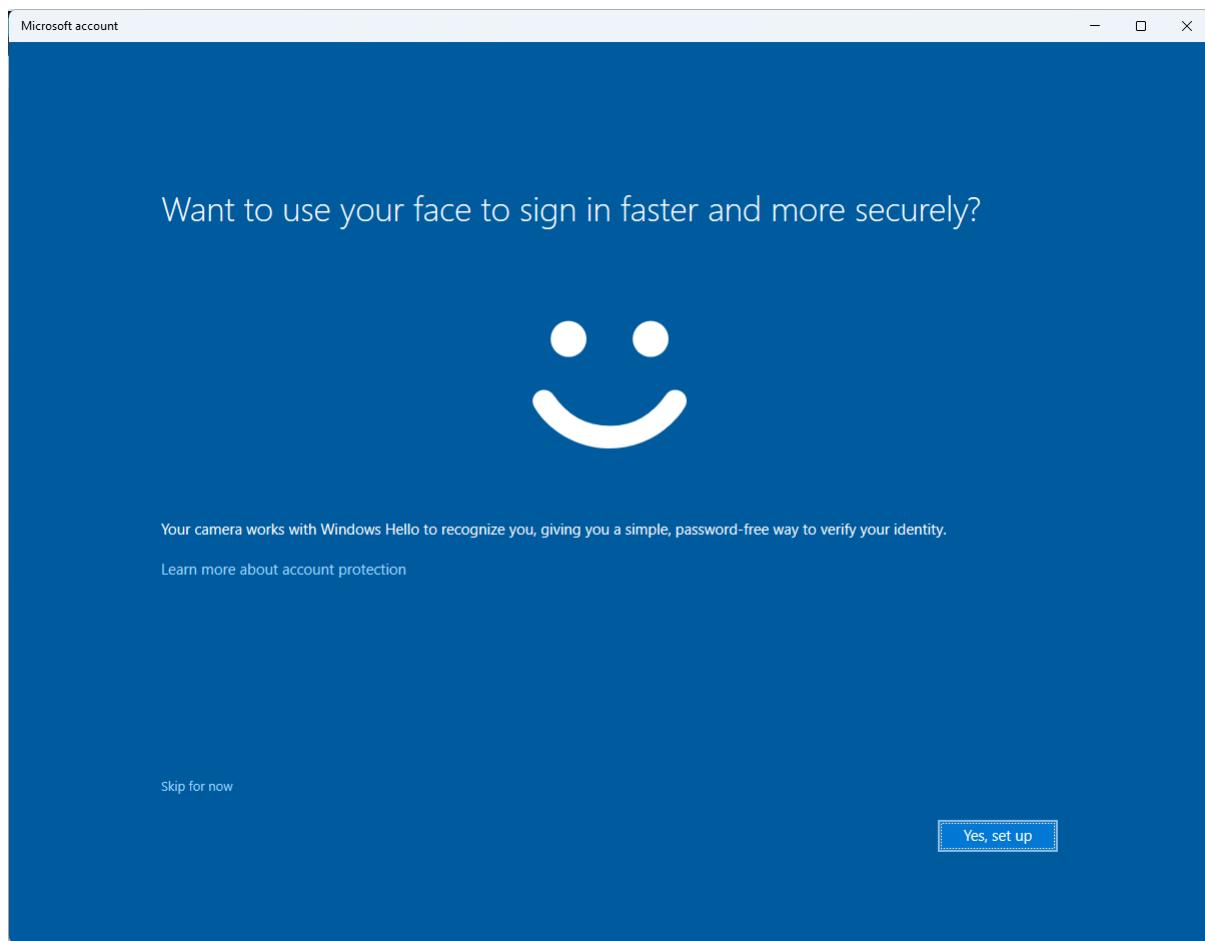


Figure 5.9 – Windows Hello for Business enrollment

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information (labadmin@M365w5204...). Below the navigation is a breadcrumb trail: Home > Contoso | Security > Security | Authentication methods > Authentication methods | Policies.

The main content area is titled "Authentication methods | Policies". It features a sidebar with "Manage" sections for "Policies", "Password protection", "Registration campaign", "Authentication strengths (Preview)", and "Settings". The "Monitoring" section includes "Activity", "User registration details", "Registration and reset events", and "Bulk operation results".

The central pane displays a policy configuration for "Manage migration". A note states: "Use this policy to configure the authentication methods your users may register and use. If a user is in scope for a method, they may use it to authenticate and for password reset (some methods aren't supported for some scenarios). [Learn more](#)". Another note says: "If your tenant doesn't yet use [combined security info registration](#), turn it on now – it's required to use this policy." A "Manage migration" button is present.

A table lists authentication methods:

Method	Target	Enabled
FIDO2 security key		No
Microsoft Authenticator		No
SMS		No
Temporary Access Pass		No

Figure 5.10 – Authentication methods

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information (labadmin@M365w5204...). Below the navigation is a breadcrumb trail: Home > Contoso | Security > Security | Authentication methods > Authentication methods | Policies > Microsoft Authenticator settings.

The main content area is titled "Microsoft Authenticator settings". It includes a note: "Number Matching will begin to be enabled for all users of the Microsoft Authenticator app starting 8th of May 2023. [Learn more](#)".

The configuration section has tabs for "Enable and Target" (selected) and "Configure". Under "Enable", the "Enable" switch is turned on. Under "Target", "Include" is selected, and "All users" is chosen. The "Configure" tab shows a table:

Name	Type	Registration	Authentication mode
All users	Group	Optional	Any

Figure 5.11 – Enabling Microsoft Authenticator

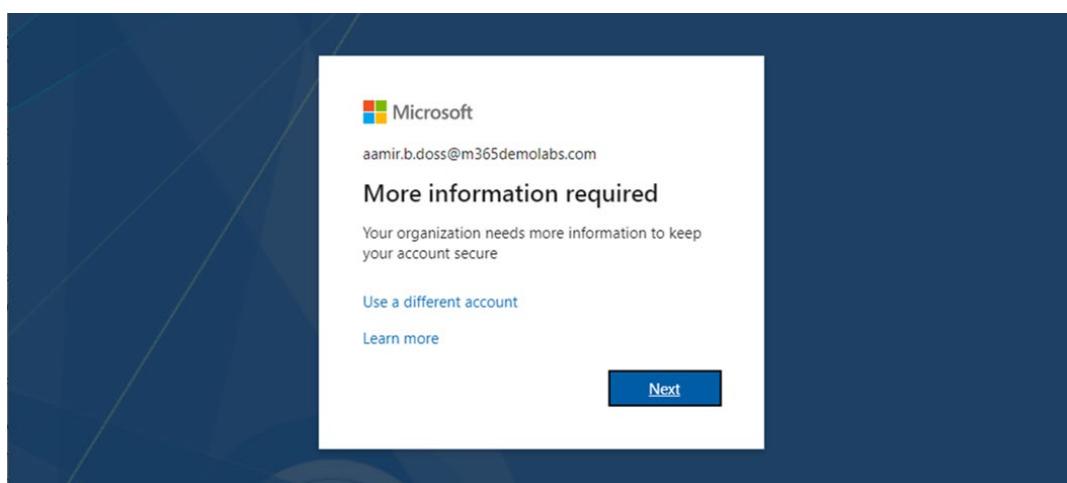


Figure 5.12 – More information required

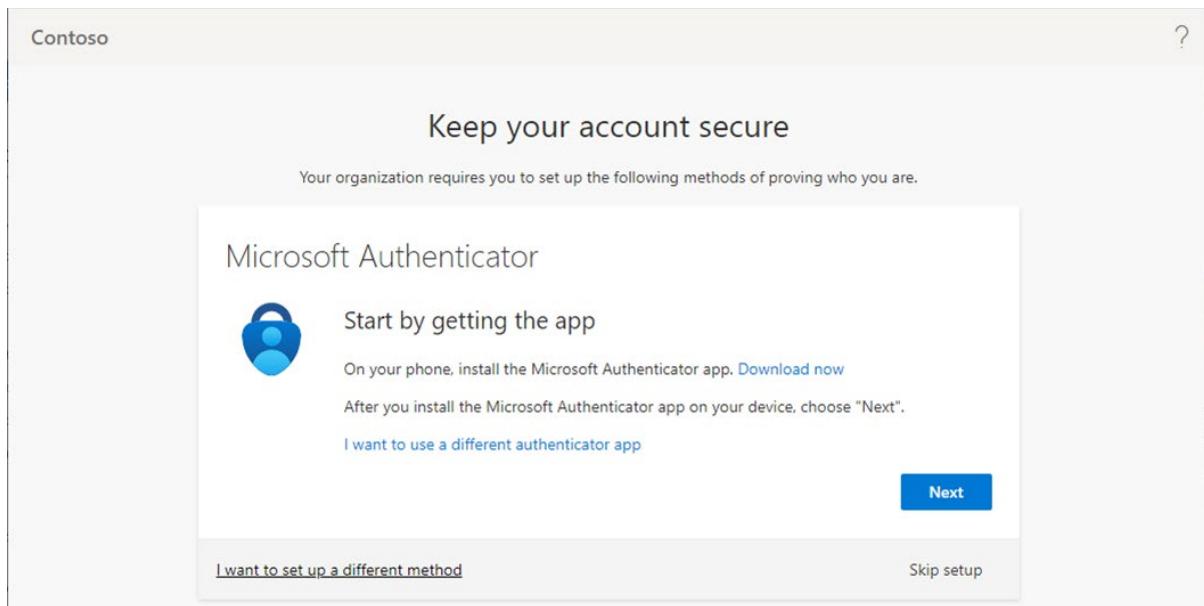


Figure 5.13 – Keep your account secure page

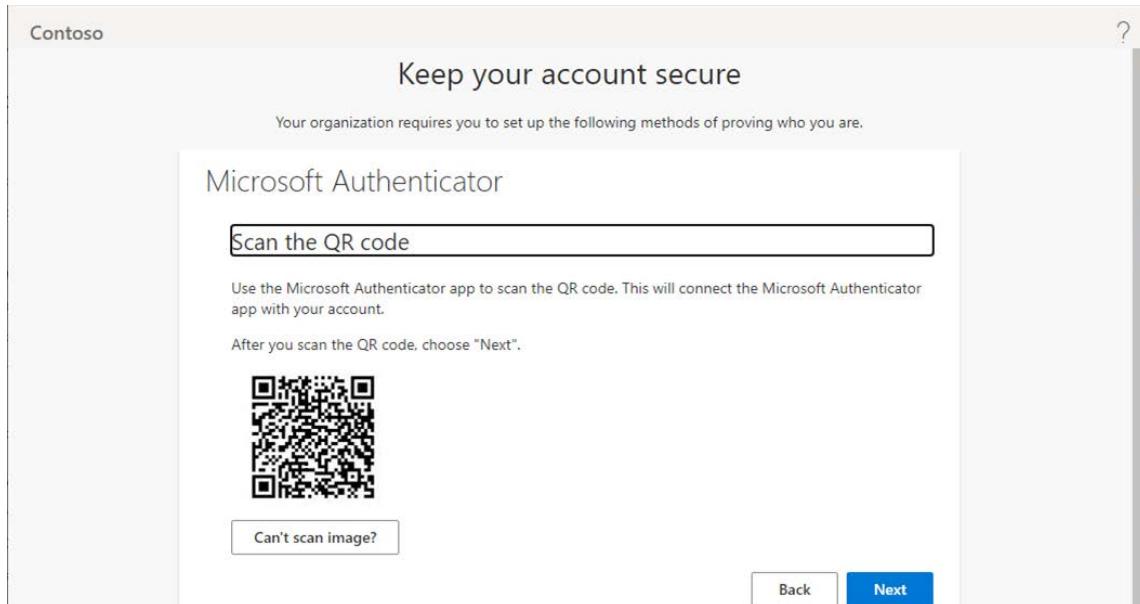


Figure 5.14 – Registering a device

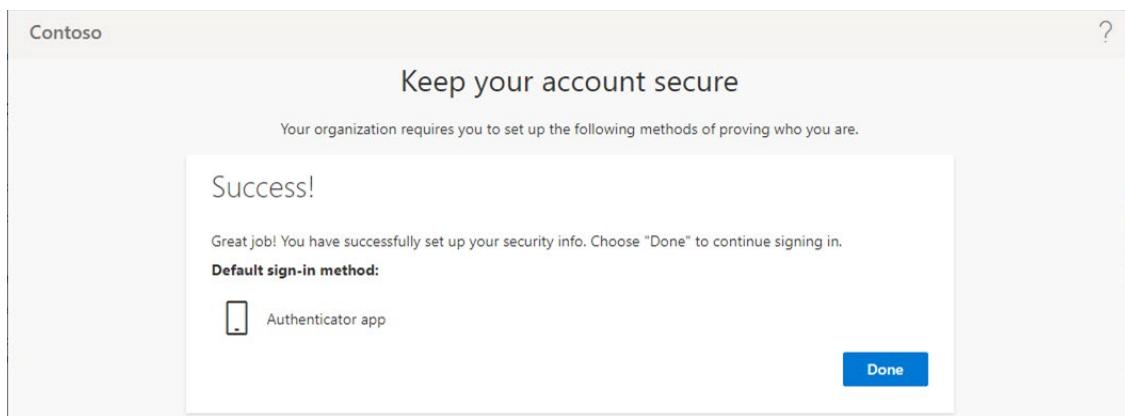


Figure 5.15 – Authenticator registration screen



Contoso

Aamir.B.Doss@m365demolabs.com



Notifications enabled

You can use this device to approve notifications to verify your sign-ins



One-time password code

920 809



Enable phone sign-in >



Change password >



Update security info >



Review recent activity >

Figure 5.16 – Microsoft Authenticator Enable phone sign-in

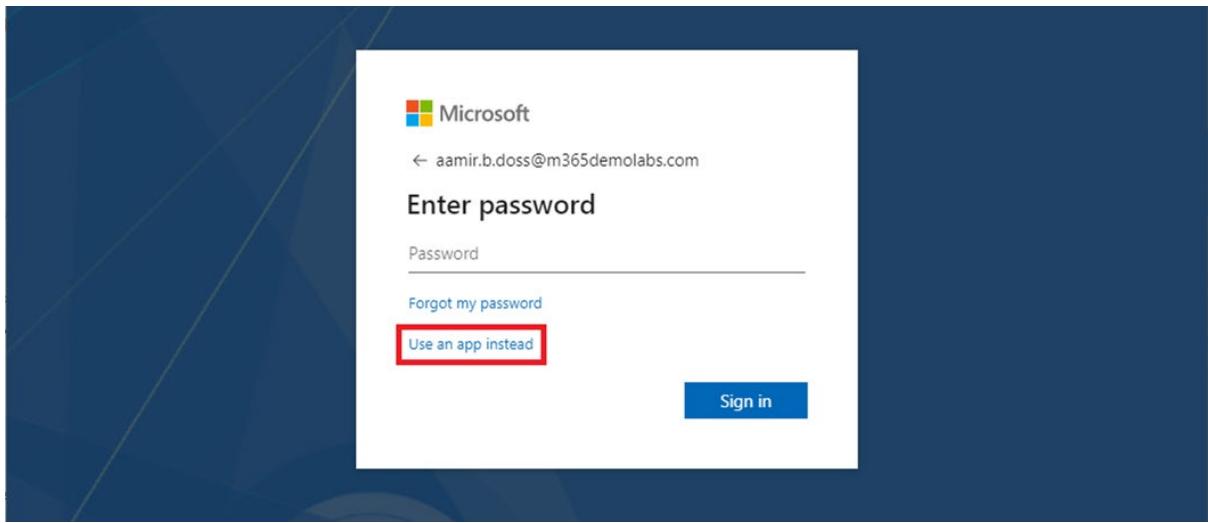


Figure 5.17 – Launching passwordless sign-in

A screenshot of the Microsoft Azure FIDO2 security key settings page. The URL is 'Home > Contoso | Security > Security | Authentication methods > Authentication methods | Policies > FIDO2 security key settings'. The page shows an 'Enable and Target' section with an 'Enable' toggle switch turned on, 'Include' selected, and 'All users' chosen as the target. A table below lists 'Name' (All users), 'Type' (Group), and 'Registration' (Optional).

Figure 5.18 – Enabling Microsoft Authenticator

A screenshot of the Microsoft 365 Home page. The top navigation bar includes 'Microsoft 365', a search bar, and user information for 'Contoso labadmin'. Below the navigation is a dashboard with various icons. On the left, there's a sidebar with 'Home', 'Create', and 'My Content' options. The main area shows a profile picture of 'labadmin' and links to 'View account' and 'My Microsoft 365 profile'.

Figure 5.19 – Accessing My account



Figure 5.20 – Sign in with Windows Hello or a security key

A screenshot of the Microsoft Azure portal. The URL bar shows "Microsoft Azure". The main navigation bar includes "Search resources, services, and docs (G+/-)" and various icons. The user is signed in as "labadmin@M365w5204... CONTOSO (M365WS20429.ONM...)". The page title is "Password reset | Properties". On the left, a sidebar titled "Manage" lists "Properties" (selected), "Authentication methods", "Registration", and "Notifications". The main content area shows a "Save" and "Discard" button. Under "Properties", the "Self service password reset enabled" section is expanded, showing three tabs: "None", "Selected", and "All" (highlighted). A note below the tabs states: "These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.".

Figure 5.21 – Enabling self-service password reset

The screenshot shows the 'Password reset | Authentication methods' page in the Microsoft Azure portal. On the left, a sidebar menu includes 'Diagnose and solve problems', 'Properties', 'Authentication methods' (which is selected), 'Registration', 'Notifications', 'Customization', 'On-premises integration', and 'Administrator Policy'. Under 'Authentication methods', there are sections for 'Methods available to users' (with checkboxes for 'Mobile app notification', 'Mobile app code' checked, 'Email', 'Mobile phone', 'Office phone', and 'Security questions'), 'Number of questions required to register' (set to 5), 'Number of questions required to reset' (set to 5), and a note 'Select security questions' with '11 security questions selected'. At the top right, there are 'Save' and 'Discard' buttons.

Figure 5.22 – Authentication methods

The screenshot shows the 'Password reset | On-premises integration' page in the Microsoft Azure portal. On the left, a sidebar menu includes 'Diagnose and solve problems', 'Properties', 'Authentication methods' (selected), 'Registration', 'Notifications', 'Customization', 'On-premises integration' (selected), and 'Administrator Policy'. A green notification bar at the top states 'We detected an agent has been configured. Password writeback can now be enabled'. In the main area, there are two sections: 'Azure AD Connect sync agent' (Status: Set up complete, View details) and 'Azure AD Connect provisioning agent (cloud sync)' (Status: Set up complete, View details). Below these are 'Manage settings' with checkboxes for 'Enable password write back for synced users' (checked), 'Write back passwords with Azure AD Connect cloud sync' (unchecked), and 'Allow users to unlock accounts without resetting their password?' (checked).

Figure 5.23 – On-premises integration

The screenshot shows the 'Authentication methods | Password protection' section in the Microsoft Azure portal. On the left, there's a navigation sidebar with 'Manage' and 'Monitoring' sections. Under 'Manage', 'Password protection' is selected. The main area contains several configuration options:

- Custom smart lockout:** Includes 'Lockout threshold' (set to 10) and 'Lockout duration in seconds' (set to 60).
- Custom banned passwords:** Shows a toggle switch set to 'Yes'.
- Password protection for Windows Server Active Directory:** Shows a toggle switch set to 'Yes'.
- Mode:** Shows a toggle switch set to 'Enforced'.

Figure 5.24 – Password protection

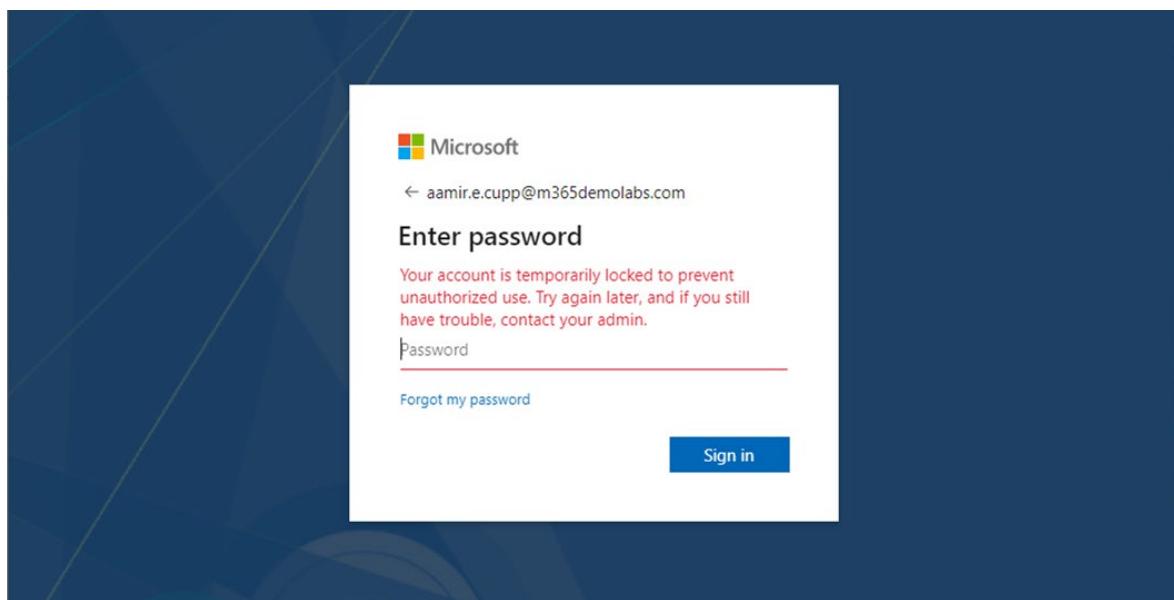


Figure 5.25 – Account lockout

The screenshot shows the 'Active users' page in the Microsoft 365 admin center. The top navigation bar includes 'Home > Active users' and a 'Dark mode' toggle. The main area has a header with 'Active users' and several action buttons: 'Add a user', 'User templates', 'Add multiple users', 'Multi-factor authentication', 'Filter', and 'Search active users list'. Below this is a table with columns: 'Display name ↑', 'Username', 'Sync status', and 'Licenses'. One user row is visible:

Display name ↑	Username	Sync status	Licenses
Aamir B Doss	Aamir.B.Doss@m365demolabs.com	Microsoft Teams Exploratory	

Figure 5.26 – Active users page

The screenshot shows the 'Multi-factor authentication' section under 'users service settings'. A 'bulk update' button is visible. The table lists six users with their display names, user names, and multi-factor auth status. Four users have checkboxes checked: Adrick G Porterfield, Cyndy M Reynoso, Kacie A Dupont, and Dionis X Sherry. A sidebar on the right shows '4 selected' and quick steps: Disable and Manage user settings.

DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
<input checked="" type="checkbox"/> Adrick G Porterfield	Adrick.G.Porterfield@m365demolabs.com	Enforced
<input type="checkbox"/> Townie M Laws	Townie.M.Laws@m365demolabs.com	Enabled
<input type="checkbox"/> Astra S Hough	Astra.S.Hough@m365demolabs.com	Enabled
<input checked="" type="checkbox"/> Cyndy M Reynoso	Cyndy.M.Reynoso@m365demolabs.com	Enforced
<input checked="" type="checkbox"/> Kacie A Dupont	Kacie.A.Dupont@m365demolabs.com	Enforced
<input checked="" type="checkbox"/> Dionis X Sherry	Dionis.X.Sherry@m365demolabs.com	Enforced

Figure 5.27 – Selecting users

The screenshot shows the 'Conditional Access | Policies' page in Microsoft Azure. The left sidebar includes 'Overview (Preview)', 'Policies' (selected), 'Insights and reporting', 'Diagnose and solve problems', and 'Manage' sections. The main area displays a table of policies with one entry: 'Exchange Online Requires Compliant Device'. A notification bar at the top right says 'IPv6 is coming to Azure Active Directory! Update Named locations today with IPv6 ranges.' A search bar and filter options are also present.

Policy Name ↑	State ↑↓	Creation Date ↑↓	Modified Date ↑↓
Exchange Online Requires Compliant Device	Off	1/21/2023, 7:17:04 PM	...

Figure 5.28 – Creating a new Conditional Access policy from a template

The screenshot shows the 'Create new policy from templates' page in the Microsoft Azure Conditional Access Policies section. At the top, there's a search bar and a navigation bar with 'labadmin@M365w5204...' and 'CONTOSO (M365WS20429.ONM...)'.

The main area has tabs for 'Select a template' (which is selected) and 'Review + Create'. A search bar is present above the template list.

The template list includes categories: 'Secure foundation', 'Zero Trust', 'Remote work', 'Protect administrator', 'Emerging threats', and 'All'. The 'Secure foundation' category is selected.

Two templates are visible:

- Require multifactor authentication for admins**: Described as securing privileged administrative accounts. It includes a link to 'Learn more'.
- Securing security info registration**: Described as securing user registration for Azure AD multifactor authentication. It includes a link to 'Learn more'.

Below these, two more templates are shown:

- Block legacy authentication**: Described as blocking legacy authentication endpoints. It includes a link to 'Learn more'.
- Require multifactor authentication for all users**: Described as requiring multifactor authentication for all user accounts. This option is selected.

At the bottom, there are buttons for 'Review + create' and navigation links 'Previous' and 'Next: Review + Create'.

Figure 5.29 – Selecting a template

The screenshot shows the 'Contoso | Sign-in logs' page in the Azure Active Directory section. At the top, there's a search bar and a navigation bar with 'labadmin@M365w5204...' and 'CONTOSO (M365WS20429.ONM...)'.

The left sidebar lists navigation options: Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, User settings, Properties, Security, Monitoring, Sign-in logs (which is selected and highlighted in grey), and Audit logs.

The main area displays sign-in logs. It includes a header with 'Date : Last 24 hours', 'Show dates as : Local', and 'Add filters'. A note says 'Want to switch back to the default sign-ins experience? Click here to leave the preview.' Below is a table of sign-in logs:

Date	Request ID	User	Application	Status	IP
3/27/2023, 4:18:57 AM	1fbcd15d2-da67-440f...	Aamir E Cupp	OfficeHome	Failure	17
3/27/2023, 4:18:40 AM	83ba05f7-abd9-4fb7...	Aamir E Cupp	OfficeHome	Failure	17
3/27/2023, 4:18:34 AM	7e8f5d47-0f91-4c7a...	Aamir E Cupp	OfficeHome	Failure	17
3/27/2023, 4:16:32 AM	00ffa02-7005-44e5...	labadmin	Azure Portal	Success	17

Figure 5.30 – Sign-in logs

The screenshot shows the 'Activity Details: Sign-ins' page in the Microsoft Azure portal. The left sidebar lists various Azure Active Directory features like Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, User settings, Properties, Security, Monitoring, and Sign-in logs. The 'Sign-in logs' option is selected. The main pane displays a table of activity details. A red box highlights the 'Failure reason' row, which contains the text 'Error validating credentials due to invalid username or password.' Another red box highlights the 'Additional Details' section, which states 'The user didn't enter the right credentials. It's expected to see some number of these errors in your logs due to users making mistakes.' Below this, user information is listed: User (Aamir E Cupp), Username (aamir.e.cupp@m365demolabs.com), and User ID (b6f53aad-cfe7-4d82-bc99-905535b184f5).

Date	3/27/2023, 4:19:38 AM
Request ID	29cbc9cc-11c5-41bb-8f58-5dee343ee600
Correlation ID	59896895-c7e4-46e0-bd3e-caabb434ccdf
Authentication requirement	Single-factor authentication
Status	Failure
Continuous access evaluation	No
Sign-in error code	50126
Failure reason	Error validating credentials due to invalid username or password.
Additional Details	The user didn't enter the right credentials. It's expected to see some number of these errors in your logs due to users making mistakes.
User	Aamir E Cupp
Username	aamir.e.cupp@m365demolabs.com
User ID	b6f53aad-cfe7-4d82-bc99-905535b184f5

Figure 5.31 – Activity details

The screenshot shows the 'Activity Details: Sign-ins' page in the Microsoft Azure portal. The left sidebar lists various Azure Active Directory features like Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, User settings, Properties, Security, Monitoring, and Sign-in logs. The 'Sign-in logs' option is selected. The main pane displays a table of activity details. A red box highlights the 'Failure reason' row, which contains the text 'The account is locked, you've tried to sign in too many times with an incorrect user ID or password.' Another red box highlights the 'Additional Details' section, which states 'This error can be returned for two reasons - the sign in could have come from a malicious IP address, or the account was locked due to repeated sign-in attempts. Only one error code is used to prevent an attacker from distinguishing between the states. In your Azure AD tenant, you can distinguish between these states by looking at the specific sign-in log entry for this request. For accounts locked for too many attempts, see <https://docs.microsoft.com/azure/active-directory/identity-protection/howto-unblock-user>' Below this, user information is listed: User (Aamir E Cupp), Username (aamir.e.cupp@m365demolabs.com), User ID (b6f53aad-cfe7-4d82-bc99-905535b184f5), Sign-in identifier (aamir.e.cupp@m365demolabs.com), and User type (Member).

Date	3/27/2023, 4:19:43 AM
Request ID	1fb15d2-da67-440f-96ad-99f9cb4f1701
Correlation ID	59896895-c7e4-46e0-bd3e-caabb434ccdf
Authentication requirement	Single-factor authentication
Status	Failure
Continuous access evaluation	No
Sign-in error code	50053
Failure reason	The account is locked, you've tried to sign in too many times with an incorrect user ID or password.
Additional Details	This error can be returned for two reasons - the sign in could have come from a malicious IP address, or the account was locked due to repeated sign-in attempts. Only one error code is used to prevent an attacker from distinguishing between the states. In your Azure AD tenant, you can distinguish between these states by looking at the specific sign-in log entry for this request. For accounts locked for too many attempts, see https://docs.microsoft.com/azure/active-directory/identity-protection/howto-unblock-user
User	Aamir E Cupp
Username	aamir.e.cupp@m365demolabs.com
User ID	b6f53aad-cfe7-4d82-bc99-905535b184f5
Sign-in identifier	aamir.e.cupp@m365demolabs.com
User type	Member

Figure 5.32 – Sign-in detail showing locked-out account

The screenshot shows the Microsoft Azure portal with the URL https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/SigninLogs. The user is signed in as labadmin@M365w5204... with the email address CONTOSO (M365W520429.ONM). The left sidebar shows the 'Contoso | Sign-in' section under 'Azure Active Directory'. The main content area is titled 'Activity Details: Sign-ins' and has tabs for 'Basic info', 'Location', 'Device info', 'Authentication Details' (which is selected), 'Conditional Access', and 'Report-only'. A table displays a single row of data:

Date	Authentication met...	Authentication met...	Succeeded	Result detail	Requirements
3/27/2023, 4:19:38 AM	Password	Password Hash Sync	false	Invalid username or p...	

Figure 5.33 – Authentication details

The screenshot shows the 'Practice Resources' section of the Microsoft 365 Administrator MS-102 Exam Guide. The top navigation bar includes 'DASHBOARD > CHAPTER 5', 'Practice Resources', and 'SHARE FEEDBACK'. The main content area is titled 'Implementing and Managing Authentication' and includes a 'Summary' section. The summary text states:

In this chapter, you learned how to evaluate passwordless sign-in options for your organization and deploy the ones that best suit your needs. Some passwordless options, such as Windows Hello or FIDO2 keys, may require specialized hardware such as cameras, USB devices, or fingerprint readers, while the Microsoft Authenticator app method requires only the Microsoft Authenticator app on any supported Android or iOS-based device.

You also learned about deploying features such as self-service password reset and Azure AD password protection to further reduce administrative overhead, helping your organization comply with security policies.

In the next chapter, you'll learn about implementing secure access in the context of Microsoft 365.

To the right, there is a 'Chapter Review Questions' section with the title 'The Microsoft 365 Administrator MS-102 Exam Guide by Aaron Guilmette'. It includes a 'Select Quiz' section with 'Quiz 1' and a 'START' button, and a 'SHOW QUIZ DETAILS' dropdown menu.

Figure 5.34 – Chapter Review Questions for Chapter 5

Chapter 6: Implementing and Managing Secure Access

The screenshot shows the Microsoft Azure Identity Protection interface. The left sidebar has 'Protect' and 'Report' sections. Under 'Report', 'Risky sign-ins' is selected. The main area displays a table of risky sign-in detections. The top of the table includes filters: 'Auto refresh: Off', 'Date: Last 1 month', 'Show dates as: Local', 'Risk state: 2 selected', 'Risk level (real-time): None Selected', 'Risk level (aggregate): None Selected', 'Detection type(s): None Selected', 'Sign-in Type: 2 selected', and a 'Add filters' button. A single row is shown in the table:

Date	User	IP address	Location	Risk state
3/13/2023, 6:48:52 PM	labadmin	172.58.123.48	Detroit, Michigan, US	At risk

A note at the bottom says: "Users can also have detections not linked to sign-in activity. To see all the detections, go to Risk detections."

Figure 6.1 – Identity protection reports

The screenshot shows the Microsoft Azure Identity Protection interface. The left sidebar has 'Protect' and 'Report' sections. Under 'Report', 'Risky users' is selected. The main area displays a table of risky user accounts. The top of the table includes filters: 'Learn more', 'Download', 'Select all', 'Confirm user(s) compromised', 'Dismiss user(s) risk', 'Auto refresh: Off', 'Show dates as: Local', 'Risk state: 2 selected', and 'Status: Active'. A 'User' column has an ascending sort arrow. A 'Risk level' column has a descending sort arrow. A 'Risk last updated' column has a descending sort arrow. Two rows are shown in the table:

User	Risk state	Risk level	Risk last updated
labadmin	At risk	Low	3/13/2023, 6:56:33 PM
MOD Administrator	At risk	Low	2/22/2023, 5:52:45 PM

Figure 6.2 – Risky users report

The screenshot shows the Microsoft Azure Identity Protection interface. The left sidebar has 'Protect' and 'Report' sections. Under 'Report', 'Risky sign-ins' is selected. The main area displays a table of risky sign-in detections. The top of the table includes tabs: 'User's sign-ins', 'User's risky sign-ins', 'User's risk detections', 'Reset password', 'Confirm user compromised', and buttons for 'Dismiss user risk', 'Block user', and 'Investigate with Microsoft 365 Defender'. The table has columns: Date, Activity, Actor, Risk state, and Risk history. Five rows are shown in the table:

Date	Activity	Actor	Risk state	Risk history
2/22/2023, 5:52:45 PM	Unfamiliar sign-in from... (redacted)	Azure AD	At risk	Low
1/23/2023, 6:33:53 PM	User performed secured... (redacted)	MOD Administrator	Remediated	-
1/23/2023, 12:15:33 PM	User performed secured... (redacted)	MOD Administrator	Remediated	-
1/22/2023, 11:40:09 AM	Password spray	Azure AD	At risk	High

Figure 6.3 – Risky User Details pane

Figure 6.4 – Risky Sign-in Details page

Figure 6.5 – User risk policy

The screenshot shows the Microsoft Azure Identity Protection interface. The left sidebar has a 'Protect' section with 'Sign-in risk policy' selected. The main area shows a policy named 'Sign-in risk remediation policy' assigned to 'All users' with the condition 'Sign-in risk: Low and above'. The controls set are 'Access' with 'Block access'. The policy enforcement status is 'Disabled'.

Identity Protection | Sign-in risk policy

Policy Name
Sign-in risk remediation policy

Assignments
Users
All users
Sign-in risk: Low and above

Controls
Access
Block access

Policy enforcement
Enabled **Disabled**

Figure 6.6 – Sign-in risk policy

The screenshot shows the Microsoft Azure Identity Protection interface. The left sidebar has a 'Protect' section with 'Multifactor authentication registration policy' selected. The main area shows a policy named 'Multifactor authentication registration policy' assigned to 'All users'. The control set is 'Require Azure AD multifactor authentication registration' which is checked.

Identity Protection | Multifactor authentication registration policy

Policy Name
Multifactor authentication registration policy

Assignments
Users
All users

Controls
 Require Azure AD multifactor authentication registration

Figure 6.7 – Multifactor authentication registration policy

The screenshot shows the Microsoft Azure Conditional Access Policies page. A modal window titled "Sign-in risk" is open on the right side. The main page displays a policy named "Require multifactor authentication for all users". The policy settings include:

- Name ***: Require multifactor authentication for all users...
- Assignments**:
 - Users**: All users included and specific users excluded
 - Cloud apps or actions**: All cloud apps
 - Conditions**: 0 conditions selected
- Enable policy**: Report-only (selected), On, Off

The "Sign-in risk" modal contains the following information:

- Control user access to respond to specific sign-in risk levels.** Learn more
- Configure**: Yes (selected), No
- Sign-in risk level is generated based on all real-time risk detections.**
- Select the sign-in risk level this policy will apply to**:
 - High
 - Medium
 - Low
 - No risk

Figure 6.8 – Migrating Identity Protection policies to Conditional Access

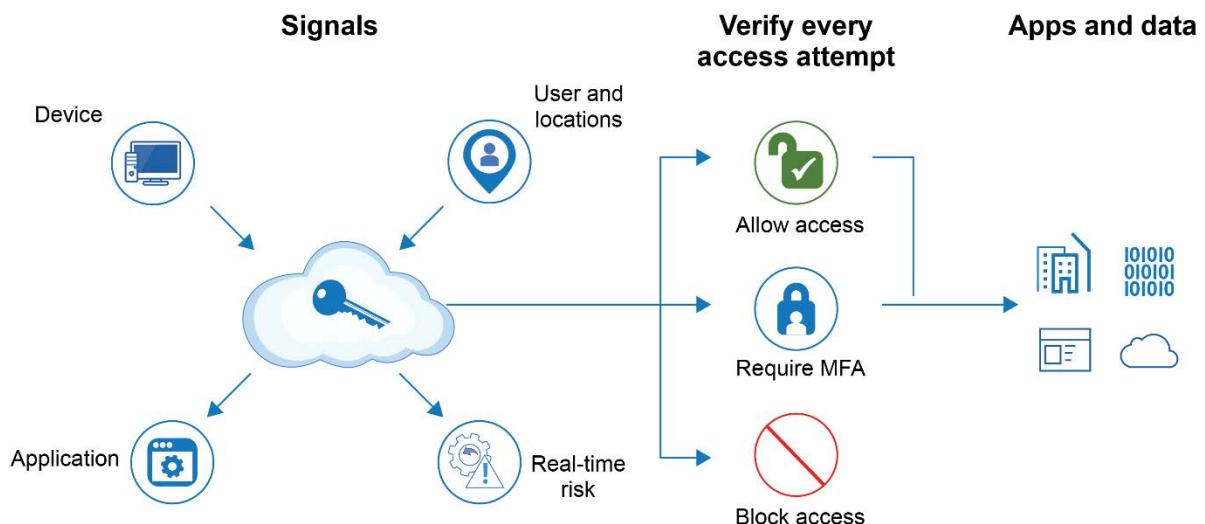


Figure 6.9 – Conditional Access signals

The screenshot shows the 'Conditional Access | Policies' section in the Microsoft Azure portal. A policy named 'Bypass MFA for Trusted Locations' is selected. The 'Assignments' section is expanded, showing 'Users' set to 'Specific users included' and 'Target resources' set to 'All cloud apps'. The 'Conditions' section shows '1 condition selected'. The 'Access controls' section is collapsed. On the right, the 'User assignments' tab is selected, showing the 'Include' tab is active. Under 'Include', 'Select users and groups' is chosen, and 'Users and groups' is checked. A list of '3 users' is shown. Below this, an 'Enable policy' section has 'Report-only' selected. A 'Save' button is at the bottom.

Figure 6.10 – Conditional Access policy user assignments

The screenshot shows the 'Conditional Access | Policies' section in the Microsoft Azure portal. The same policy 'Bypass MFA for Trusted Locations' is selected. The 'Assignments' section is expanded, showing 'Users' set to 'Specific users included' and 'Target resources' set to 'All cloud apps'. The 'Conditions' section shows '1 condition selected'. The 'Access controls' section is collapsed. On the right, the 'Target resources' tab is selected, showing a dropdown menu set to 'Cloud apps'. A warning message box is displayed, stating: '⚠️ Don't lock yourself out! This policy impacts the Azure portal. Before you continue, ensure that you or someone else will be able to get back into the portal. Disregard this warning if you are configuring persistent browser session policy that works correctly only if "All cloud apps" are selected.' A 'Learn more' link is provided. A 'Save' button is at the bottom.

Figure 6.11 – Conditional Access policy target resources assignments

The screenshot shows the Microsoft Azure Conditional Access Policies blade. A modal dialog titled 'Select' is open, listing various cloud applications. The 'Cloud apps' tab is selected. In the 'Selected items' section, four applications are listed: Office 365, Office 365 SharePoint Online, P2P Server, and SurveyMonkey Enterprise. Below the 'Selected items' section is a 'Select' button.

Bypass MFA for Trusted Locations

Name: Bypass MFA for Trusted Locations

Assignments:

Users: Specific users included

Target resources: No target resources selected

Conditions: 1 condition selected

Access controls:

Grant: Report-only

Save

Select

Cloud apps

PR ProvisioningPowerBi ea708463-7f80-4331-bb6d-bdd6d7128daf

SF Skype for Business Online 00000004-0000-0ff1-ce00-000000000000

SurveyMonkey Enterprise b7890659-1cb5-4f32-b95d-80b65fb59f98

Tenant Schema Extension App 7b2d3d08-b343-4261-8f04-251f9ba1494

Office 365

Office 365 SharePoint Online

P2P Server

SurveyMonkey Enterprise

Figure 6.12 – Conditional Access policy cloud apps

The screenshot shows the Microsoft Azure Conditional Access Policies blade. The 'Conditions' section is highlighted. It contains several configuration options: Device state (Not configured), User risk (Not configured), Sign-in risk (Not configured), Device platforms (Not configured), Locations (Any location and 1 excluded), Client apps (Not configured), and Filter for devices (Not configured). The 'Report-only' policy grant is also visible.

Bypass MFA for Trusted Locations

Name: Bypass MFA for Trusted Locations

Assignments:

Users: Specific users included

Target resources: All cloud apps

Conditions: 1 condition selected

Access controls:

Grant: Report-only

Save

Device state: Learn more

User risk: Not configured

Sign-in risk: Not configured

Device platforms: Not configured

Locations: Any location and 1 excluded

Client apps: Not configured

Filter for devices: Not configured

Figure 6.13 – Conditional Access policy conditions

The screenshot shows the Microsoft Azure Conditional Access Policies blade for a policy named "Bypass MFA for Trusted Locations". The left pane displays policy details and configuration sections for users, target resources, conditions, and access controls. The right pane is titled "Grant" and contains the following settings:

- Control access enforcement to block or grant access.** (Learn more)
- Grant access** (radio button selected)
- Require multifactor authentication** (checkbox checked)
 - Consider testing the new "Require authentication strength".** (Learn more)
- Require authentication strength** (checkbox unchecked)
 - "Require authentication strength" cannot be used with "Require multifactor authentication".** (Learn more)
- Require device to be marked as compliant** (checkbox unchecked)

A "Select" button is located at the bottom right of the "Grant" pane.

Figure 6.14 – Granting access control with the Conditional Access policy

The screenshot shows the Microsoft Azure Conditional Access Policies blade for the same policy. The left pane is identical to Figure 6.14. The right pane is titled "Session" and contains the following settings:

- Control access based on session controls to enable limited experiences within specific cloud applications.** (Learn more)
- Use app enforced restrictions** (checkbox unchecked)
 - This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions.** (Learn more)
- Use Conditional Access App Control** (checkbox unchecked)
- Sign-in frequency** (checkbox unchecked)
- Persistent browser session** (checkbox unchecked)
- Customize continuous access evaluation** (checkbox unchecked)
- Disable resilience defaults** (checkbox unchecked)
- Require token protection for sign-in sessions (Preview)** (checkbox unchecked)

A "Select" button is located at the bottom right of the "Session" pane.

Figure 6.15 – Conditional Access policy session controls

The screenshot shows the Microsoft Azure Conditional Access Policies page. In the top navigation bar, there is a search bar with placeholder text "Search resources, services, and docs (G+/-)" and several icons for account management and help. The user's email address "labadmin@M365w5204..." and the name "CONTOSO (M365WS20429.ONM...)" are displayed. On the left, a sidebar menu includes "Home > Conditional Access", "Conditional Access | Policies", "Azure Active Directory", "Overview (Preview)", "Policies" (which is selected), "Insights and reporting", "Diagnose and solve problems", "Manage", and "Named locations". The main content area has a banner stating "IPv6 is coming to Azure Active Directory! Update Named locations today with IPv6 ranges." Below this is a search bar with placeholder "Search policies" and a "Add filters" button. A table lists three policies: "Exchange Online Requires Compliant Device" (State: Off, Creation Date: 1/21/2023, Modified Date: 1/21/2023). The table has columns for Policy Name, State, Creation Date, and Modified Date.

Figure 6.16 – Creating a new Conditional Access policy from a template

The screenshot shows the "Create new policy from templates" wizard. The title bar says "Create new policy from templates". The top navigation bar is identical to Figure 6.16. The left sidebar shows "Home > Conditional Access | Policies". The main content area has a "Select a template" section with a "Review + Create" link. Below it is a search bar. A horizontal navigation bar includes "Secure foundation", "Zero Trust", "Remote work", "Protect administrator", "Emerging threats", and "All". There are four template cards: 1. "Require multifactor authentication for admins": Describes requiring MFA for privileged admin accounts. It has a "View" and "Download JSON file (Preview)" link. 2. "Securing security info registration": Describes securing user registration for Azure AD MFA. It has a "View" and "Download JSON file (Preview)" link. 3. "Block legacy authentication": Describes blocking legacy authentication endpoints. It has a "View" and "Download JSON file (Preview)" link. 4. "Require multifactor authentication for all users": Described as requiring MFA for all user accounts. It has a "View" and "Download JSON file (Preview)" link. The fourth template is selected, indicated by a blue circle. At the bottom are "Review + create", "Previous", and "Next: Review + Create >" buttons.

Figure 6.17 – Selecting a template

The screenshot shows the Microsoft Entra admin center Diagnostic settings page. The left sidebar includes sections like Identity governance, External Identities, User experiences, Hybrid management, Monitoring & health, Protection, Identity governance, Verifiable credentials, Permissions Management, Global Secure Access (Preview), and Learn & support. The main content area is titled "Diagnostic settings | General" under "M365 Demo Labs". It displays a table of diagnostic settings with columns for Name, Storage account, Event hub, and Log Analytic. A note states "No diagnostic settings defined". Below this is a section titled "Click 'Add Diagnostic setting' above to configure the collection of the following data:" followed by a list of log categories.

Name	Storage account	Event hub	Log Analytic
No diagnostic settings defined			

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- AuditLogs
- SignInLogs
- NonInteractiveUserSignInLogs
- ServicePrincipalSignInLogs
- ManagedIdentitySignInLogs
- ProvisioningLogs
- ADFSSignInLogs
- RiskyUsers
- UserRiskEvents
- NetworkAccessTrafficLogs
- RiskyServicePrincipals
- ServicePrincipalRiskEvents
- EnrichedOffice365Audits

Figure 6.18 – Entra ID Diagnostic settings page

The screenshot shows the Microsoft Entra admin center Diagnostic setting configuration page. The left sidebar has a navigation tree with Home, Diagnostic settings, General, and a star icon. The main content area is titled "Diagnostic setting" and shows a "Diagnostic setting name" input field with "Entra ID Logs". The "Logs" section lists various log categories with checkboxes: AuditLogs (unchecked), SignInLogs (checked), NonInteractiveUserSignInLogs (checked), ServicePrincipalSignInLogs (checked), ManagedIdentitySignInLogs (checked), ProvisioningLogs (unchecked), and ADFSSignInLogs (checked). The "Destination details" section contains four unchecked checkboxes: "Send to Log Analytics workspace", "Archive to a storage account", "Stream to an event hub", and "Send to partner solution". A "JSON View" link is located in the top right corner.

Figure 6.19 – Selecting log categories

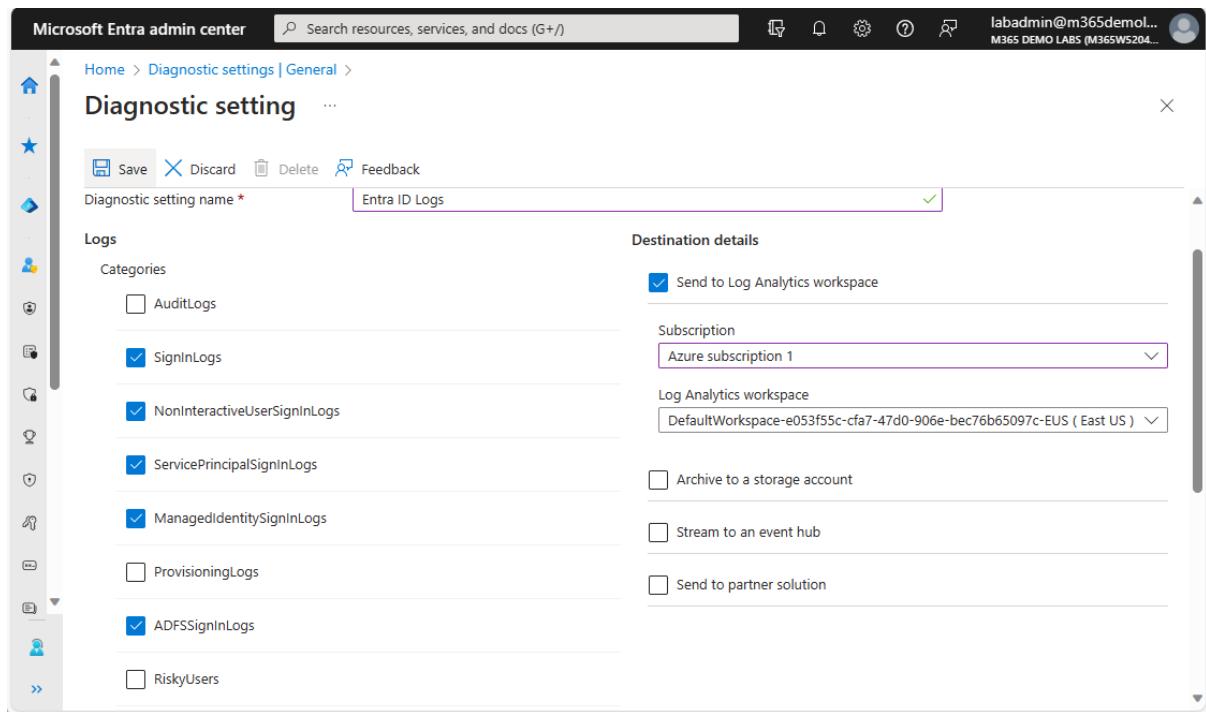


Figure 6.20 – Selecting the destination

Total: Number of users in the Last 24 hours
Success: Number of users where the selected policy(ies) granted access and the required controls were satisfied
Failure: Number of users where the selected policy(ies) denied access and the required controls were not satisfied
User action required: Number of users where the selected report-only policy applied but user action (e.g. MFA or Terms of Use) would be required if the policy were enabled.
Not applied: Number of users that are bypassing the selected policy(ies) because the sign-in did not match at least one of the

Figure 6.21 – Setting filters to display data

DASHBOARD > CHAPTER 6

Implementing and Managing Secure Access

Summary

In this chapter, you learned about Identity Protection features and Conditional Access policies. You also learned about Identity Protection features such as risk-based access policies and how to investigate and remediate risks.

In the next chapter, you will learn about configuring application access.

Chapter Review Questions

The Microsoft 365 Administrator MS-102 Exam Guide
by Aaron Guilmette

Select Quiz

Quiz 1

[SHOW QUIZ DETAILS](#) ▾

START

Figure 6.22 – Chapter Review Questions for Chapter 6

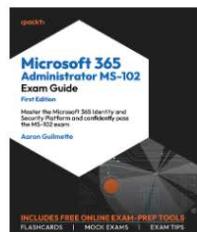
Chapter 7 : Managing Security Reports and Alerts by Using the Microsoft 365 Defender Portal

 Practice Resources

REPORT ISSUE

UNLOCK YOUR PRACTICE RESOURCES

You're about to unlock the free online content that came with your book. Make sure you have your book with you before you start, so that you can access the resources in minutes.



MS-102 Exam Guide First Edition

 Book ISBN: 9781835083963

Aaron Guilmette • Dec 2023 • pages

Do you have a Packt account?

Yes, I have an existing Packt account No, I don't have a Packt account

PROCEED

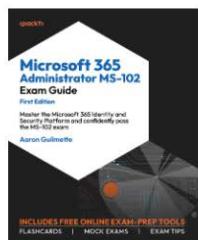
Figure 7.1 – Unlock page for MS-102 Exam Guide First Edition Practice Resources

 Practice Resources

REPORT ISSUE

UNLOCK YOUR PRACTICE RESOURCES

You're about to unlock the free online content that came with your book. Make sure you have your book with you before you start, so that you can access the resources in minutes.



MS-102 Exam Guide First Edition

 Book ISBN: 9781835083963

Aaron Guilmette • Dec 2023 • pages

ENTER YOUR PURCHASE DETAILS

Enter Unique Code *

E.g 123456789

 Where To Find This?

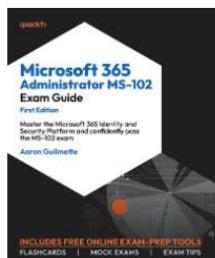
Check this box to receive emails from us about new features and promotions on our other certification books. You can opt out anytime.

REQUEST ACCESS

Figure 7.2 – Enter your unique sign-up code to unlock the resources

PACKT PRACTICE RESOURCES

You've just unlocked the free online content that came with your book.



MS-102 Exam Guide First Edition

 Book ISBN: 9781835083963

Aaron Guilmette • Dec 2023 • pages

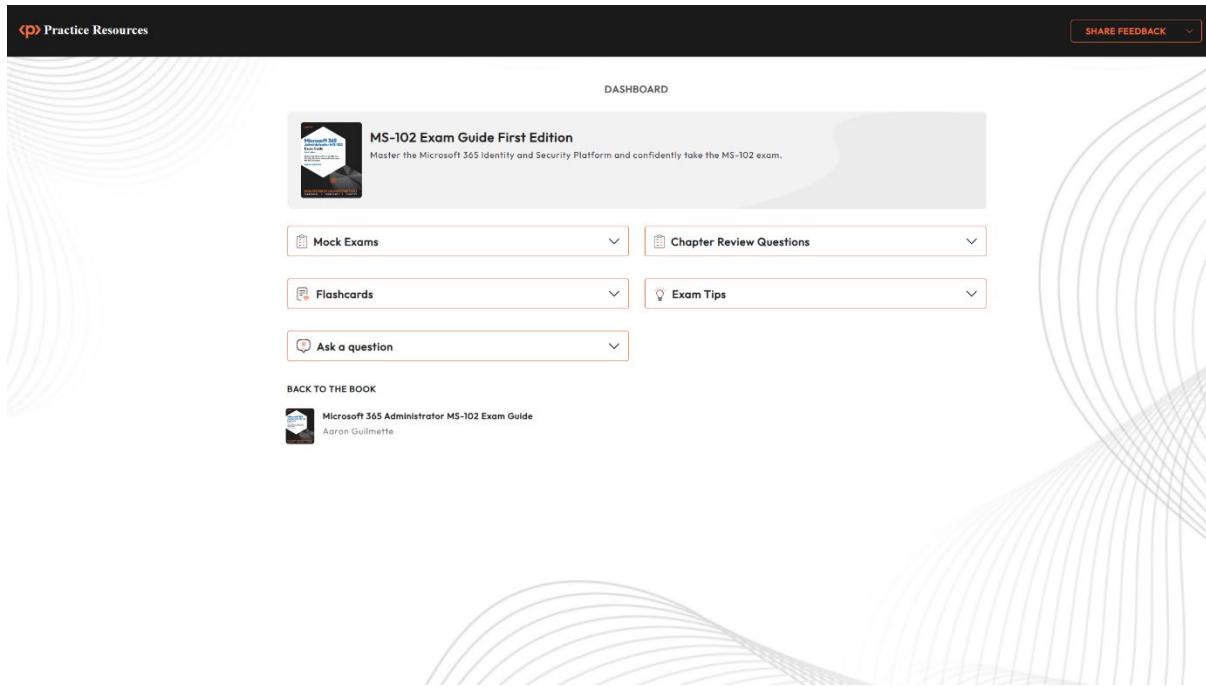
 **Unlock Successful**

Click the following link to access your practice resources at any time.

Pro Tip: You can switch seamlessly between the ebook version of the book and the practice resources. You'll find the ebook version of this title in your [Owned Content](#)

[OPEN PRACTICE RESOURCES](#) 

Figure 7.3 – Page that shows up when you've successfully unlocked the free online content



The dashboard page displays the following content:

- DASHBOARD** header with a **SHARE FEEDBACK** button.
- MS-102 Exam Guide First Edition** section:
 - Book cover thumbnail.
 - Description: "Master the Microsoft 365 Identity and Security Platform and confidently take the MS-102 exam."
- Resources:** A row of four dropdown menus:
 -  Mock Exams
 -  Chapter Review Questions
 -  Flashcards
 -  Exam Tips
- Ask a question:** A dropdown menu with an icon of a person talking.
- BACK TO THE BOOK** section:
 - Book cover thumbnail.
 - Book title: Microsoft 365 Administrator MS-102 Exam Guide
 - Author: Aaron Guilmette

Figure 7.4 – Dashboard page upon successful unlock of practice resources

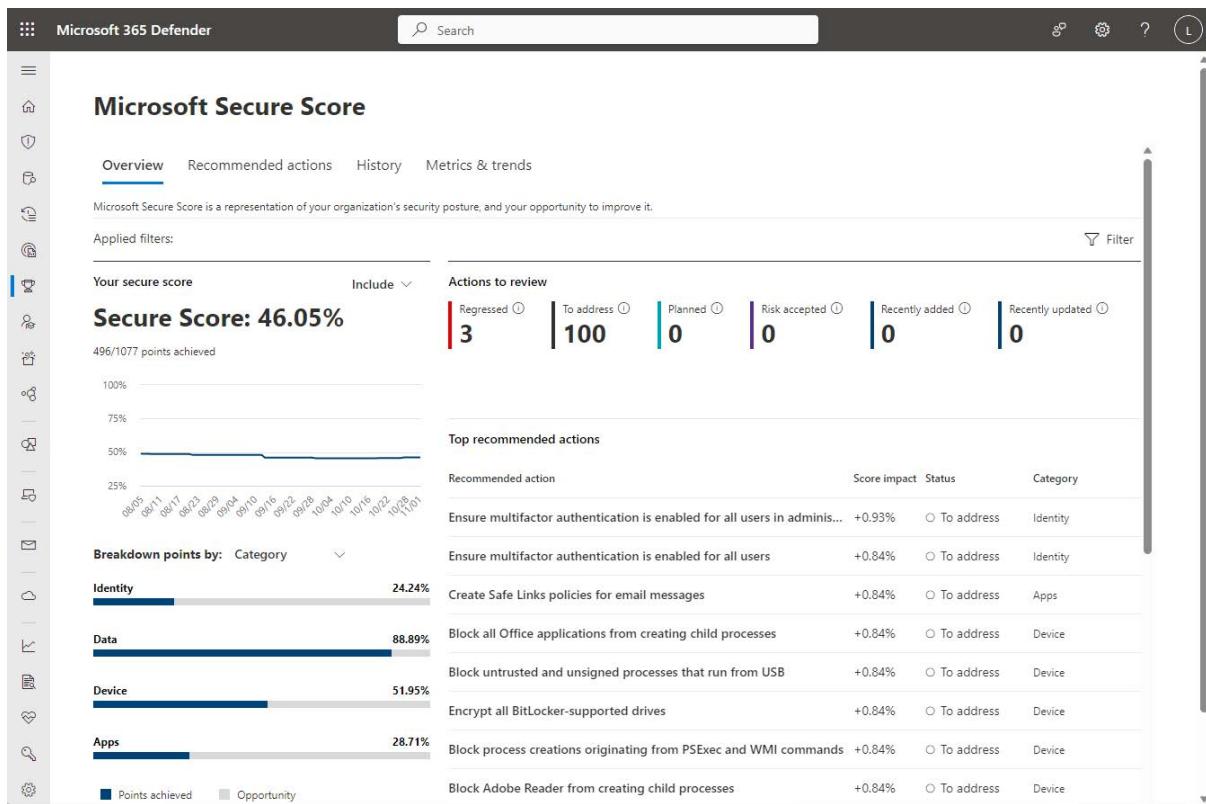


Figure 7.5 – Microsoft Secure Score

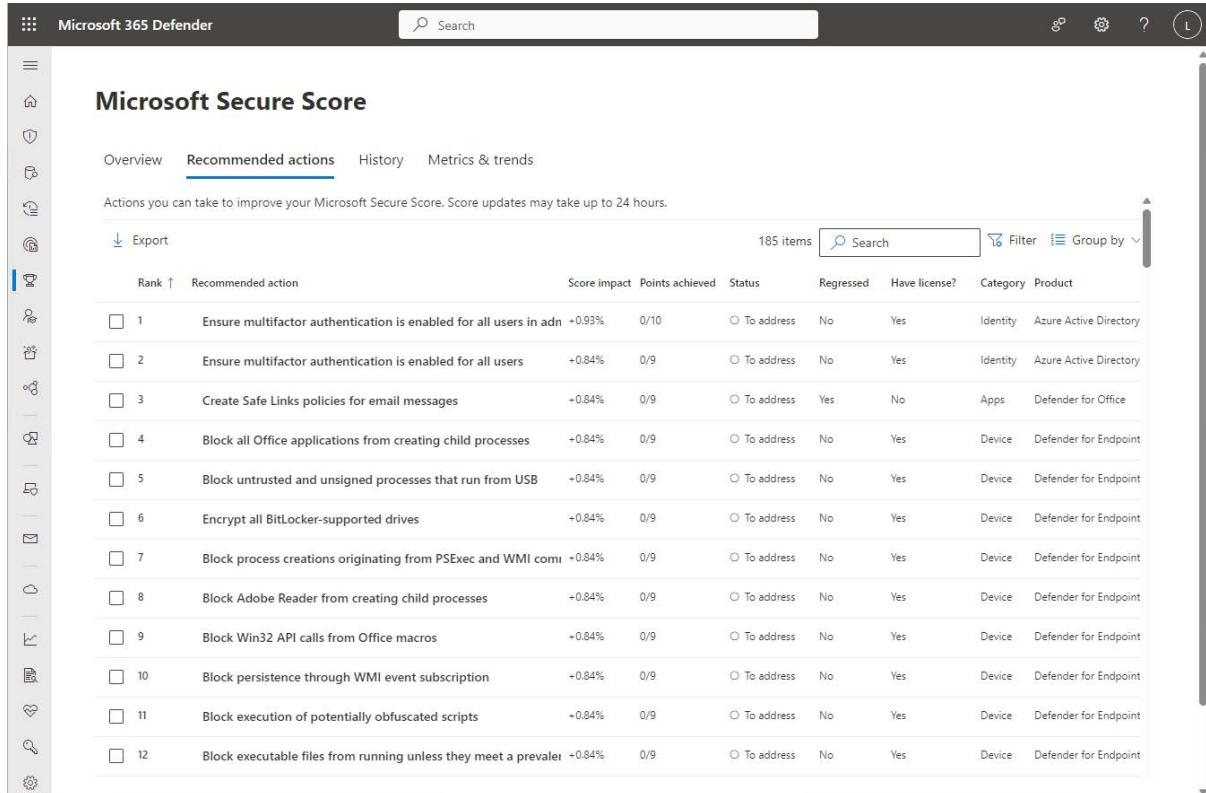


Figure 7.6 – Microsoft Secure Score improvement actions

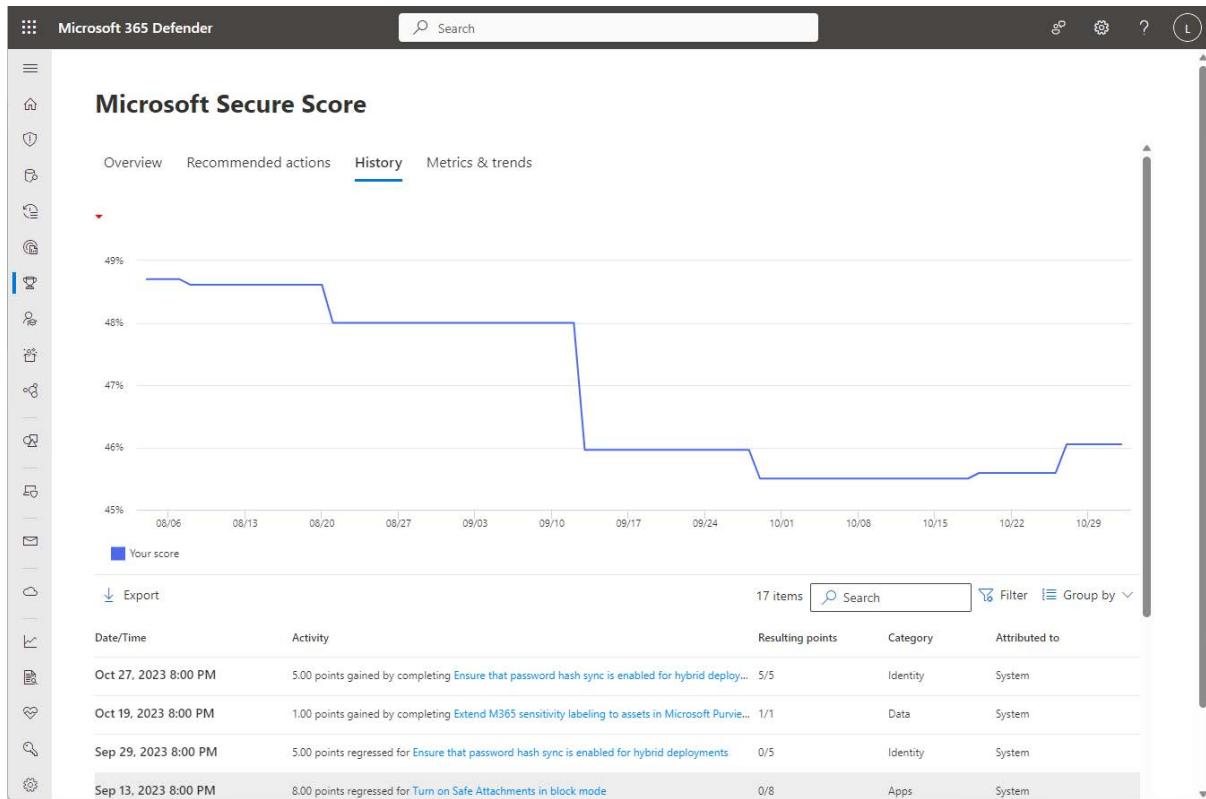


Figure 7.7 – Viewing the Secure Score history

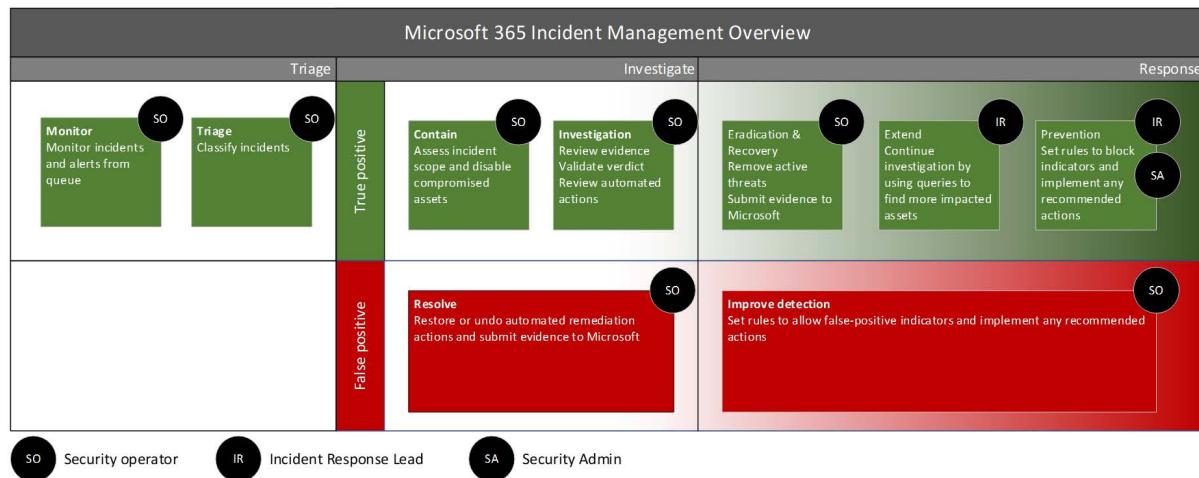


Figure 7.8 – The Microsoft 365 Incident Management phases

The screenshot shows the Microsoft 365 Defender portal's 'Alerts' page. The left sidebar includes sections for Home, Incidents & alerts (selected), Hunting, Actions & submissions, Threat intelligence, Secure score, Learning hub, Trials, Partner catalog, Assets, and Devices. The main content area is titled 'Alerts' and displays a table of 23 selected items. The table columns are: Alert name, Tags, Severity, Investigation state, Status, Category, Detection source, and Product. The first alert listed is 'Administrative acti...' with a severity of 'Informational' and status 'Remediated'. Other alerts include 'DLP policy (Privacy...)', 'Suspicious Process ...', and various suspicious activity entries.

Figure 7.09 – Viewing the Alerts page in the Microsoft 365 Defender portal

The screenshot shows the Microsoft 365 Defender portal's 'Incidents' page, specifically viewing a 'Multi-stage incident involving Defense evasion & Discovery on one endpoint'. The left sidebar lists various categories like Home, Incidents & alerts (selected), Hunting, Actions & submissions, Threat intelligence, Secure score, Learning hub, Trials, Partner catalog, Assets, Devices, and Identities. The main content area shows a detailed view of the incident, including an 'Attack story' tab with two active alerts: 'Suspicious Process Discovery' (resolved) and 'Attempt to stop Microsoft Defender for Endpoint sensor' (resolved). To the right, there are sections for 'Manage incident', 'RELATED THREATS' (Technique profile: Antivirus tampering, 0 impacted asset), and 'Incident details' (Assigned to labadmin@m365demolabs.com, Incident ID 12, Classification Not set, Categories Defense evasion, Discovery, First activity Aug 1, 2023 2:08:43 PM, Last activity Aug 1, 2023 2:13:18 PM).

Figure 7.10 – Reviewing an incident

The screenshot shows the Microsoft 365 Defender interface. The left sidebar has sections like Home, Incidents & alerts (selected), Hunting, Threat intelligence, Secure score, Learning hub, Trials, Partner catalog, Assets, Devices, Identities, Endpoints, and Configuration management. The main area shows an 'Incidents > Multi-stage incident involving Defense evasion & Discovery on one endpoint' page. At the top right are 'Manage incident' and 'Comments and history' buttons. Below is a navigation bar with 'Attack story' (selected), 'Alerts (2)', 'Assets (2)', 'Investigations (0)', 'Evidence and Response (6)', and 'Summary'. The 'Alerts' section shows 0/2 Active alerts. The 'Suspicious Process Discovery' alert (Aug 1, 2023 2:08 PM, Resolved) is highlighted. The 'Attack story' pane shows a timeline of process interactions:

- 8/1/2023 1:31:12 PM: [4] ntoskrnl.exe
- 1:31:13 PM: [428] smss.exe
- 1:50:36 PM: [2612] smss.exe 000000a4 0000000c
- 1:50:36 PM: [5204] winlogon.exe

The 'Incident graph' pane shows nodes for labadmin and win11-01, with 2/4 Processes associated.

Figure 7.11 – Reviewing the Incident graph as part of an Attack story

This screenshot is identical to Figure 7.11, showing the same 'Multi-stage incident involving Defense evasion & Discovery on one endpoint' page. The 'Attack story' tab is selected, and the 'Alerts' section shows the same timeline of process interactions. The 'Incident graph' pane also shows the same node connections between labadmin and win11-01.

Figure 7.12 – Reviewing an alert in the Attack story

The screenshot shows the Microsoft 365 Defender interface. On the left, the navigation pane includes sections like Home, Incidents & alerts (Incidents, Alerts, Email & collaboration alerts), Hunting, Actions & submissions, Threat intelligence, Secure score, Learning hub, Trials, Partner catalog, Assets (Devices, Identities), Endpoints, and Configuration management. The main area displays a "Multi-stage incident involving Defense evasion & Disruption" with a shield icon. Below it, tabs for Attack story, Alerts (2), Assets (2), and Investigations (0) are shown. Under the Alerts tab, an alert titled "Attempt to stop Microsoft Defender for Endpoint sensor" is selected. The alert details show it's Medium severity (red bar) and In progress. It has two entries: "Attempt to stop Mi..." and "Suspicious Process ...". The right side of the screen shows the "Details" tab with sections for INSIGHT (Quickly classify this alert, Classify alerts button), Alert state (Classification: Not Set, Assigned to labadmin@m365demolabs.com), Alert details (Set Classification, Unassign), and Evidence.

Figure 7.13 – Reviewing an alert’s details

The screenshot shows the Microsoft 365 Defender interface focusing on an investigation graph. The navigation pane is partially visible on the left. The main area shows an investigation for "Powershell dropped a suspicious file on the machine" with a shield icon. The title "PowerShell dropped a suspicious file on the machine" is at the top, along with a "Comments (0)" link. Below the title, a message says "Investigation #1 is complete - Some findings might require review". The investigation graph shows a central node connected to a "Device (1) WIN11-01" and other nodes representing entities analyzed (3083), evidence found (7 entities), and a result (Partially investigated, 2 entities remediated). Navigation tabs include Investigation graph, Alerts (4), Devices (1), Evidence (7), Entities (3.08k), and Log (133).

Figure 7.14 – Reviewing an investigation

The screenshot shows the Microsoft 365 Defender interface. In the center, there's a detailed view of a process named "powershell.exe" which is flagged as "Suspicious". The "Evidence and Response" tab is selected. On the left, there's a sidebar with various icons and a main content area titled "Multi-stage incident involving Initial ...". Below this title, there's a table showing "All evidence (22)" items, including URLs, Processes, IP Addresses, and Files. The "Processes" section lists several entries, with one entry for "powershell.exe" on Jul 5, 2023 at 7:47 PM being highlighted. The right side of the screen displays "Execution details" such as Process name [1484] powershell.exe, Execution time Jul 5, 2023 11:47:18 PM, Integrity level Token elevation, User system, and Command line powershell -ExecutionPolicy Unrestricted -File script0.ps1.

Figure 7.15 – Reviewing data on the Evidence and Response tab

The screenshot shows the Microsoft 365 Defender interface with the "Attack story" tab selected. The main content area displays a "Multi-stage incident involving Initial a..." with a user icon and a shield icon. Below this, there's a "View entity details" section with an "Incident graph" showing nodes for "win11-01" (a computer), "labadmin" (a user), and "204.79.197.203" (an IP address). The graph shows connections between these entities. To the right, there's a detailed view for the user "labadmin" with the status "Confirm user compromised". A dropdown menu is open, showing options like "Suspend user in Azure AD", "Require user to sign in again", "Azure AD account settings", and "View related incidents". Other sections visible include "User threat" (Open incidents 1, Active alerts 0, Azure AD No users), "Observed in organization" (Last Seen —, First Seen —, Lateral movement paths 0, Devices 0, Groups 0, Locations 0, Matched files 0, Accounts 2), and a "Close" button at the bottom.

Figure 7.16 – Taking action on a user in the Attack story

Microsoft 365 Defender

Incidents > Multi-stage incident involving Initial access & Lateral movement on one endpoint reported

Multi-stage incident involving Initial a...

win11-01
Internet facing Device value: Low All devices

Attack story Alerts (15) Assets (3) Investigations (1) Evidence and Response (22)

View entity details

Incident graph Layout Group similar nodes

win11-01 (3 Files, 204.79.197.203, 5 Processes, 2 Users)

Communication Association

Internet facing

This device is internet facing
This device was detected by ai

More details

Logged on users (last 30 days)

VM details

Domain

Report device inaccuracy
Run Antivirus Scan
Collect Investigation Package
Restrict App Execution
Initiate Automated Investigation
Isolate Device
Action center
Download force release from isolation script
Go hunt
Turn on troubleshooting mode
Policy sync

Close

Figure 7.17 – Responding to a problematic device

Microsoft 365 Defender

Incidents > Multi-stage incident involving Initial access & Lateral movement on one endpoint reported

Multi-stage incident involving Initial access & Lateral movement on one endpoint reported

Attack story Alerts (1)

View entity details

Not set

True positive

Multi staged attack

Malware

Malicious user activity

Unwanted software

Phishing

Compromised account

Other

Informational, expected activity

Security testing

Confirmed activity

Line of business application

Other

False positive

Not malicious

Not enough data to validate

Other

Communication Association

Manage incident

Incident name: Multi-stage incident involving Initial access & Lateral movement on one endpoint reported

Incident tags: SOC testing

Assign to: labadmin@m365demolabs.com

Status: Resolved

Classification: Informational, expected activity - Security testing

Comment: This was a sample incident created to test the response capabilities of Microsoft 365 Defender.

Save Cancel

Figure 7.18 – Updating incident details

The screenshot shows the Microsoft 365 Defender interface. On the left, there's a navigation sidebar with options like Home, Incidents & alerts, Hunting, Actions & submissions, Threat intelligence, Secure score, Learning hub, Trials, Partner catalog, Assets, Devices, and Identities. The main area is titled 'Incidents' and shows a table of recent incidents. The table has columns for First activity, Last activity, Data sensitivity, Status, Assigned to, Classification, and Determination. There are four rows of data:

	First activity	Last activity	Data sensitivity	Status	Assigned to	Classification	Determination
1	Aug 3, 2023 3:08 PM	Aug 3, 2023 3:08 PM	Not set	Active	labadmin@m365demolab	Not set	Not set
2	Aug 1, 2023 2:08 PM	Aug 1, 2023 2:13 PM	Not set	Active	labadmin@m365demolab	Not set	Not set
3	Jul 5, 2023 7:47 PM	Jul 6, 2023 3:06 PM	Benign	Active	labadmin@m365demolab	Positive	Security testing
4	Jul 5, 2023 6:39 PM	Jul 5, 2023 6:39 PM	Benign	Resolved	labadmin@m365demolab	Positive	Security testing

Figure 7.19 – Viewing assigned incidents

This screenshot shows the 'Manage incident' dialog box overlaid on the Microsoft 365 Defender interface. The main window displays an 'Administrative action' incident with one alert. The 'Alerts (1)' tab is selected. The right side of the dialog contains fields for 'Incident name' (set to 'Administrative action submitted by an Administrator'), 'Incident tags' (a text input field), 'Assign to' (set to 'labadmin@m365demolabs.com'), and 'Status' (set to 'Resolved'). Below these are buttons for 'Active', 'In Progress', and 'Resolved'.

Figure 7.20 – Updating an incident status

The screenshot shows the Microsoft 365 Defender interface. On the left, a navigation sidebar lists various security categories: Attack simulation, Policies & rules, Cloud apps, Cloud discovery, Cloud app catalog, OAuth apps, Files, Activity log, Governance log, Policies, Reports (which is selected), Audit, Health, Permissions, Settings, More resources, and Customize navigation. The main content area is titled "Reports" and displays a list of 19 items under two sections: "General (2)" and "Endpoints (8)".

Name	Description
Security report	View information about security trends and track the protection status of your identities, data, devices, apps, and infrastructure.
Query resources	Review how your hunting queries consume resources and understand how to prevent thr...
Threat protection	See details about the security detections and alerts in your organization.
Device health	Monitor device health, antivirus software status, operating system platform, and Windows...
Vulnerable devices	View information about the vulnerable devices in your organization, including their expos...
Monthly security summary	View a monthly executive report that shows a snapshot of your organization's protection ...
Web protection	Get information about the web activity and web threats detected within your organization.
Firewall	View connections blocked by your firewall including related devices, why they were block...
Device control	This report shows your organization's media usage data.
Attack surface reduction rules	View information about detections, misconfiguration, and suggested exclusions in your en...

Figure 7.21 – Viewing the available Microsoft 365 reports

The screenshot shows the Microsoft 365 Defender interface. The navigation sidebar is partially visible on the left. The main content area is titled "Identities". It features two main sections: "Users at risk" and "Global admins".

Users at risk: Displays "0 users at risk". A legend indicates risk levels: High Risk (red), Medium Risk (orange), and Low risk (grey). A "View all users" button is present.

Global admins: Displays "2 global admins". It includes a link to "Review users with global admin permissions" and a note: "Global admins have access to all your data and tools. Limiting the number of users with this role lowers the risk to your organization." A "Manage roles" button is present.

Figure 7.22 – Viewing the security report

The screenshot shows the Microsoft 365 Defender interface. The left sidebar includes icons for Home, Dashboard, All services, Devices, Apps, Endpoint security (selected), Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled "Web threat summary" and displays the message "0 Attempts to access malicious URLs". It includes a note: "It might take a while for web protection data to start coming in. To ensure you have web protection, deploy network protection using the Microsoft Defender for Endpoint security baseline." Below this, there are three tabs: "Details", "Indicators", and "Configure the security baseline".

Figure 7.23 – Viewing the web protection report

The screenshot shows the Microsoft Intune admin center. The left sidebar lists Home, Dashboard, All services, Devices, Apps, Endpoint security (selected), Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled "Create profile" and shows the "Configuration settings" tab selected. It includes sections for "Attack Surface Reduction Rules" with various configuration options like "Enable" or "Block" for different rules. At the bottom are "Previous" and "Next" buttons.

Figure 7.24 – Creating a baseline security policy

The screenshot shows the Microsoft 365 Defender interface. The left sidebar includes icons for Home, Dashboard, All services, Devices, Apps, Endpoint security (selected), Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled "Reports > Attack surface reduction rules". It shows a "Device configuration overview" with counts for different rule states: All exposed devices (0), Devices with rules not configured (0), Devices with rules in audit mode (0), Devices with rules in warn mode (0), and Devices with rules in block mode (1). Below this, a section titled "Identify and fix devices with limited protection due to missing prerequisites or misconfigured rules" includes a link to "Learn about prerequisites" and a search bar. A table at the bottom provides detailed information for one device, "win11-01".

Device	Overall configur...	Rules in block mode	Rules in audit mode	Rules in warn mode	Rules turned off	Rules not applicable	Unknown	Device ID
win11-01	Rules in block mode	11	0	0	5	0	0	7fe462ebf887358a...

Figure 7.25 – Viewing the Attack surface reduction rules overview

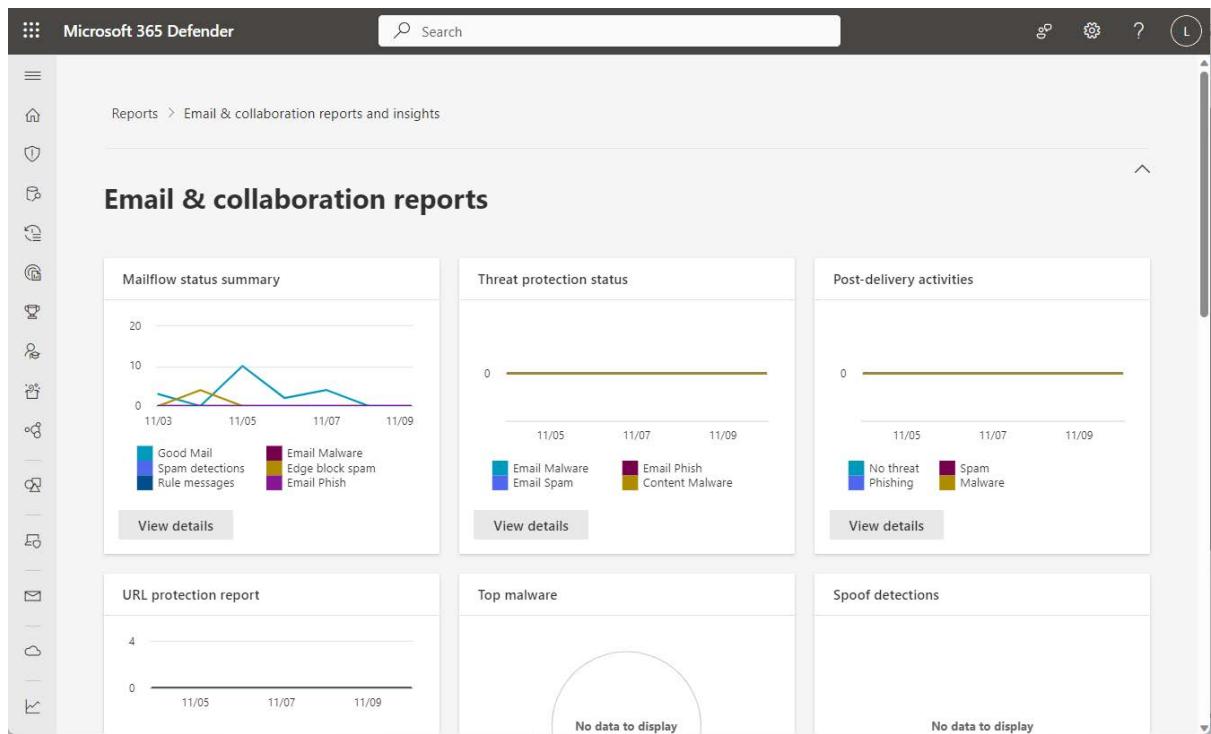


Figure 7.26 – Viewing the Email & collaboration reports dashboard

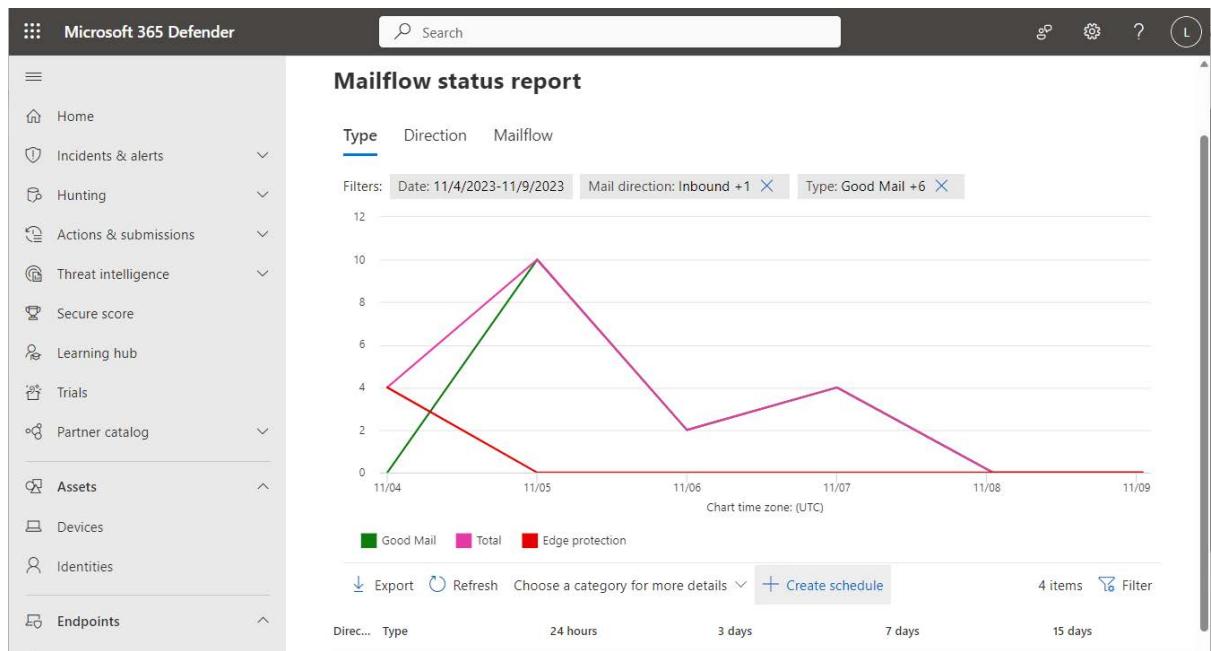


Figure 7.27 – Creating a scheduled Mailflow status report

The screenshot shows the Exchange admin center interface with the title "Mail flow reports". On the left, there's a navigation sidebar with various links like "Remote domains", "Accepted domains", "Connectors", etc. The main area displays a table of reports:

Name	Description
Auto forwarded messages report	Monitor for potential data leaks when people in your organization automatically forward email messages to an external domain, such as a personal email address.
Inbound messages report	Use this report to monitor message volume and TLS encryption for each connector. Mailflow between your Microsoft cloud organization, your on-premises email servers, and partner servers is often more important and you might want to apply extra security to these connections. Inbound includes messages from the internet and from on-premises organizations to Office 365.
Mail flow map report	View and learn the mail flow patterns to and from your Microsoft cloud organization, look for trends and anomalies, and fix issues.
Non-accepted domain report	This report shows messages from your on-premises organization where the sender's email domain isn't configured as an accepted domain in Office 365.
Non-delivery details report	Monitor messages that aren't getting delivered to the intended recipients. When a message can't be delivered, the sender gets an emailed non-delivery report (NDR) with an error code that indicates

Figure 7.28 – Viewing the Mailflow reports in the Exchange admin center

The screenshot shows the "Request an inbound message report" dialog. It includes a chart titled "Messages volume" showing a steady increase over time, and a table of "Connector report details" with four entries. The right side of the dialog contains form fields:

- Report name ***: Custom Report - ConnectorReport_Inbound - 11/10/2023
- Start date ***: 8/12/2023
- End date ***: 11/8/2023
- Recipients**: labadmin@m365demolabs.com
- Direction**: Received
- Connector type**: All, including no connector
- TLS version**: All, including no TLS

A large blue "Request" button is at the bottom.

Figure 7.29 – Requesting a custom report

The screenshot shows the Microsoft 365 Defender interface. The top navigation bar includes the Microsoft 365 Defender logo, a search bar, and various icons for settings and help. Below the navigation is a breadcrumb trail: Reports > Exported reports. The main title is "Exported reports". A table displays two reports:

Type	Description	Status	Generated on
Control	Policies overview report during 10/11/2023 - 11/1	Ready	Nov 10, 2023 11:25 AM
Control	Policies overview report during 11/03/2023 - 11/1	Ready	Nov 10, 2023 11:25 AM

At the bottom right of the table are download and more options buttons.

Figure 7.30 – Viewing the Cloud Apps' Exported reports page

The screenshot shows the Microsoft 365 Defender Threat analytics dashboard. The left sidebar contains navigation links: Home, Incidents & alerts, Hunting, Actions & submissions, Threat intelligence (selected), Threat analytics, Secure score, Learning hub, Trials, Partner catalog, Assets, Devices, Identities, Endpoints, and Vulnerability management. The main content area is titled "Threat analytics". It features a summary bar with counts for various threat types: Ransomware (54), Extortion (0), Phishing (43), Hands on keyboard (0), Activity group (111), Vulnerability (39), and Attack campaign (0). Below this is a section for "Tool or technique" with a count of 0. The dashboard is divided into three sections: "Latest threats", "High-impact threats", and "Highest exposure threats". Each section contains a list of items with threat names, counts, and severity indicators. At the bottom, there is a search bar, a summary of 200 items, and buttons for "Customize columns" and "Filter".

Figure 7.31 – Viewing the Threat analytics dashboard

The screenshot shows the Microsoft 365 Defender interface for viewing a threat's vulnerability profile. The top navigation bar includes 'Microsoft 365 Defender', a search bar, and various settings icons. The main content area is titled 'Threats > Activity profile: Midnight Blizzard targets diplomatic, NGOs, and humanitarian organizations in global spear phishing activity'. A note at the top states: 'Threat actor names are being updated in stages to align with the new Microsoft weather-themed naming taxonomy. Read [How Microsoft names threat actors](#) for details.' Below this, the 'Overview' tab is selected, followed by 'Analyst report', 'Related incidents', 'Impacted assets', 'Endpoints exposure', and 'Recommended actions'. The 'Analyst report' section contains several paragraphs of text detailing the threat, including updates from November 8, 2023, about the use of CVE-2023-38831 in RARLabs WinRAR. It also mentions the detection of VaporRage and EnvyScout malware. A link to 'Read the full analyst report' is provided. To the right, a 'Report details' sidebar lists the report type as 'Threat tags' (Phishing +1), attack campaigns, publication date (Aug 11, 2023), and last update (Nov 8, 2023). At the bottom left, there are links for 'Related incidents' and 'Alerts over time'. The bottom center displays a bold '0 active incidents' message.

Figure 7.32 – Viewing a threat’s vulnerability profile

This screenshot shows the Microsoft 365 Defender interface specifically for the 'Analyst report' tab of the threat profile. The layout is identical to Figure 7.32, with the 'Analyst report' tab now active. The main content area contains the detailed text from the Analyst report, including the November 8, 2023, update about the CVE-2023-38831 exploit. It also describes the spear-phishing emails sent to diplomatic entities, which instructed recipients to open attachments for details of a diplomatic car for sale. The report notes that these emails were diplomatic-themed and contained malicious ZIP files. A sample attachment is shown with the title 'DIPLOMATIC CAR FOR SALE' and details for a 'BMW | F10 5 Series Sedan 528i xDrive' car, listing a price of 28.000 EUR and a year of 2016. The rest of the interface, including the sidebar and report details, remains consistent with Figure 7.32.

Figure 7.33 – Reviewing the Analyst report

The screenshot shows the Microsoft 365 Defender interface. The top navigation bar includes 'Microsoft 365 Defender', a search bar, and various icons. The main content area is titled 'Threats > Activity profile: Midnight Blizzard targets diplomatic, NGOs, and humanitarian organizations in global spear phishing activity'. A note at the top states: 'Threat actor names are being updated in stages to align with the new Microsoft weather-themed naming taxonomy. Read [How Microsoft names threat actors](#) for details.' Below this, tabs for 'Overview', 'Analyst report' (which is selected), 'Related incidents', 'Impacted assets', 'Endpoints exposure', and 'Recommended actions' are visible. The 'Recommendations' section contains a list of mitigation steps:

- Use the latest [WinRAR version 6.23](#), which addresses CVE-2023-38831.
- Invest in advanced, anti-phishing solutions that monitor incoming emails and visited websites. [Microsoft Defender for Office 365](#) brings together incident and alert management across email, devices, and identities, centralizing investigations for threats in email. Organizations can also leverage web browsers that automatically [identify and block malicious websites](#), including those used in this phishing campaign.
- Run endpoint detection and response ([EDR in block mode](#)) so that Microsoft Defender for Endpoint can block malicious artifacts, even when your non-Microsoft antivirus does not detect the threat or when Microsoft Defender Antivirus is running in passive mode. EDR in block mode works behind the scenes to remediate malicious artifacts that are detected post-breach.
- Configure [investigation and remediation](#) in full automated mode to allow Microsoft Defender for Endpoint to take immediate action on alerts to resolve breaches, significantly reducing alert volume.
- Turn on [cloud-delivered protection](#) in Microsoft Defender Antivirus, or the equivalent for your antivirus product, to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block a majority of new and unknown variants.
- For organizations using Microsoft Teams, apply [security best practices for Microsoft Teams](#). Refer to the [security guide for Microsoft Teams](#).
 - Understand and select the [best access settings for external collaboration](#) for your organization.
 - [Specify trusted Microsoft 365 organizations](#) to define which external domains are allowed or blocked to chat and meet.

Figure 7.34 – Reviewing recommendations for non-Microsoft products in the Analyst report

The screenshot shows the Microsoft 365 Defender interface. The top navigation bar includes 'Microsoft 365 Defender', a search bar, and various icons. The main content area is titled 'Threats > Vulnerability profile: CVE-2023-4863 and CVE-2023-5217 vulnerabilities in WebP and libvpx'. A note at the top states: 'Threat actor names are being updated in stages to align with the new Microsoft weather-themed naming taxonomy. Read [How Microsoft names threat actors](#) for details.' Below this, tabs for 'Overview', 'Analyst report', 'Related incidents', 'Impacted assets', 'Endpoints exposure' (which is selected), and 'Recommended actions' are visible. The 'Exposure level' is shown as 76. The 'Vulnerability patching status' section indicates 1 vulnerable device, all of which are exposed. The 'Mitigation details' table provides a breakdown of affected products and components:

Vulnerabilities	Product/Component	Vulnerability IDs	Exposed devices
teams	libvpx	CVE-2023-4863, CVE-2023-5217	1
libvpx	libvpx	CVE-2023-5217	0
vlc-jack	vlc-jack	CVE-2023-5217	0

Figure 7.35 – Viewing the exposed endpoints

The screenshot shows the Microsoft 365 Defender interface. On the left, there's a navigation sidebar with sections like Vulnerability management, Configuration management, Email & collaboration, Investigations, Explorer, and Real-time detections. The main content area is titled 'Weaknesses' and displays a summary of vulnerabilities: 136 total, 6 Exploitable, 5 Critical, and 0 Zero-day. Below this, it shows 0 vulnerabilities with no security update and 0 with some updates. A search bar at the top right contains the query 'Exposed devices: Affects my organization'. The results table has columns for Name, Severity, CVSS, Related Software, Age, Published on, First detected, Updated on, Threats, and Exp... . Two items are listed:

Name	Severity	CVSS	Related Software	Age	Published on	First detected	Updated on	Threats	Exp...
CVE-2023-5217	High	8.8	Oracle Thunderbird (+ 65 more)	a month	Sep 26, 2023 ...	Nov 9, 2023 4...	Oct 24, 2023 ...	1	
CVE-2023-4863	High	8.8	Oracle Firefox (+ 115 more)	2 months	Sep 10, 2023 ...	Nov 9, 2023 4...	Oct 28, 2023 ...	1	

Figure 7.36 – Searching for the product related to the threat on the Endpoint exposures page

The screenshot shows the Microsoft 365 Defender interface. The left sidebar includes icons for Home, Threats, and Actor profiles. The main area is titled 'Actor profile: Octo Tempest' and includes a note about threat actor naming conventions. Below this, tabs for Overview, Analyst report, Related incidents, Impacted assets, Endpoints exposure, and Recommended actions are visible. The 'Recommended actions' tab is selected. A message encourages performing actions to address the threat. The results table has columns for Rank, Recommended action, Score impact, Points achieved, Status, Regressed, Have license?, Category, and Prod. Five items are listed:

Rank	Recommended action	Score impact	Points achieved	Status	Regressed	Have license?	Category	Prod
3	Use advanced protection against ransomware	+0.91%	0/9	<input type="radio"/> To address	No	Yes	Device	Defe
5	Block process creations originating from PSEXEC and WMI comr	+0.91%	0/9	<input type="radio"/> To address	No	Yes	Device	Defe
74	Block credential stealing from the Windows local security authc	+0.91%	9/9	<input checked="" type="radio"/> Completed	No	Yes	Device	Defe
99	Turn on Tamper Protection	+0.81%	8/8	<input checked="" type="radio"/> Completed	No	Yes	Device	Defe
171	Use least privileged administrative roles	+0.1%	1/1	<input checked="" type="radio"/> Completed	No	Yes	Identity	Azur

Figure 7.37 – Reviewing Recommended actions

DASHBOARD > CHAPTER 7

Managing Security Reports and Alerts by Using the Microsoft 365 Defender Portal

Summary

In this chapter, you learned about the Microsoft 365 Defender portal and some of the specific capabilities around incident and threat management. Using the insights from Secure Score and Vulnerability Management's recommendations, you can quickly build a list of high-impact actions that will dramatically improve your overall security posture and reduce threat exposure.

In the next chapter, you'll learn about the Microsoft 365 Defender for Office features, which are used to protect threats targeting the Microsoft 365 email and collaboration tools.

Chapter Review Questions

The Microsoft 365 Administrator MS-102 Exam Guide
by Aaron Guilmette

Select Quiz

Quiz 1

[SHOW QUIZ DETAILS](#) ▾

START

Figure 7.38 – Chapter Review Questions for Chapter 7

Chapter 8: Implementing and Managing Email and Collaboration Protection Using Microsoft Defender for Office 365

The screenshot shows the Microsoft 365 Defender interface. On the left, a sidebar lists various security features: Real-time detections, Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, Policies & rules (which is selected and highlighted in blue), and Cloud apps. The main content area is titled "Policies & rules" and contains a sub-section titled "Threat policies". A sub-instruction "Set up policies to manage devices, protect against threats, and receive alerts about various activities in your organization." is present, along with a "Learn more" link. Below this, there is a list of three items: "Threat policies", "Alert policy", and "Activity alerts". A "3 items" badge is located in the top right corner of the main content area.

Figure 8.1 – Navigating to Threat policies

The screenshot shows the "Threat policies" page under "Policies & rules". The left sidebar has a "Policies & rules > Threat policies" entry. The main content area is titled "Threat policies" and contains a "Templated policies" section with two items: "Preset Security Policies" (selected and highlighted in blue) and "Configuration analyzer". Below this is a "Policies" section with five items: "Anti-phishing", "Anti-spam", "Anti-malware", "Safe Attachments", and "Safe Links". Each item has a brief description and a small icon.

Figure 8.2 – Configuring preset security policies

The screenshot shows the "Preset security policies" page under "Threat policies". The left sidebar has a "Policies & rules > Threat policies > Preset security policies" entry. The main content area is divided into three sections: "Built-in protection" (represented by a shield icon), "Standard protection" (represented by a colorful globe icon), and "Strict protection" (represented by a padlock icon). Each section lists its features. A note states: "Note: Built-in protection is enabled only for paid Microsoft Defender for Office 365 tenants." A toggle switch indicates "Standard protection is off". Buttons for "Manage protection settings" are available for each section.

Figure 8.3 – Configuring Standard protection settings

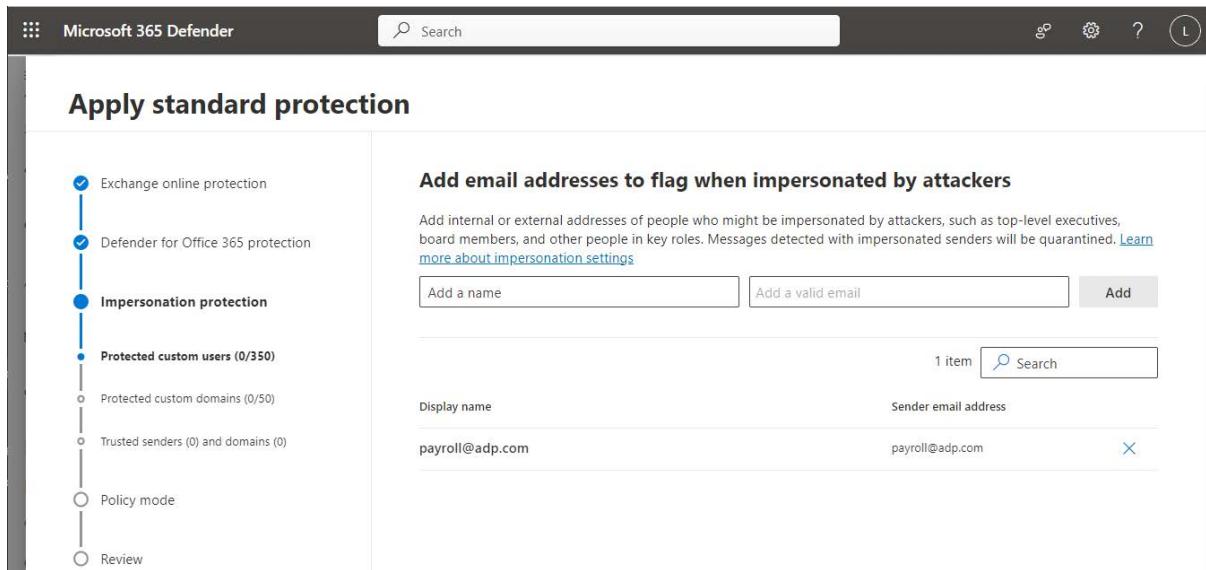


Figure 8.4 – Configuring impersonation settings

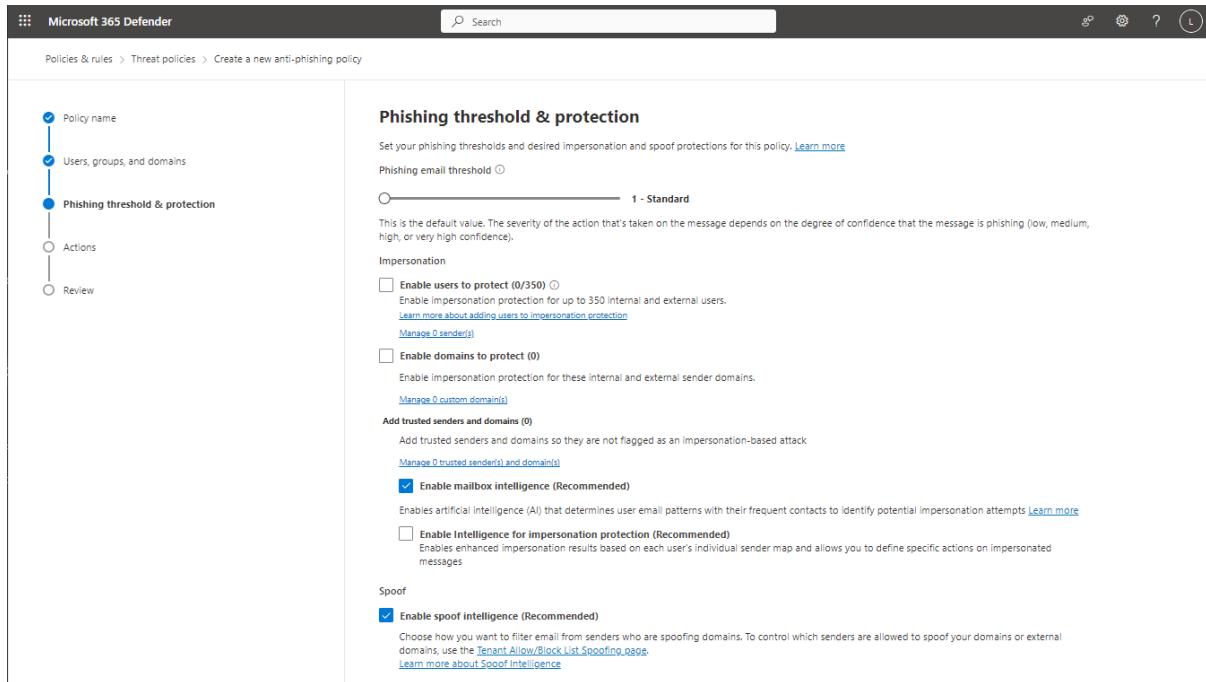


Figure 8.5 – Phishing threshold & protection page

The screenshot shows the Microsoft 365 Defender interface for creating a threat policy. On the left, a vertical navigation pane lists steps: Name your policy (checkmark), Users and domains (checkmark), Settings (checkmark), and Review (circle). The main content area is titled "Safe Attachments unknown malware response". It includes a warning about monitor and block actions, a section for selecting an action (Off, Monitor, Block, Dynamic Delivery), and a "Quarantine policy" dropdown set to "AdminOnlyAccessPolicy". Below that is a note about ignoring release requests for messages with detected malware. A "Redirect messages with detected attachments" section is present with a checkbox for "Enable redirect".

Figure 8.6 – Choosing Safe Attachments options

The screenshot shows an Outlook inbox with a message from "Office 365 Safe Attachments <noreply@office365.sa.microsoft.com>" titled "Safe Attachments Scan In Progress". The message body says "We're making sure your attachments are safe....." and contains a "Dynamic Delivery in Safe Attachments" section with instructions about scanning and previewing attachments. To the right, another message from "labadmin" is shown, with the subject "Safe Attachments Scan In Pr... Outlook Item" and the body "I've updated the file for deployment. Thanks!". Both messages have standard Outlook ribbon icons above them.

Figure 8.7 – Viewing a Safe Attachments message

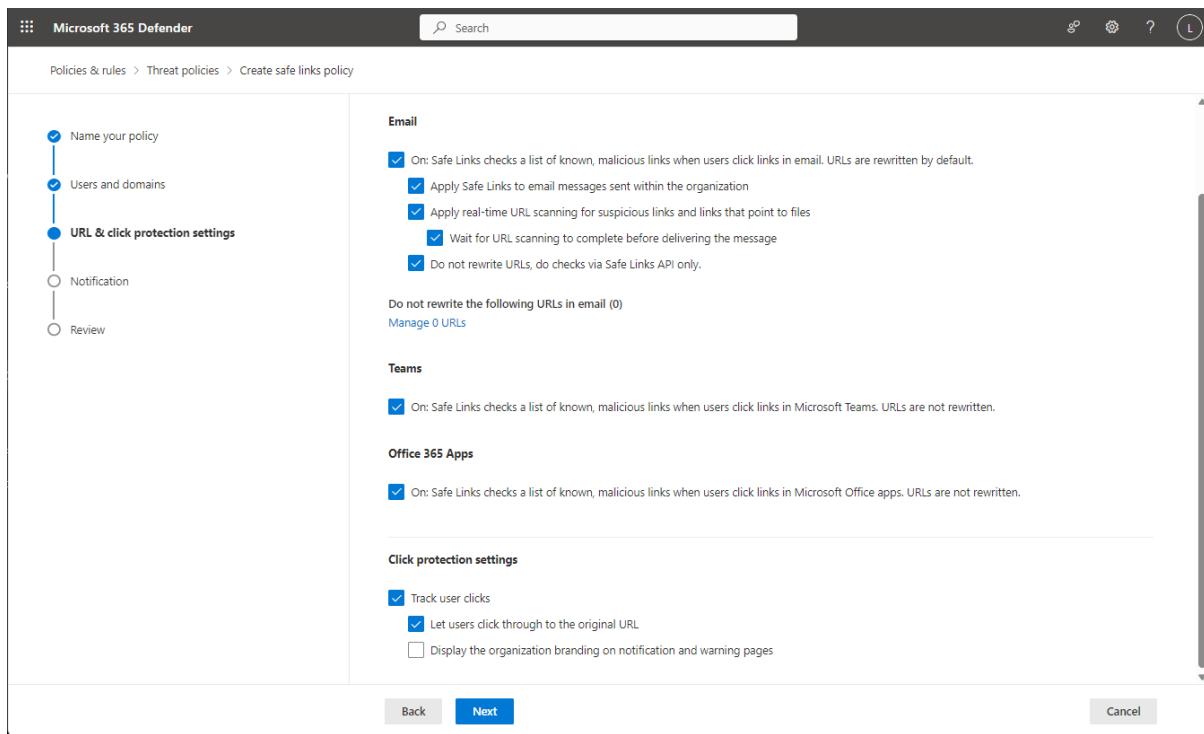


Figure 8.8 – Configuring a Safe Links policy

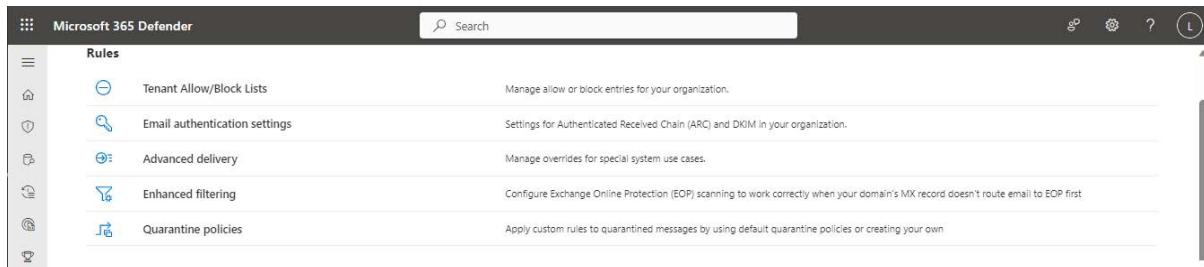


Figure 8.9 – Exchange Online Protection standard features

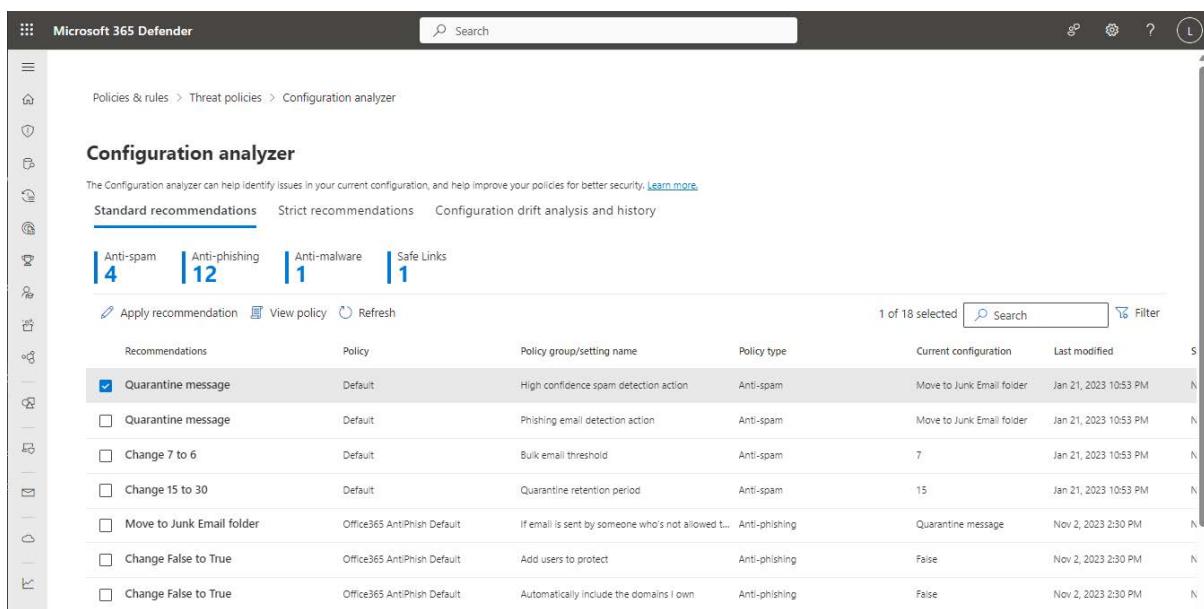


Figure 8.10 – Viewing the Configuration analyzer's recommendations

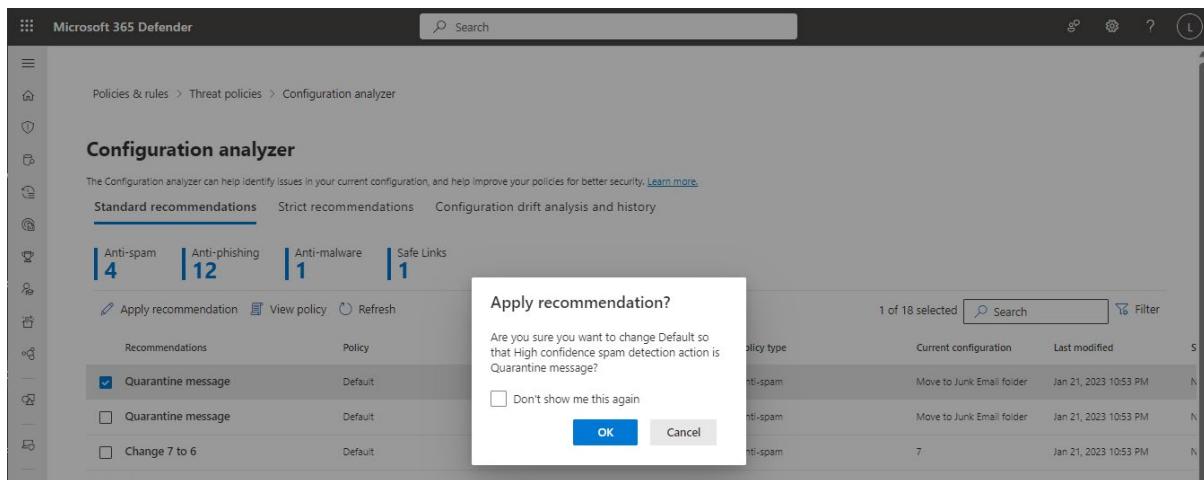


Figure 8.11 – Applying a Microsoft 365 Defender recommendation

The screenshot shows the 'View Alerts' page. The left sidebar includes 'Incidents & alerts' (selected), 'Email & collaboration alerts' (selected), 'Hunting', 'Actions & submissions', 'Threat intelligence', 'Secure score', 'Learning hub', 'Trials', 'Partner catalog', 'Assets', and 'Devices'. The main area displays a table of alerts with columns for Severity, Alert name, and Details. An alert for 'DLP-Low volume of content detected U.S. PII Enhanced' is selected, showing details like Date (Nov 10, 2023 5:25 PM), Category (Data loss prevention), Activity count (1), and Activity (DlpRuleMatch). The alert status is Active, with a comment 'New alert'.

Figure 8.12 – Viewing Email & collaboration alerts

The screenshot shows the 'Investigations' page. The left sidebar includes 'Configuration management', 'Email & collaboration' (selected), 'Investigations' (selected), 'Explorer', 'Review', 'Campaigns', 'Threat tracker', 'Exchange message trace', 'Attack simulation training', and 'Policies & rules'. The main area displays a table of investigations with columns for ID, Status, Detection, Investigation, Users, Creation Time, Last Changed, Threat confidence, Action count, and Duration. One investigation is listed: 'Mail with malicious file is zapped ...' by 'Office365'.

Figure 8.13 – Viewing the Investigations page

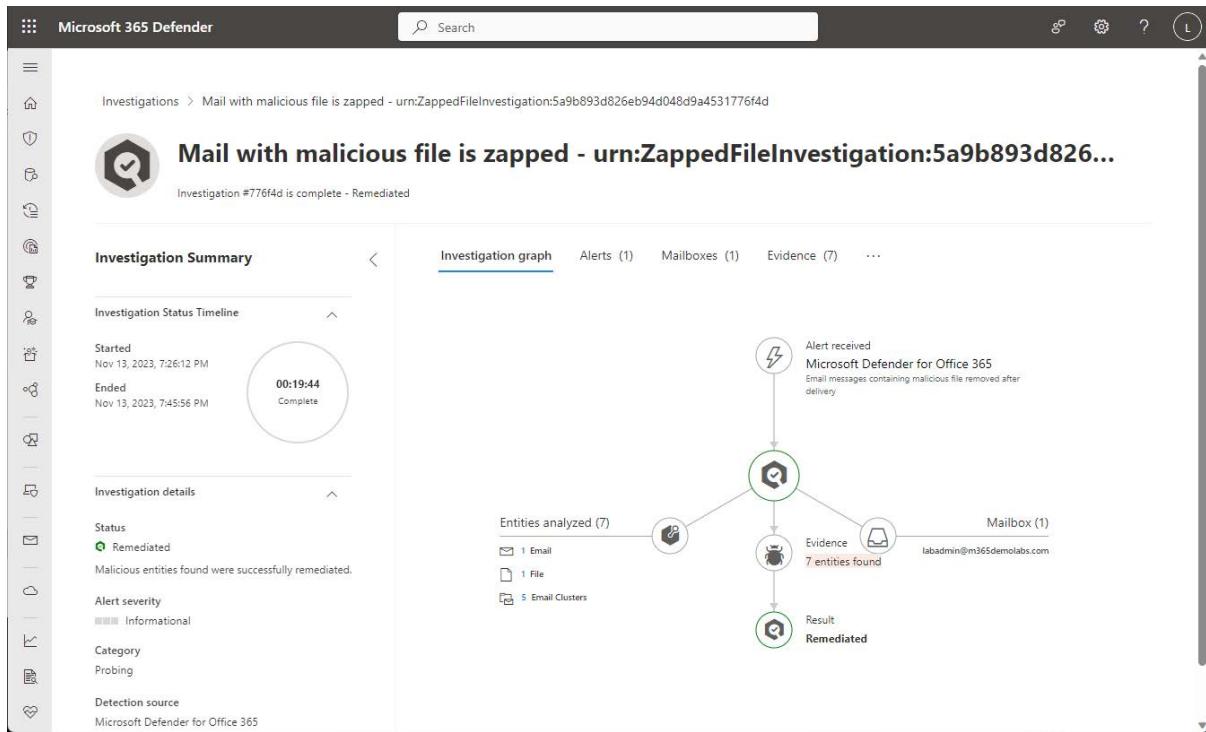


Figure 8.14 – Viewing the Investigation graph

The screenshot shows the Microsoft 365 Defender interface for the same investigation. The evidence tab is selected, displaying a list of suspicious entities. One entity, "DemoMalware.zip", is highlighted. A detailed view of this file is shown on the right side of the screen:

- File details:** DemoMalware.zip
- Actions:** Manage indicator, Add indicator, Manage in tenant block list.
- File verdict:** VirusTotal detection ratio 0/0, Malware detected None.
- Instance details:** Created (Nov 13, 2023, 7:26:12 PM), Device (not specified).
- File path:** DemoMalware.zip

The investigation summary on the left shows the investigation is complete and remediated.

Figure 8.15 – Reviewing actions for evidence in an investigation

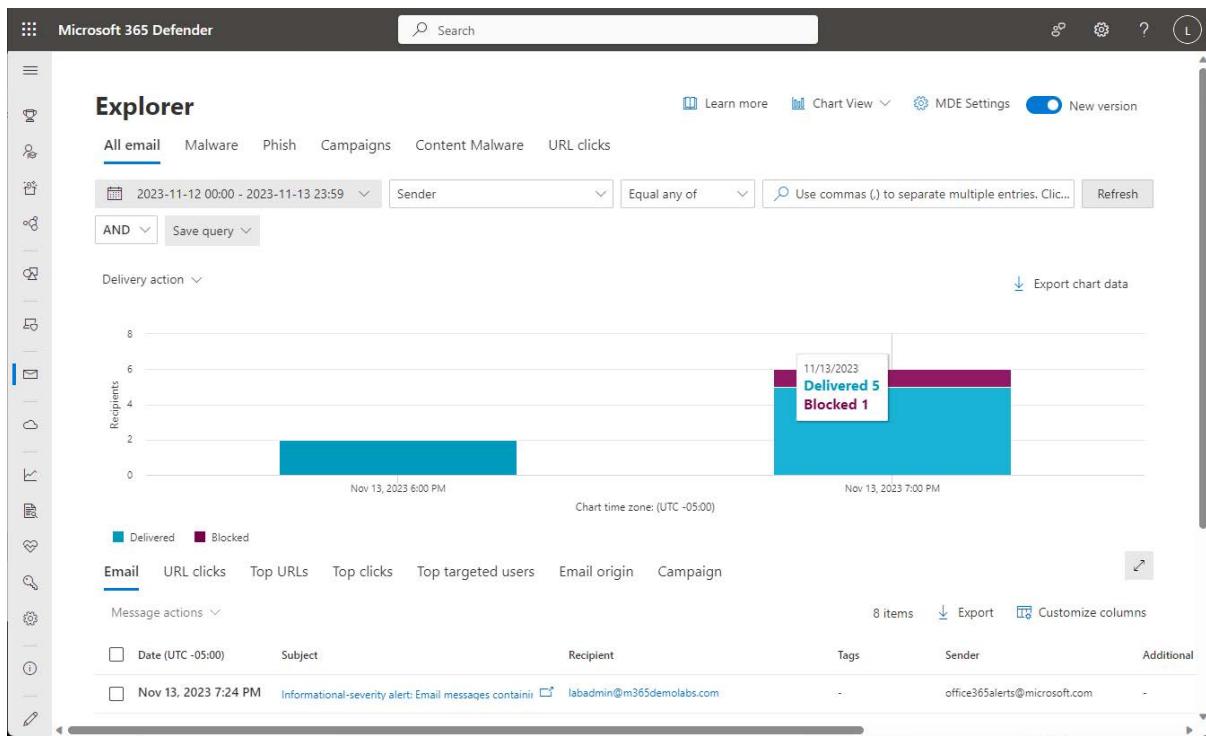


Figure 8.16 – Viewing the Explorer dashboard

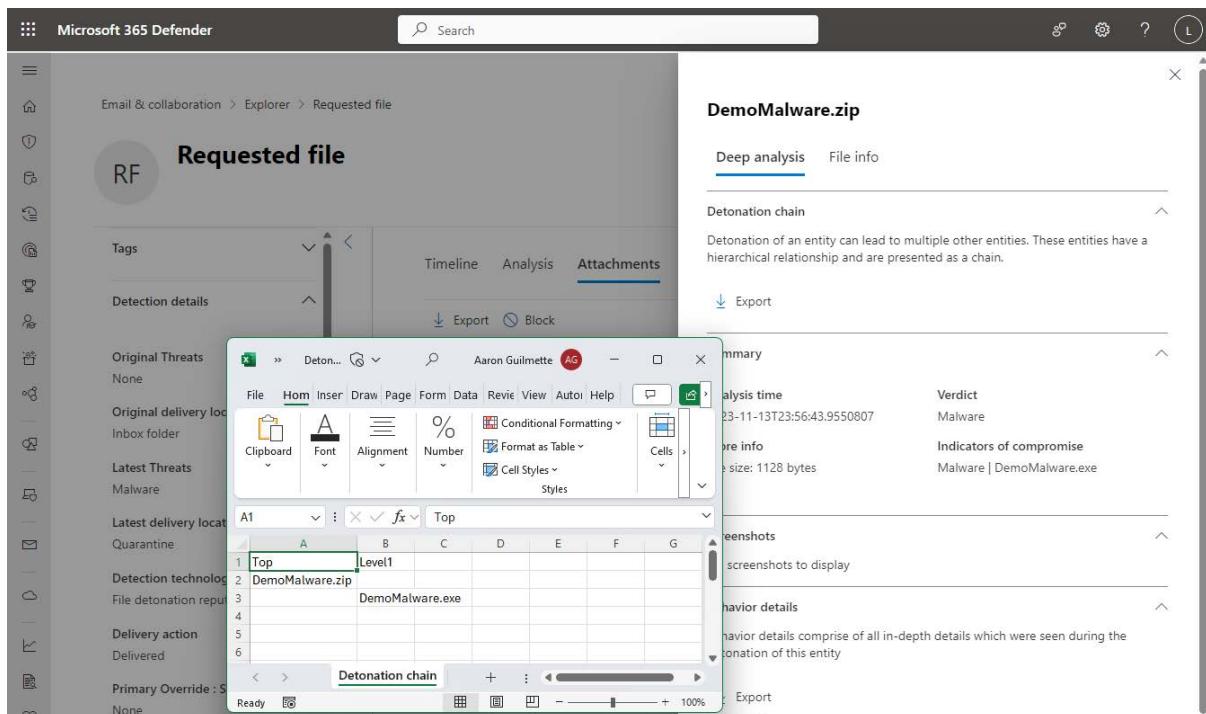


Figure 8.17 – Viewing the details of an attachment

The screenshot shows the Microsoft 365 Defender interface. On the left, there's a navigation bar with various icons. The main area displays a chart titled 'Recipients' over time, with a specific point on Nov 13, 2023, 6:00 PM highlighted. Below the chart, a list of messages is shown, with the first message being selected: 'Nov 13, 2023 7:12 PM Review proposal'. To the right of the message list, a detailed view is open under the heading 'Review proposal'. This view includes sections for 'Delivery details' (Original Threats: None, Delivery action: Blocked) and 'Email details' (Sender display name: labadmin, Sender address: labadmin@m365demolabs.com). At the top of the detailed view, there are buttons for 'Open email entity', 'View header', 'Take action', and more.

Figure 8.18 – Viewing the actions for a message

The screenshot shows the 'Take action' dialog box. On the left, there's a sidebar with icons and a list: 'Choose actions' (selected), 'Choose target entities', and 'Review and submit'. The main area is titled 'Choose response actions' and contains instructions: 'Specify the actions you want to take. Only actions applicable to the selected entity are available. We've grayed out the actions that aren't relevant to you.' Below this, there's a section for 'Email message actions' with an unchecked checkbox for 'Move to mailbox folder' and a checked checkbox for 'Submit to Microsoft for review (Should have been blocked)', which has three radio button options: 'Report as clean', 'Report as phishing' (selected), 'Report as junk', and 'Report as malware'. There's also a section for 'Select entities to block (1/3 entities selected)' with a dropdown menu showing 'Attachment: DemoMalware.exe' and a 'Never expire' option selected. At the bottom of the dialog are 'Next' and 'Cancel' buttons.

Figure 8.19 – Taking action on a message

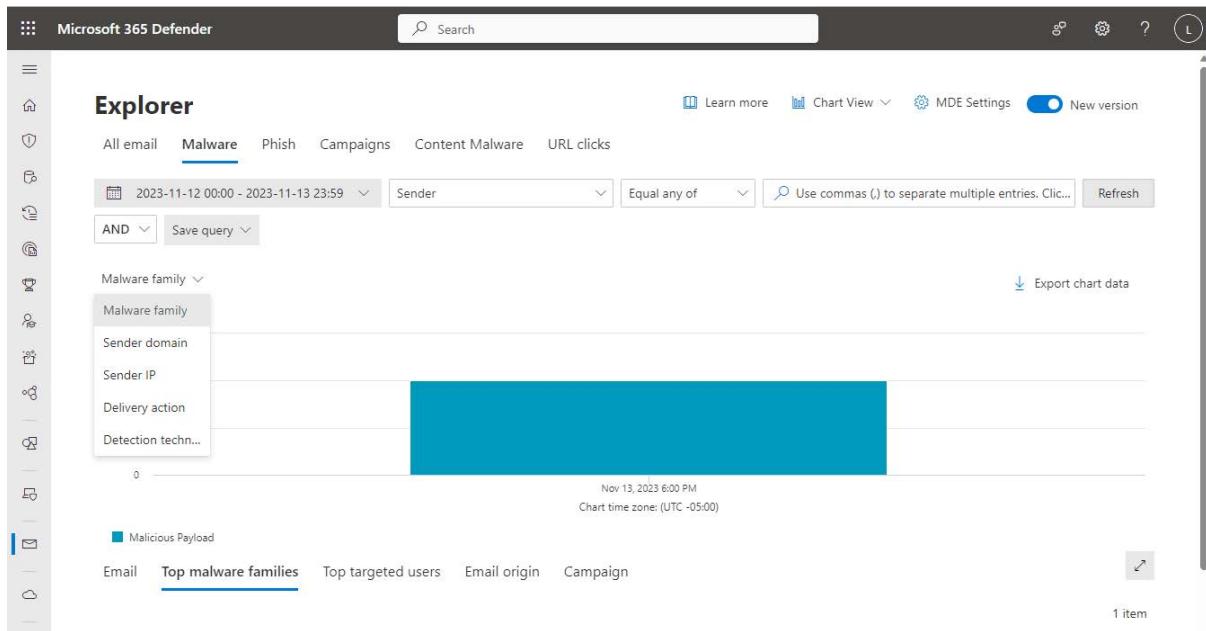


Figure 8.20 – Reviewing the malware page in Explorer

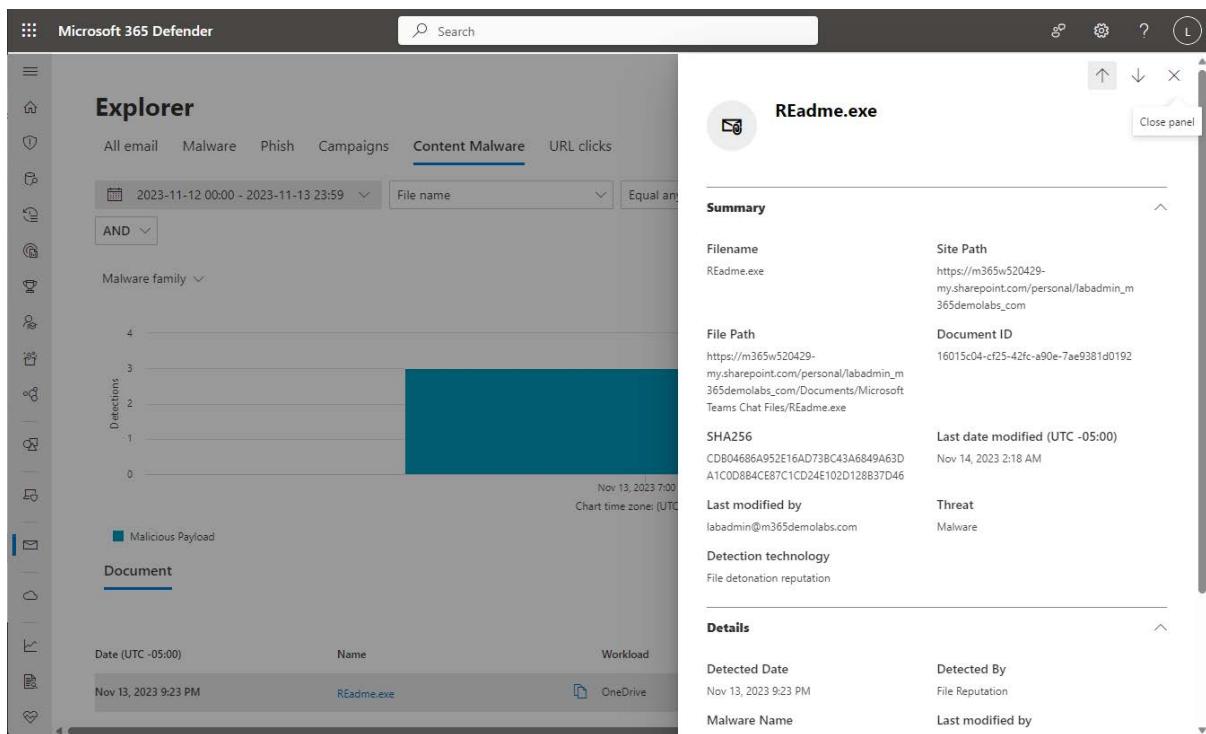


Figure 8.21 – Reviewing a malicious file detection on the Content Malware page

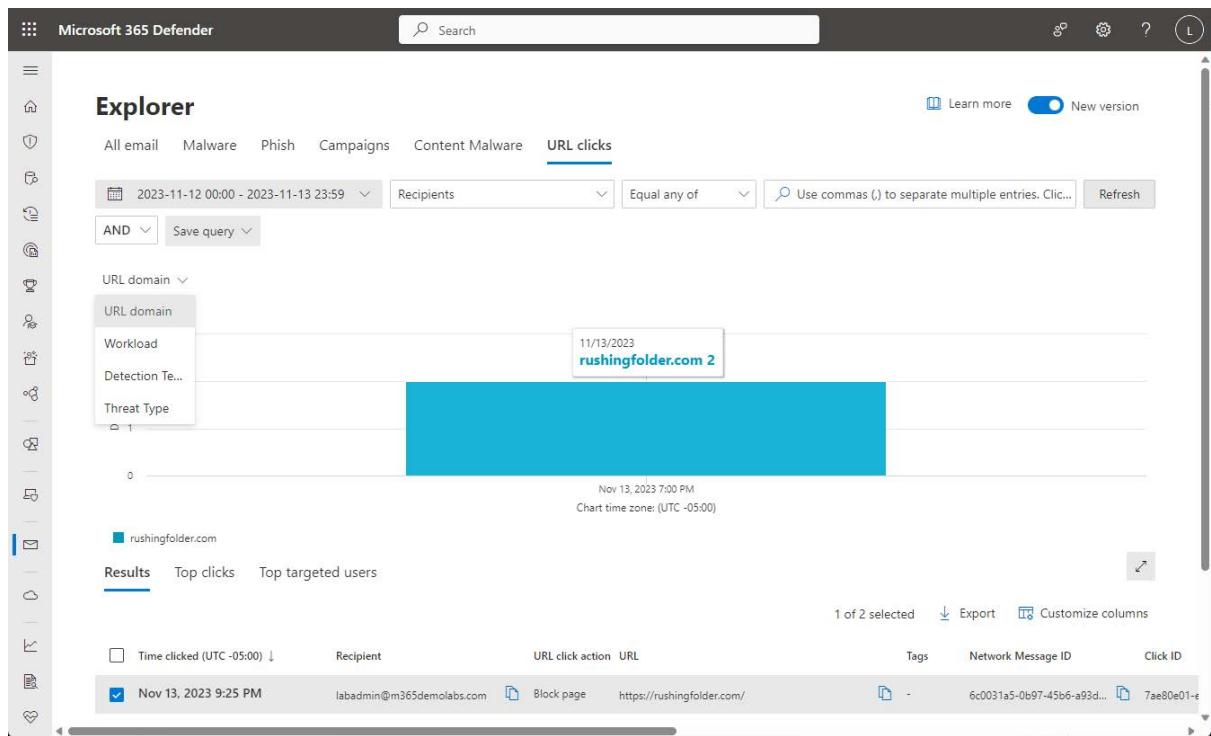


Figure 8.22 – Reviewing the URL clicks page

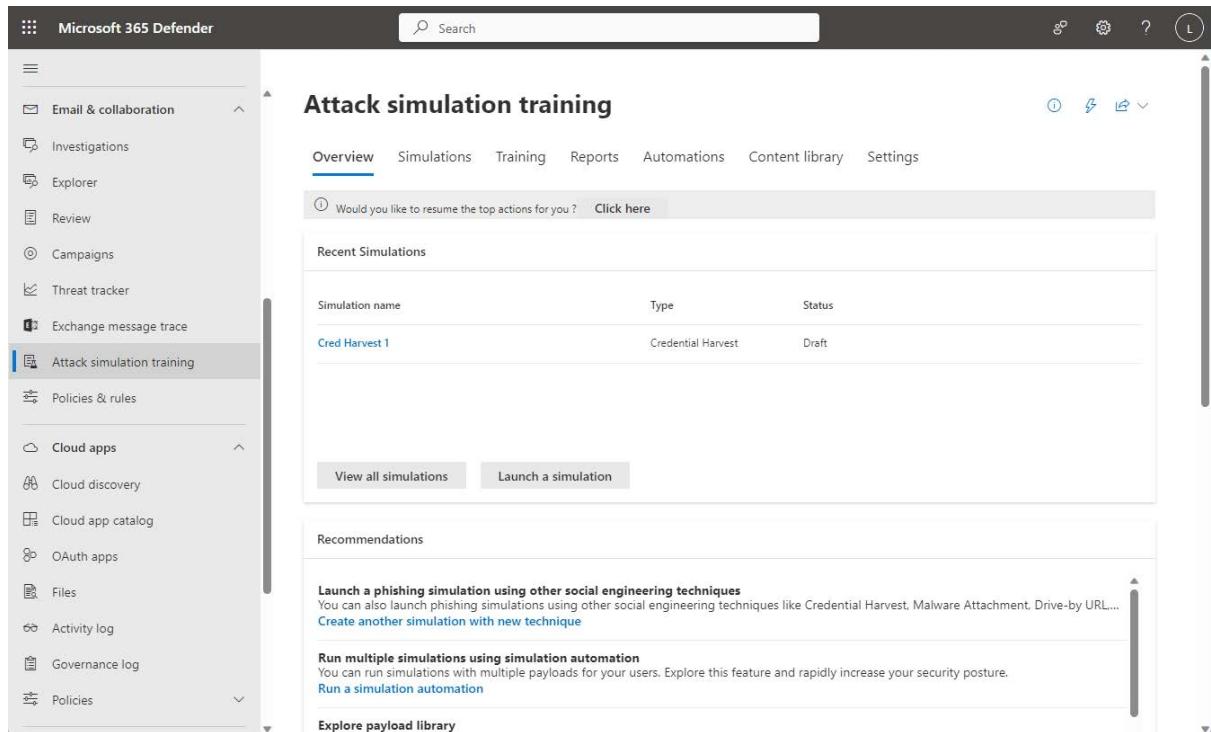


Figure 8.23 – Attack simulation training overview

The screenshot shows the Microsoft 365 Defender interface with the 'Attack simulation training' page. The 'Simulations' tab is active. At the top, there are status counts for Draft (1), Scheduled (0), In progress (0), Completed (0), Failed (0), and Cancelled (0). A button to 'Launch a simulation' is visible. Below the status bar is a table with columns for Simulation Name, Type, Platform, Launch Date, End Date, and Actual Comp. The table currently has one item listed.

Figure 8.24 – Launching a phishing campaign

The screenshot shows the 'Simulation > Create' wizard at the 'Select technique' step. On the left, a sidebar lists steps: Select technique (selected), Name simulation, Select payload and login page, Target users, Assign training, Select end user notification, Launch details, and Review simulation. The main panel displays a list of social engineering techniques:

- Credential Harvest** (selected): In this type of technique, a malicious actor creates a message, with a URL in the message. When the target clicks on the URL within the message, they are taken to a web site, the website often... [View details of Credential harvest](#)
- Malware Attachment**: In this type of technique, a malicious actor creates a message, with an attachment added to the message. When the target opens the attachment, typically some arbitrary code such as a macro... [View details of Malware attachment](#)
- Link in Attachment**: In this type of technique, which is a hybrid of a Credential Harvest and Malware Attachment, a malicious actor creates a message, with a URL in an attachment, and then inserts the attachment into the message. When the target opens the attachment, they are represented with a URL in the actual attachment... [View details of Link in attachment](#)
- Link to Malware**: In this type of technique, a malicious actor creates a message, with an attachment added to the message. However instead of directly inserting the attachment into the message, the malicious actor will host the attachment on a well-known file sharing site, (such as SharePoint, or Dropbox) and insert the URL to the attachment file path... [View details of Link to malware](#)
- Drive-by URL**: In this type of technique, a malicious actor creates a message, with a URL in the message. When the target clicks on the URL within the message, they are taken to a website, the site will then try and run some background code to gather information... [View details of Drive-by URL](#)

At the bottom are 'Next', 'Save and close', and 'Cancel' buttons.

Figure 8.25 – Selecting a technique for the campaign

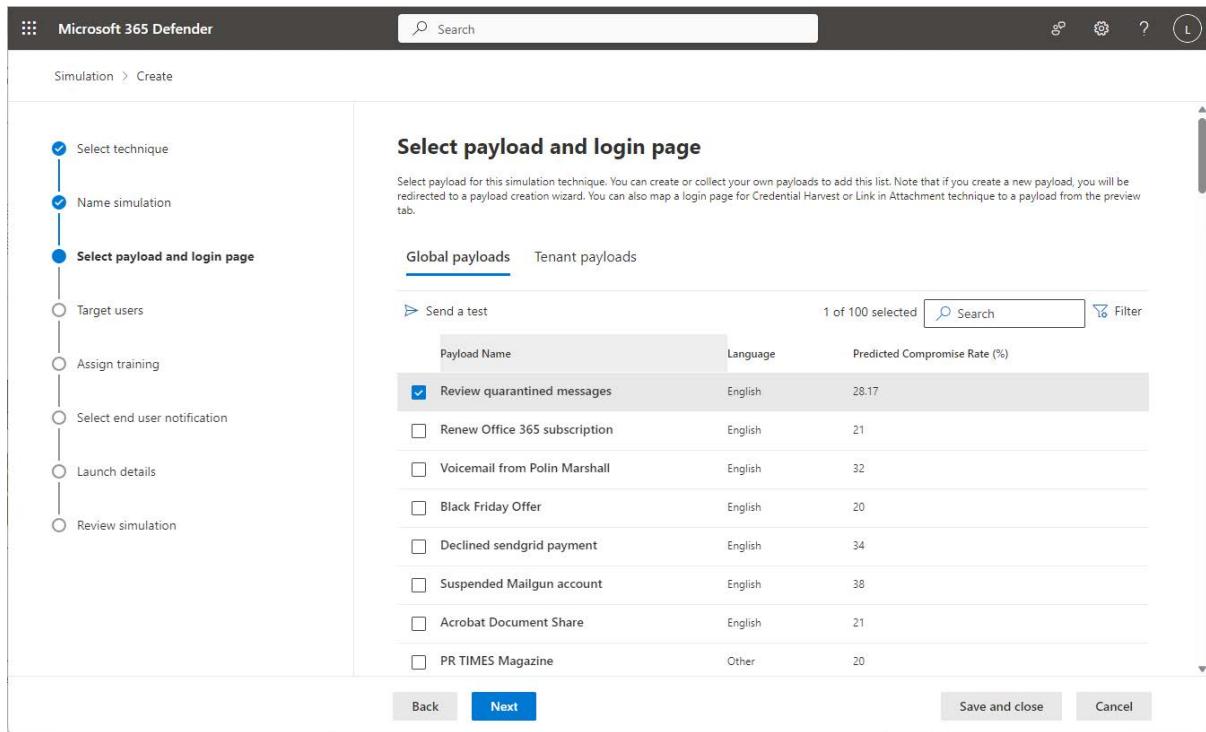


Figure 8.26 – Selecting a payload

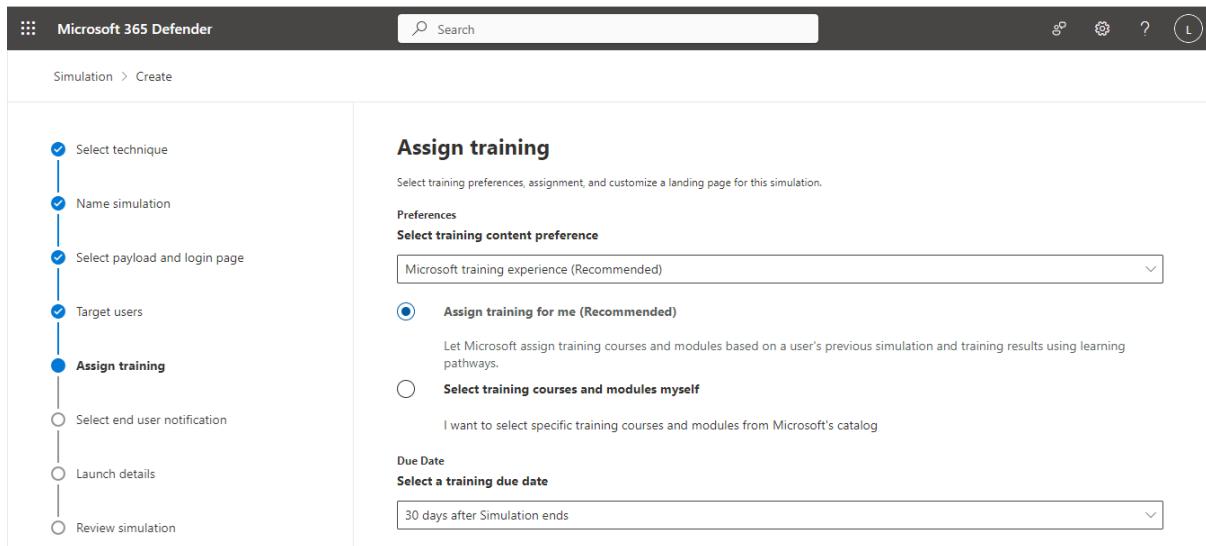


Figure 8.27 – Selecting training options

The screenshot shows the Microsoft 365 Defender interface with the title 'Microsoft 365 Defender' at the top. A search bar is present. The main area is titled 'Add Training' with the sub-instruction '6 training(s) selected'. A message below states: 'Security trainings are the best in class trainings made available by Microsoft for you to train your professionals about security and compliance of your organization and help in improving their behaviour to common attacks and rules. Below is the list of all available trainings that you can use to run a campaign or a simulation. [Learn more](#)'.

A progress bar indicates 'Ready 89' items. Below is a table listing training modules:

Training name	Languages	Tags	Source	Duration (mins)	Last assigned date
Introduction to Information Security	Turkish, Polish... +37	Compliance, Basic... +1	Global	7	
Business Email Compromise	Turkish, Polish... +37	Compliance, Basic... +1	Global	7	
Email	Turkish, Polish... +37	AttachmentMalware, LinkInAttachment... +5	Global	7	
Identity Theft	Turkish, Polish... +37	AttachmentMalware, LinkInAttachment... +5	Global	7	
Malware	Turkish, Polish... +37	AttachmentMalware, LinkToMalwareFile... +3	Global	7	
Phishing	Turkish, Polish... +37	DriveByUrl, CredentialHarvesting... +3	Global	7	

A blue 'Add' button is located at the bottom left of the table.

Figure 8.28 – Adding training modules from the built-in catalog

The screenshot shows the Microsoft 365 Defender interface with the title 'Microsoft 365 Defender' at the top. A search bar is present. The main area is titled 'Custom Training URL'.

Form fields include:

- Custom Training URL ***: A text input field containing 'Custom training URL'.
- Custom Training Name ***: A text input field containing 'Custom training name'.
- Custom training description**: A text input field containing 'Custom training description'.
- Custom training duration (in minutes)**: A text input field containing '0'.

A blue 'Add' button is located at the bottom left of the form.

Figure 8.29 – Adding custom training options

The screenshot shows the Microsoft 365 Defender interface under the 'Attack simulation training' section. The 'Reports' tab is selected. The page is divided into several sections:

- Simulation coverage:** A card with the heading "Look for how many people..." and a sub-instruction "Find details about who received a simulation, and those who haven't received a simulation." It includes a "Learn more" button.
- Training completion:** A card showing "0% users have completed training". Below it is a "Training status" bar with three segments: Completed (blue), In Progress (teal), and Incomplete (light green). A legend indicates: Completed (blue square), In Progress (teal square), and Incomplete (light green square). It also includes a "View training completion report" button.
- Repeat Offenders:** A card with the heading "Investigate repeat offenders..." and a sub-instruction "A repeat offender is a user who was compromised by consecutive simulations. Find repeat offenders in your organisation by running multiple simulations." It includes a "Learn more" button.
- Behavior impact on compromise rate:** A card showing "0 users less susceptible to compromise". It includes a chart comparing "Actual Compromised Rate" (blue dot at 32%) and "Predicted Compromised Rate" (grey dot at 0%). A legend indicates: Actual Compromised Rate (blue square) and Predicted Compromised Rate (grey square). It also includes a "View simulations and training efficacy report" button.

Figure 8.30 – Reviewing training reports

The screenshot shows the Microsoft 365 Defender interface under the 'Alert policy' section. 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." It includes a "Try it now" button.

The main area displays a table of alert policies:

Name	Severity	Type	Category	Date modified (UTC -05:00)	Tags	Status
User restricted from sharing forms and collecting responses	High	System	Threat management	Feb 10, 2021 3:53 PM	-	On
User restricted from sending email	High	System	Threat management	Feb 5, 2020 1:51 PM	-	On

Filter options include: New Alert Policy, Manage Activity Alerts, Refresh, 2 items, user restricted, Filter.

Figure 8.31 – Locating the alert policy

DASHBOARD > CHAPTER 8

Implementing and Managing Email and Collaboration Protection by Using Microsoft Defender for Office 365**Summary**

In this chapter, you learned about the advanced email protection features of Microsoft Defender for Office 365, including Safe Links and Safe Attachments, and how to use threat management tools such as Explorer to investigate and remediate risks. You also learned about the education component, Attack simulation training.

In the next chapter, you'll continue learning about the Microsoft Defender platform by exploring Defender for Endpoint.

Chapter Review Questions

The Microsoft 365 Administrator MS-102 Exam Guide
by Aaron Guilmette

Select Quiz[Quiz 1](#)[SHOW QUIZ DETAILS ▾](#)[START](#)

Figure 8.32 – Chapter Review Questions for Chapter 8

Chapter 9: Implementing and Managing Endpoint Protection by Using Microsoft Defender for Endpoint

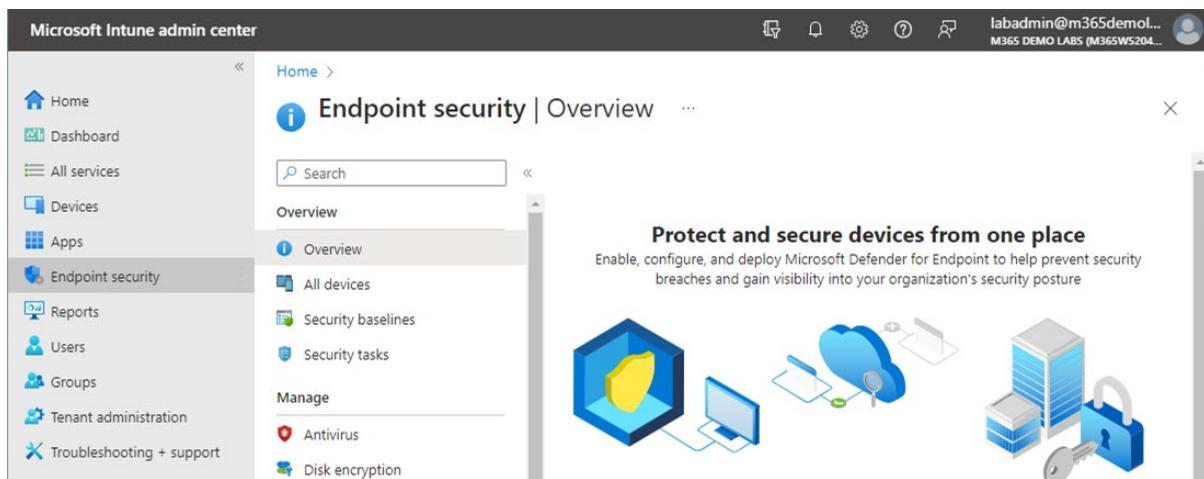


Figure 9.1 – Intune admin center

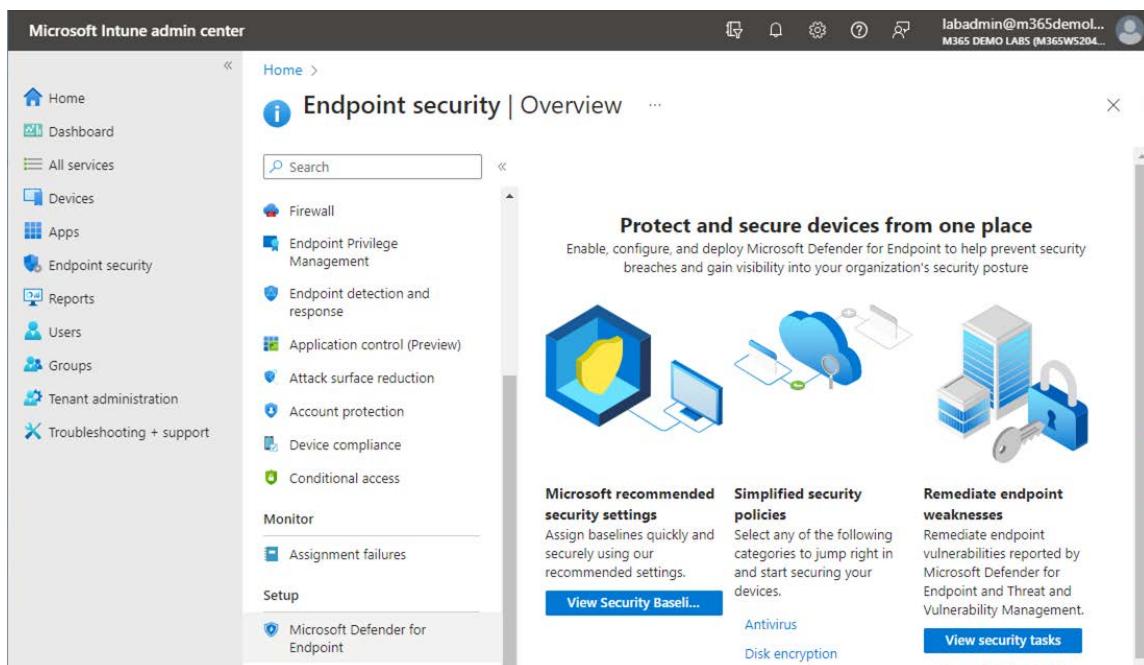


Figure 9.2 – Setting up MDE

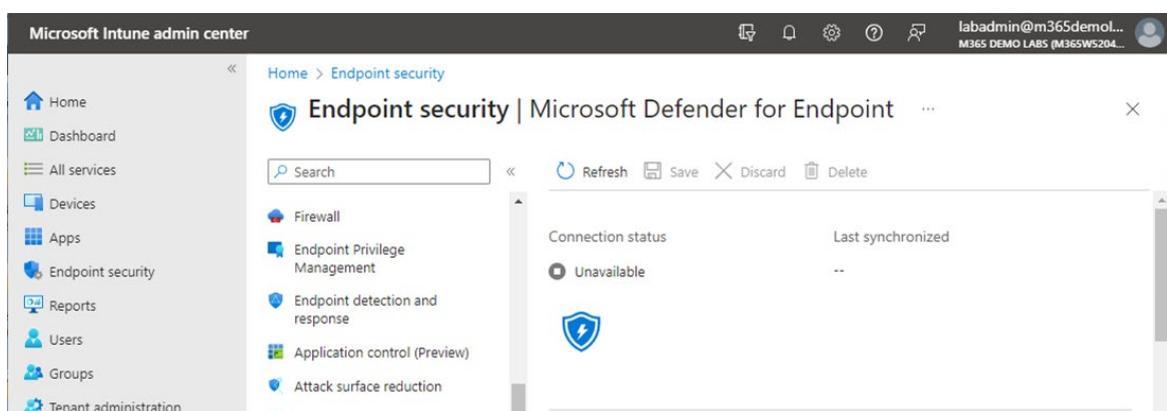


Figure 9.3 – Viewing Intune and Defender connection status

The screenshot shows the Microsoft Intune admin center interface. The left sidebar includes options like Home, Dashboard, All services, Devices, Apps, Endpoint security (which is selected), Reports, Users, Groups, and Tenant administration. The main content area is titled "Endpoint security | Microsoft Defender for Endpoint". It features a search bar and buttons for Refresh, Save, Discard, and Delete. A sidebar on the right lists configuration sections: Firewall, Endpoint Privilege Management, Endpoint detection and response, Application control (Preview), Attack surface reduction, and Account protection. A guide titled "Configuring Microsoft Defender for Endpoint" provides steps: 1. Setup a connection to Intune via the Microsoft Defender Security Center: [Connect Microsoft Defender for Endpoint to Microsoft Intune in the Microsoft Defender Security Center](#). 2. After a connection is established, click "Refresh" at the top of this section to hide this guide. 3. Configure the settings below.

Figure 9.4 – Connecting to the Microsoft 365 Defender Security Center

The screenshot shows the Microsoft 365 Defender portal. The left sidebar includes Cloud app catalog, OAuth apps, Files, Activity log, Governance log, Policies (selected), Reports, Audit, Health, Permissions, and Settings. The main content area is titled "Settings" and displays a table of settings:

Name	Description
Security center	General settings for the Microsoft 365 security center
Microsoft 365 Defender	General settings for Microsoft 365 Defender
Endpoints	General settings for endpoints
Email & collaboration	General settings for email & collaboration
Identities	General settings for identities
Device discovery	Select your device discovery mode and customize standa...
Cloud Apps	General settings for cloud apps

Figure 9.5 – Microsoft 365 Defender portal Settings page

The screenshot shows the Microsoft 365 Defender interface. On the left, there's a navigation sidebar with various options like Cloud app catalog, OAuth apps, Files, Activity log, Governance log, Policies, Reports, Audit, Health, Permissions, Settings, More resources, and Customize navigation. The main content area is titled 'Endpoints' and shows 'Settings > Endpoints > Advanced features'. A section titled 'General' has a 'Advanced features' tab selected, which is currently 'On'. To the right of this is a detailed description of the 'Microsoft Intune connection': 'Connects to Microsoft Intune to enable sharing of device information and enhanced policy enforcement.' Below this, it says 'Intune provides' and there's a 'Save preferences' button at the bottom.

Figure 9.6 – Enabling Microsoft Intune connection

The screenshot shows the Microsoft Intune admin center. The top navigation bar includes tabs for Endpoint security - Microsoft Intune and Endpoints - Microsoft 365 security. The main content area is titled 'Endpoint security | Microsoft Defender for Endpoint'. On the left, there's a sidebar with Home, Dashboard, All services, Devices, Apps, Endpoint security (which is selected), Reports, and Users. The main pane displays a 'Connection status' section with 'Available' and a shield icon. It also shows 'Last synchronized' at 6/24/2023, 2:30:02 PM. There are buttons for Refresh, Save, Discard, and Delete.

Figure 9.7 – Intune admin center after connection has been established

Microsoft Intune admin center

Endpoint security | Microsoft Defender for Endpoint

Compliance policy evaluation

- Connect Android devices version 6.0.0 and above to Microsoft Defender for Endpoint
- Connect iOS/iPadOS devices version 13.0 and above to Microsoft Defender for Endpoint
- Connect Windows devices version 10.0.15063 and above to Microsoft Defender for Endpoint
- Enable App Sync (sending application inventory) for iOS/iPadOS devices
- Send full application inventory data on personally owned iOS/iPadOS devices
- Block unsupported OS versions

App protection policy evaluation

- Connect iOS/iPadOS devices to Microsoft Defender for Endpoint

Figure 9.8 – Compliance policy evaluation section

Microsoft Intune admin center

Compliance policies | Policies

One or more Threat Defense connectors are active for Windows, iOS/iPadOS, and Android but not included in an assigned compliance policy. To protect these platforms, set up a compliance policy with the Device Threat Level rule configured under the Device Health section.

Policy name	Platform or OS	Policy type

Figure 9.9 – Device Compliance policy page

Create a policy

Platform

- Android Enterprise
- Android device administrator
- Android (AOSP)
- Android Enterprise
- iOS/iPadOS
- Linux
- macOS
- Windows 10 and later
- Windows 8.1 and later

Figure 9.10 – Creating a device compliance policy

The screenshot shows the Microsoft Intune admin center interface. On the left, there's a navigation sidebar with various service icons: Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area has a breadcrumb trail: Home > Devices | Compliance policies > Compliance policies | Policies >. The title is "Personally-owned work profile" under "Android Enterprise". Below the title, there are tabs: Basics (green checkmark), Compliance settings (blue outline), Actions for noncompliance (grey outline), Assignments (grey outline), and Review + create (grey outline). The "Compliance settings" tab is active. It contains sections for Microsoft Defender for Endpoint rules (Require the device to be at or under the machine risk score: Low) and Device Health (Rooted devices: Block, Require the device to be at or under the Device Threat Level: Medium). There are also sections for Google Play Protect (Google Play Services is configured: Not configured, Up-to-date security provider: Not configured, Play Integrity Verdict: Not configured). At the bottom, there are "Previous" and "Next" buttons.

Figure 9.11 – Configuring Compliance settings

The screenshot shows the Microsoft Intune admin center interface, similar to Figure 9.11 but with a different tab selected. The title is "Personally-owned work profile" under "Android Enterprise". The active tab is "Actions for noncompliance" (blue outline). Below it, there's a sub-section titled "Specify the sequence of actions on noncompliant devices". A table lists actions: Action (Mark device noncompliant), Schedule (days after noncompliance) (0), Message template (immediately), and Additional recipients (...). A dropdown menu is open over the "Action" column, showing options: Send email to end user, Send push notification to end user, Remotely lock the noncompliant device, and Add device to retire list.

Figure 9.12 – Configuring Actions for noncompliance

The screenshot shows the Microsoft Azure Conditional Access Policies page. On the left, there's a sidebar with 'Home > Conditional Access | Policies >'. Below it, a policy titled 'Require compliant or hybrid Azure AD joined device or multifactor auth' is selected. The 'Grant' section is open, showing several checkboxes for device requirements. One checkbox, 'Require device to be marked as compliant', is checked and highlighted in blue. A tooltip for this checkbox states: 'Don't lock yourself out! Make sure that your device is compliant.' Below this, other unselected options include 'Require Hybrid Azure AD joined device', 'Require approved client app', 'Require app protection policy', and 'Require password change'. At the bottom right of the 'Grant' section is a 'Select' button.

Figure 9.13 – Enabling device compliance as a requirement for Conditional Access policy

The screenshot shows the Windows Settings app with the 'Accounts > Access work or school' screen selected. On the left, a sidebar lists settings like System, Bluetooth & devices, Network & internet, Personalization, Apps, Accounts (which is selected and highlighted in blue), Time & language, Gaming, Accessibility, Privacy & security, and Windows Update. The main area displays a summary of connected accounts: 'Connected by labadmin@m365demolabs.com' and 'labadmin@m365demolabs.com Work or school account'. Below this, there are sections for 'Related settings' including 'Export your management log files' (with an 'Export' button) and 'Create a test-taking account' (with a 'Choose an account for the test taker and enter the address' field). At the bottom, there are links for 'Help with Access work or school' and 'Using Remote Desktop'.

Figure 9.14 – Access work or school screen

```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.2057]
(c) Microsoft Corporation. All rights reserved.

C:\Users\labadmin>dsregcmd /status

+---+
| Device State
+---+

    AzureAdJoined : YES
    EnterpriseJoined : NO
    DomainJoined : NO
    Device Name : Win11-01

+---+
| Device Details
+---+

    DeviceId : fa0305e1-a679-466a-a172-c30e4f5e37de
    Thumbprint : B9C529665643F28AC7D32B1BF9F4E160C8D3D37D
    DeviceCertificateValidity : [ 2023-06-22 23:39:46.000 UTC -- 2033-06-23 00:09:46.000 UTC ]
    KeyContainerId : 875337f8-711e-44ec-9d32-2ea0482b12ba
        KeyProvider : Microsoft Software Key Storage Provider
    TpmProtected : NO
    DeviceAuthStatus : SUCCESS

+---+
| Tenant Details
+---+

    TenantName :
        TenantId : 8719ae72-cbdf-47e3-97a9-5706e8065a56
    AuthCodeUrl : https://login.microsoftonline.com/8719ae72-cbdf-47e3-97a9-5706e8065a56/oauth2/authorize

```

Figure 9.15 – Viewing device join status

The screenshot shows the Microsoft Intune admin center interface. The left sidebar contains links for Home, Dashboard, All services, Devices, Apps, Endpoint security (which is selected), Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled "Endpoint security | Endpoint detection and response". It features a search bar, a "Create Policy" button, and refresh/export options. A message at the top right states: "By June 1st, the OS platform attribute Windows Server devices will show up as 'Windows Server' rather than 'Windows.' Dynamic group rules that use '-eq Windows' should be updated to '-eq Windows Server'. Learn more on how to prepare for this change." Below this is a search bar for "Search by profile name" and a table header for "Policy name, Policy type, Assigned, Platform". The table body shows "No results".

Figure 9.16 – Creating an EDR policy

The screenshot shows the Microsoft 365 Defender admin center interface. On the left, the navigation menu includes Home, Incidents & alerts, Hunting, Actions & submissions, Threat intelligence, Secure score, Learning hub, Trials, Partner catalog, Assets, Devices (selected), Identities, and Endpoints. The main content area is titled 'Device' and shows details for a device named 'Win11-01'. The device is listed as 'Active' with 'None' as the 'Onboarding status'. Key information includes IP addresses (10.2.0.8), first seen on Jul 2, 2023, at 3:03:29 PM. The 'Compute' section shows a total of 1 device. Under 'Device management', it is managed by Intune with an MDE Enrollment status of N/A. A filter bar at the bottom shows 'Name: Win11-01' and 'win11' selected. The status bar at the bottom right indicates '0 active alerts in 0 incidents'.

Figure 9.17 – Microsoft 365 Defender admin center device onboarding status

The screenshot shows the Microsoft Intune admin center interface. The left sidebar includes Home, Dashboard, All services, Devices (selected), Apps, Endpoint security, and Reports. The main content area is titled 'Win11-01 | Device configuration' and shows a table of policies applied to the device. The table has columns for Policy, Logged in user, Policy type, and State. It lists 'Windows EDR Policy' for user 'labadmin@m365demo...' with 'Endpoint Security' type and 'Conflict' state, and 'Windows MDE Configu...' for user 'labadmin@m365demo...' with 'Device configuration' type and 'Succeeded' state. A search bar and export button are also visible.

Figure 9.18 – Defender for Endpoint policy conflict

The screenshot shows the Microsoft 365 Defender admin center interface. The left sidebar includes Cloud app catalog, OAuth apps, Files, Activity log, Governance log, Policies (selected), Reports, Audit, Health, and Permissions. The main content area is titled 'Endpoints' and shows the 'Onboarding' section. It displays a list of configuration management options: Automation uploads, Automation folder exclusions, Configuration management, Enforcement scope, Device management, and Onboarding. A dropdown menu for 'Select operating system to start onboarding process' is set to 'Windows 10 and 11'. Below this, a section titled '1. Onboard a device' shows 'First device onboarded:' and 'Completed' with a green checkmark. The status bar at the bottom right indicates 'Completed'.

Figure 9.19 – Reviewing endpoint onboarding status

The screenshot shows the Microsoft 365 Defender interface under the 'Endpoints' section. On the left, a sidebar lists various settings like General, Permissions, APIs, and Rules. The main area is titled 'Endpoints' and shows a step-by-step onboarding process for macOS. It includes a dropdown for 'Select operating system to start onboarding process' set to 'macOS'. Below it, a section titled '1. Install the agent and onboard a device' provides instructions: 'Install the agent on the macOS device using the installation package, then onboard devices to Microsoft Defender for Endpoint using the configuration package that matches your [preferred deployment method](#). For other device preparation instructions, read [Onboard and set up](#)'. A 'Deployment method' dropdown is set to 'Mobile Device Management / Microsoft ...'. A note below says: 'You can use Mobile Device Management solutions, such as Microsoft Intune to configure and monitor your devices. Before downloading the packages, review the [instructions](#)'. At the bottom are two download buttons: 'Download installation package' and 'Download onboarding package'.

Figure 9.20 – Downloading the onboarding package for macOS

The screenshot shows the Microsoft Intune admin center under the 'Devices' section. The left sidebar includes links for Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main area is titled 'Devices | Configuration profiles' and shows a list of existing profiles. The 'Profiles' tab is selected. The table has columns for 'Profile name', 'Platform', and 'Profile type'. Two entries are listed: 'iOS 8.0 and up policy' (Platform: iOS/iPadOS, Profile type: Device restrictions) and 'iOS VPN' (Platform: iOS/iPadOS, Profile type: VPN). There are buttons for '+ Create profile', 'Refresh', 'Export', and 'Columns'.

Profile name	Platform	Profile type
iOS 8.0 and up policy	iOS/iPadOS	Device restrictions
iOS VPN	iOS/iPadOS	VPN

Figure 9.21 – Setting up a new configuration profile

The screenshot shows the Microsoft Intune admin center interface. On the left, there's a navigation sidebar with various options like Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main area is titled "Custom" under "macOS". At the top right, there's a message: "Upload Completed for WindowsDefenderATPOnboarding.xml" with a size of "9.03 KiB | Streaming upload". Below this, there are tabs: Basics (selected), Configuration settings, Assignments, and Review + create. The "Configuration settings" tab has fields for "Custom configuration profile name" (set to "macOS MDE - Device channel") and "Deployment channel" (set to "Device channel"). A "Configuration profile file" section shows the XML content of "WindowsDefenderATPOnboarding.xml":

```
1 <?xml version="1.0" encoding="utf-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
3 <plist version="1">
4   <dict>
5     <key>PayloadUUID</key>
6     <string>A27F524F-7A54-4E9A-B459-B50A321C4295</string>
7   </dict>
8 </plist>
```

At the bottom are "Previous" and "Next" buttons.

Figure 9.22 – Configuration settings tab

The screenshot shows the Microsoft Intune admin center interface. The left sidebar is identical to Figure 9.22. The main area is titled "Extensions" under "macOS". It includes a note: "These settings work for devices that were enrolled in Intune with user approval, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes all supervised devices." There are sections for "Block user overrides" (set to "Not configured"), "Allowed team identifiers", and "Allowed system extensions". Under "Allowed system extensions", there are two tables:

Bundle identifier	Team identifier
com.microsoft.wdav.epsext	UBF8T346G9
com.microsoft.wdav.netext	UBF8T346G9
com.company.application	e.g. ABCDE12345

At the bottom are "Previous" and "Next" buttons.

Figure 9.23 – Extension configuration settings

The screenshot shows the Microsoft Intune admin center interface. The left sidebar includes Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, and Tenant administration. The main navigation path is Home > Devices | Monitor > Monitor | Assignment status > macOS MDE Onboarding. The title is "macOS MDE Onboarding | Device status". The "Device status" section is selected under the "Monitor" category. A table lists one device: "Aaron's iMac" with User Principal Name "labadmin@m365de...", Deployment status "Succeeded", and Last status "07/05/202...".

Figure 9.24 – macOS enrolled in Intune

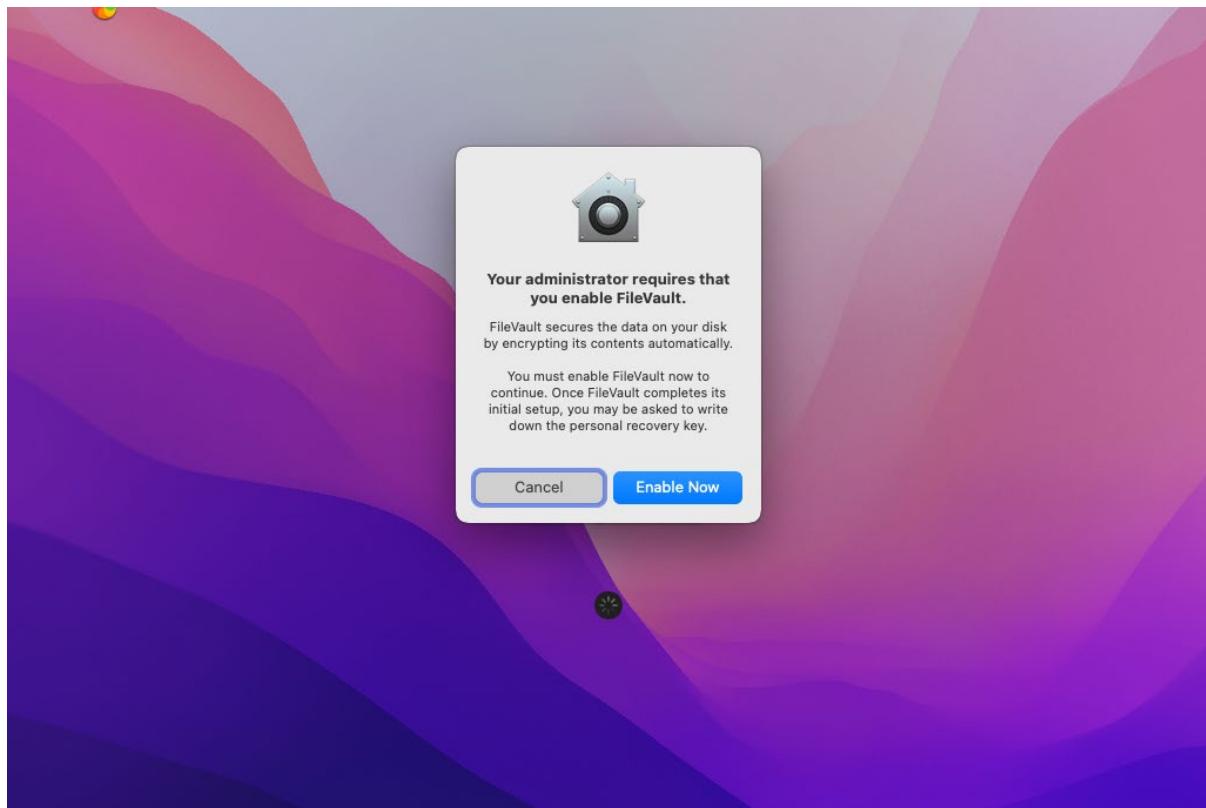


Figure 9.25 – macOS with FileVault encryption policy enabled

The screenshot shows the Microsoft Intune admin center interface. The left sidebar includes Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, and Tenant administration. The main navigation path is Home > Apps | Overview. The title is "Apps | Overview". The "By platform" section is selected, showing "Windows" and "iOS/iPadOS". A message at the top right says: "Microsoft Intune recommends managing Microsoft 365 Apps with Current Channel. [Learn more](#)". The "Essentials" section displays the following information: Tenant name (M365w520429.onmicrosoft.com), Tenant location (North America 0102), MDM authority (Microsoft Intune), and Account status (Active).

Figure 9.26 – Configuring an iOS app

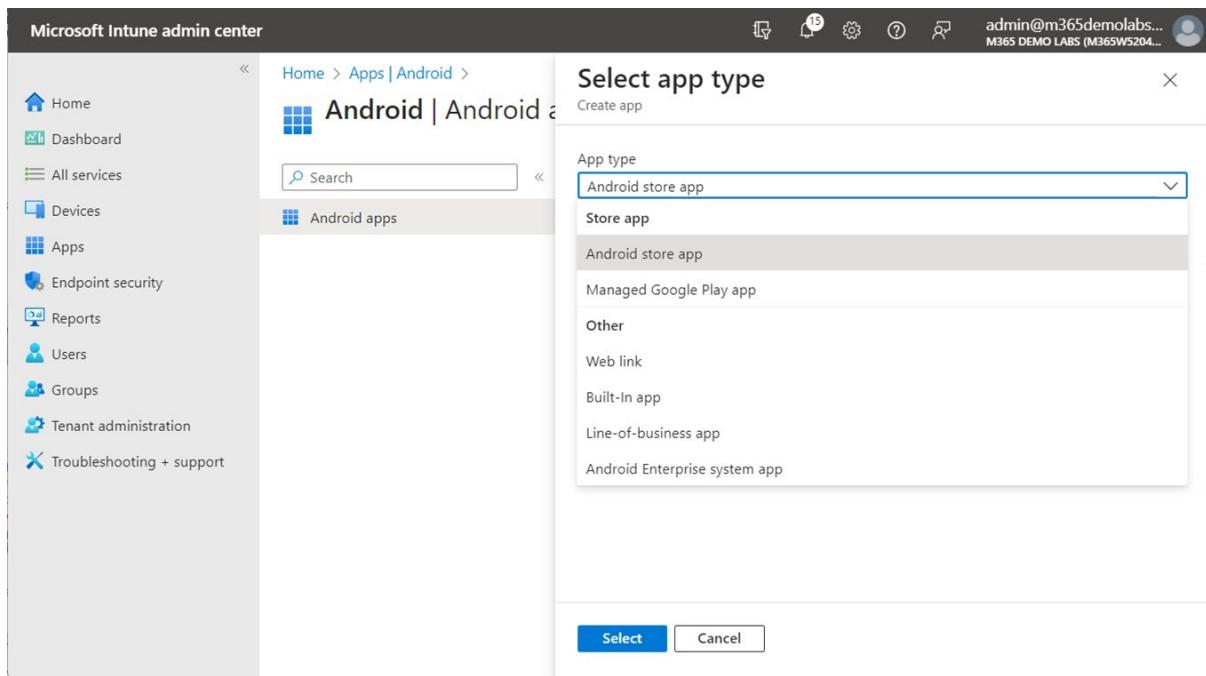


Figure 9.27 – Selecting the Android store app type

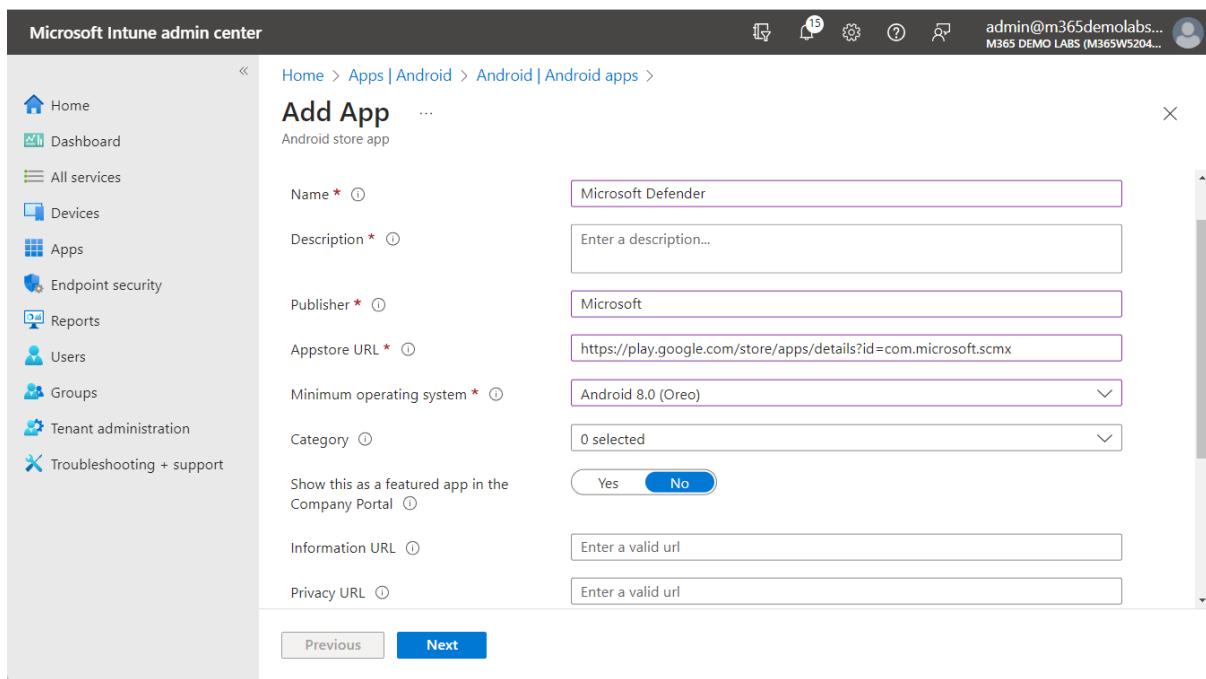


Figure 9.27 – Selecting the Android store app type

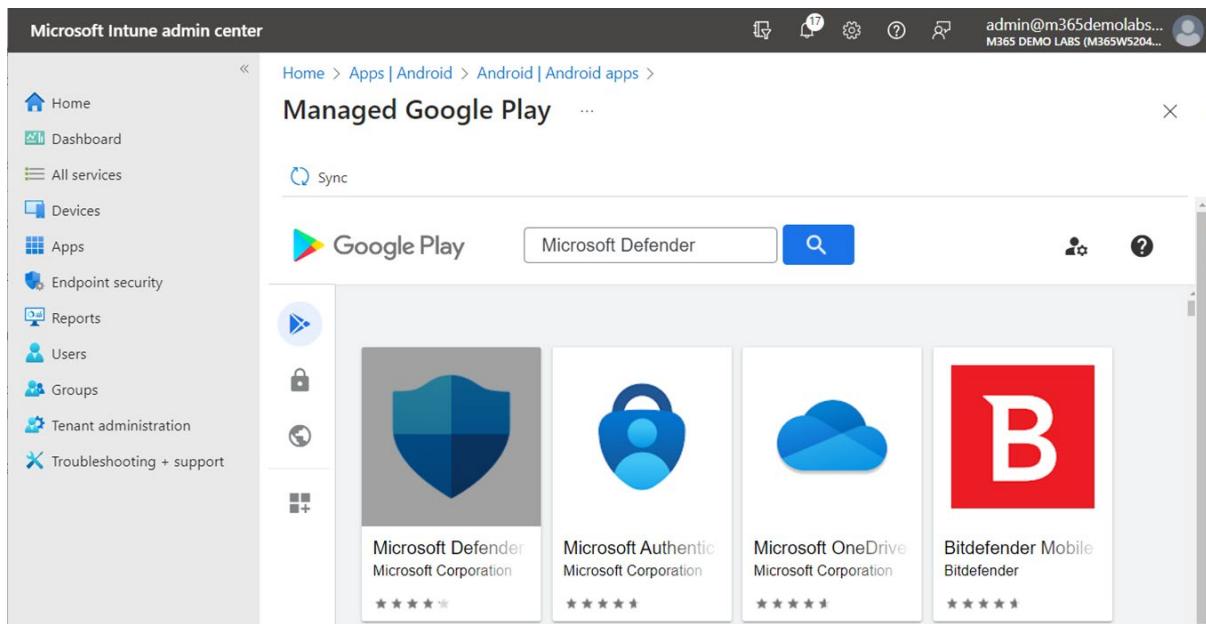


Figure 9.29 – Locating the Microsoft Defender app

The screenshot shows the Microsoft Intune admin center interface. On the left, there is a navigation sidebar with various options like Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main area is titled "Android | Android apps" and shows a search bar with "Search" and a "Filter" button. Below the search bar, there is a table of managed Google Play Store apps. The table has columns for Name, Type, and Status. The data is as follows:

Name	Type	Status
Intune Company Portal	Managed Google Play store app	
Managed Home Screen	Managed Google Play store app	
Microsoft Authenticator	Managed Google Play store app	
Microsoft Defender	Android store app	
Microsoft Intune	Managed Google Play store app	

Figure 9.30 – Managed Google Play Store apps

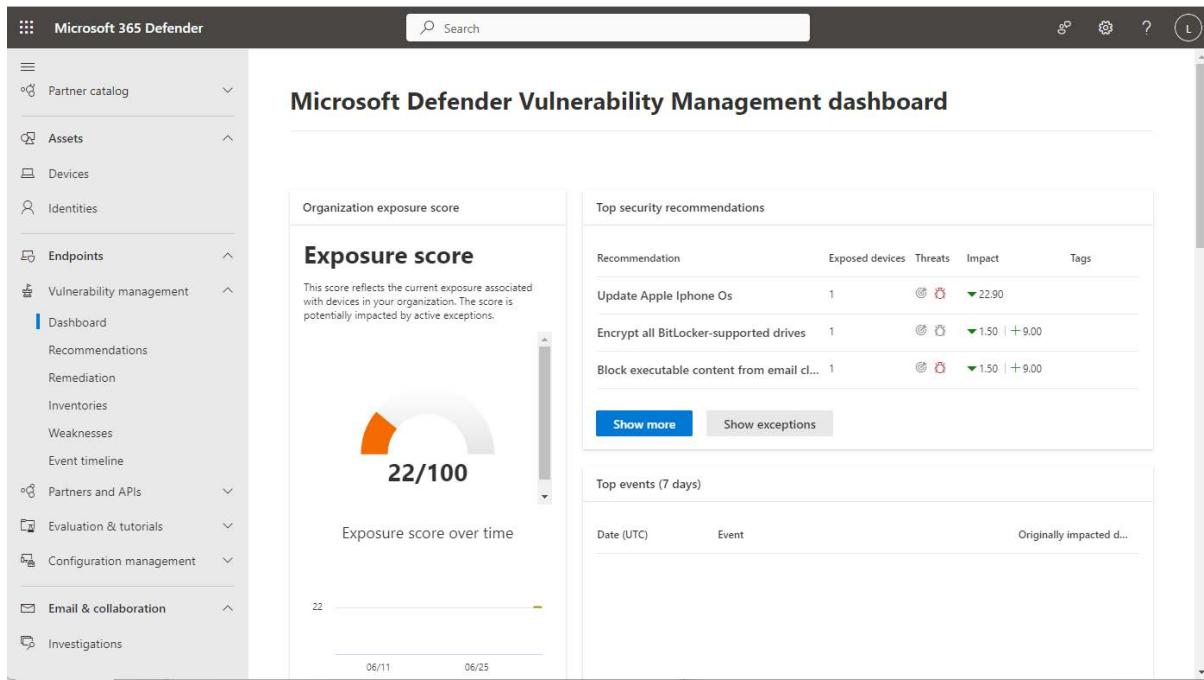


Figure 9.31 – Vulnerability Management dashboard

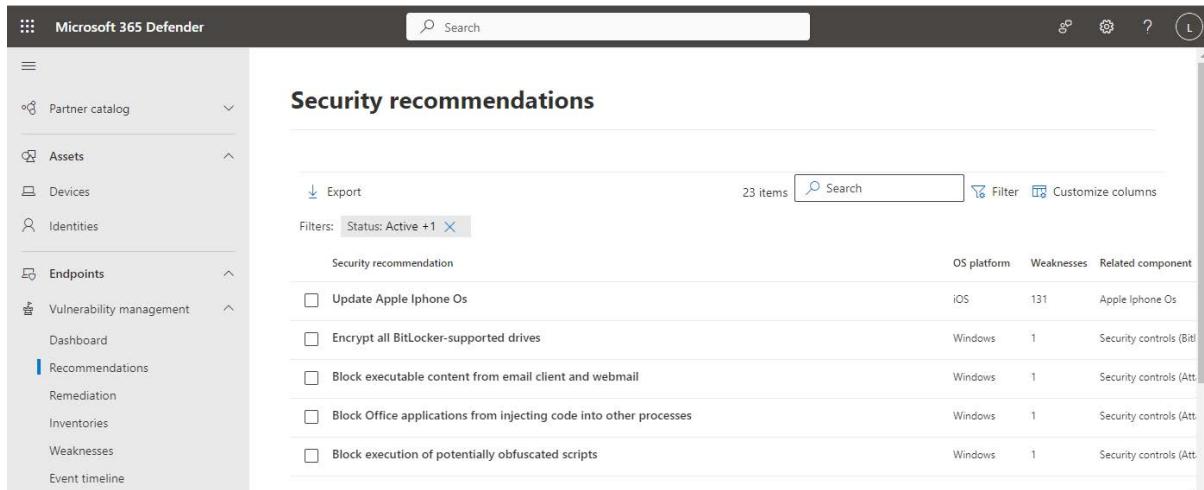


Figure 9.32 – Recommendations page

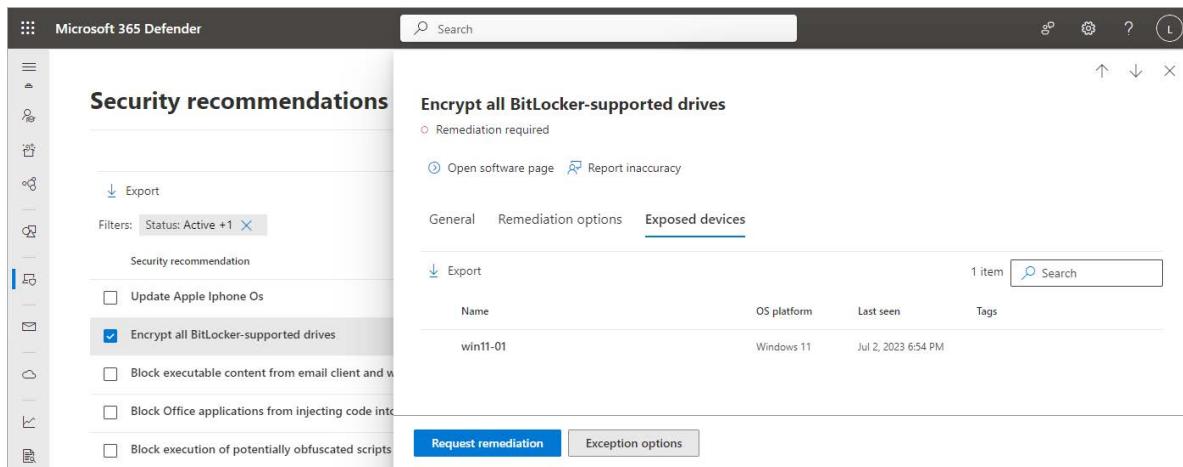


Figure 9.33 – Request remediation

The screenshot shows the Microsoft 365 Defender interface for a device named 'labadmin_iPhone 7'. The left sidebar includes 'Secure score', 'Learning hub', 'Trials', 'Partner catalog', 'Assets' (selected), 'Devices', 'Identities', and 'Endpoints'. The main panel displays the device's status as 'Active' with 'No known risks'. It features tabs for 'Overview', 'Incidents and alerts', 'Timeline', 'Security recommendations', 'Software inventory', and 'Browser exte...'. Under 'Overview', it shows 'AAD joined' and lists 'iOS', 'Unknown (Release Other Build 7)'. Below this, 'Active alerts (Last 180 days)' show 1 active alert and 1 active incident. A 'Risk level: None' section indicates 1 active security recommendation. On the right, there are buttons for 'Manage tags', 'Report device inaccuracy', 'Initiate Automated Investigation', 'Ask Defender Experts', 'Action center', and 'Exclude' (which is highlighted). A search bar at the top is empty.

Figure 9.34 – Excluding a device from Threat Management

The screenshot shows the Microsoft 365 Defender 'Remediation' page. The left sidebar has icons for Secure score, Learning hub, Trials, Partner catalog, Assets (selected), Devices, Identities, Endpoints, and a gear icon. The main area shows 'Activities' (1 in progress, 0 past due) and 'Exceptions'. An activity titled 'Encrypt all BitLocker-supported drives' is selected, showing a checked checkbox. To the right, the 'Tracking' section details the task: Service name (Intune), Ticket status (Approved (Intune)), Notes (Creating security task), Device remediation status (Active), and Device remediation progress (0/1). The 'Details' section shows Created on (Jul 5, 2023 6:58 PM), Created by (labadmin@m365demolabs.com), Priority (Medium), Remaining time until due (0 days (Jul 5, 2023 8:00 PM)), and Notes. Buttons for 'Mark as completed' and 'Export to CSV' are also present.

Figure 9.35 – Remediation page

Inventories

Software Browser extensions (trial) Certificates (trial) Hardware & Firmware (trial)

Software **10**

Export 10 items Search Filter Customize columns

Filters: Product Code (CPE): Available X

Name	OS platform	Vendor	Weaknesses	Threats	Exposed devices	Impact
Iphone Os	iOS	Apple	131	0/0	1/1	22.90
Windows 11	Windows	Microsoft	0	0/0	0/1	0.00
Openssl	Windows	Openssl	0	0/0	0/1	0.00
Windows Defender	Windows	Microsoft	0	0/0	0/1	0.00
Defender For Endpoint For IOS	iOS	Microsoft	0	0/0	0/1	0.00
.net Framework	Windows	Microsoft	0	0/0	0/1	0.00
Edge Webview2 Runtime	Windows	Microsoft	0	0/0	0/1	0.00
Internet Explorer	Windows	Microsoft	0	0/0	0/1	0.00

Figure 9.36 – Inventories page

Weaknesses

Vulnerabilities in my organization **131** Exploitable vulnerability **1** Critical vulnerabilities **3** Zero-day vulnerabilities **0** Vulnerabilities with no security update **0**

Vulnerabilities with some security updates **0**

Email notifications settings

Export 131 items Search Filter Customize columns

Filters: Exposed devices: Affects my organization X

Name	Severity	CVSS	Related Software	Age	Published on	First detected	Updated on	Threats	Exp...	Tags
CVE-2023-32423	Medium	6.5	Apple Watchos (+ 4 more)	2 months	May 17, 2023 8:00...	Jul 3, 2023 5:...	Jun 30, 2023 ...	0/0	1	
CVE-2023-32422	Medium	6.2	Apple Tvos (+ 2 more)	2 months	May 17, 2023 8:00...	Jul 3, 2023 5:...	Jun 30, 2023 ...	0/0	1	
CVE-2023-32420	Medium	5.5	Apple Watchos (+ 3 more)	2 months	May 17, 2023 8:00...	Jul 3, 2023 5:...	Jun 30, 2023 ...	0/0	1	
CVE-2023-32419	Critical	9.8	Apple Iphone Os (+ 1 more)	2 months	May 17, 2023 8:00...	Jul 3, 2023 5:...	Jun 30, 2023 ...	0/0	1	

Figure 9.37 – Weaknesses page

Event timeline

New vulnerabilities **20** New zero-day vulnerabilities **0** Exploitable vulnerabilities **0** New configuration assessments **0**

Email notifications settings

Export 8 items Search Filter Customize columns

Date (UTC) ↓	Event	Related component	Originally impacted d...	Currently impacted de...	Type
Jun 26, 2023 8:00 PM	Apple Iphone Os has 2 new vulnerabilities, impacting 1 device	Apple Iphone Os	1 (<1%)	1 (50%)	New
May 16, 2023 8:00 PM	Apple Iphone Os has a new vulnerability, impacting 1 device	Apple Iphone Os	1 (<1%)	1 (50%)	New
May 14, 2023 8:00 PM	Apple Iphone Os has a new vulnerability, impacting 1 device	Apple Iphone Os	1 (<1%)	1 (50%)	New

Figure 9.38 – Event timeline page

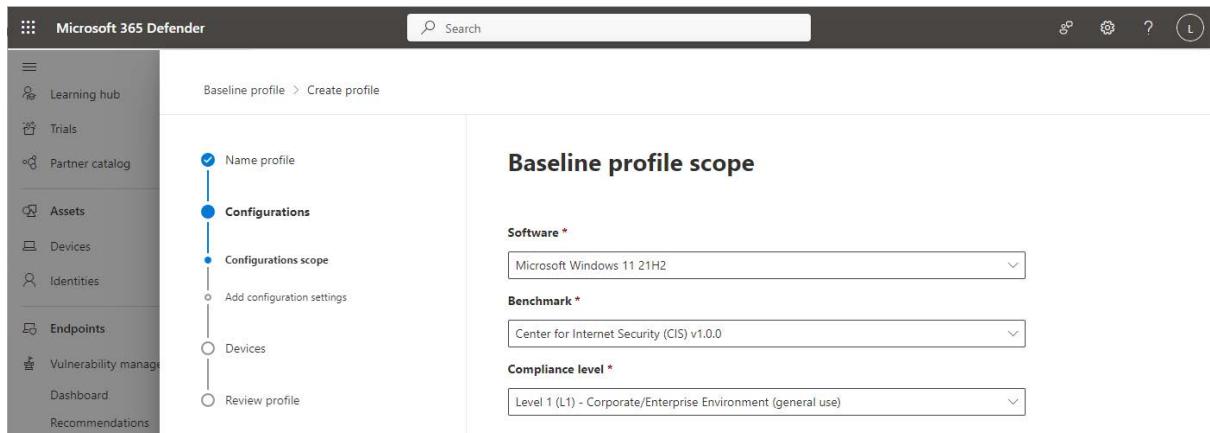


Figure 9.39 – Configuring Baseline profile scope

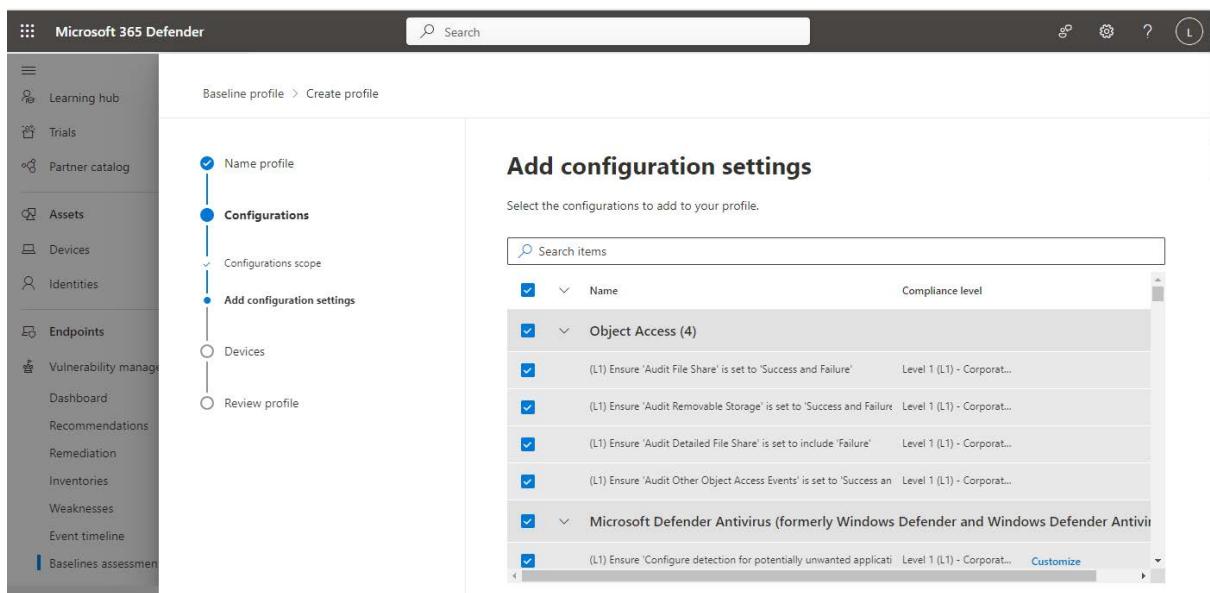


Figure 9.40 – Profile configuration settings

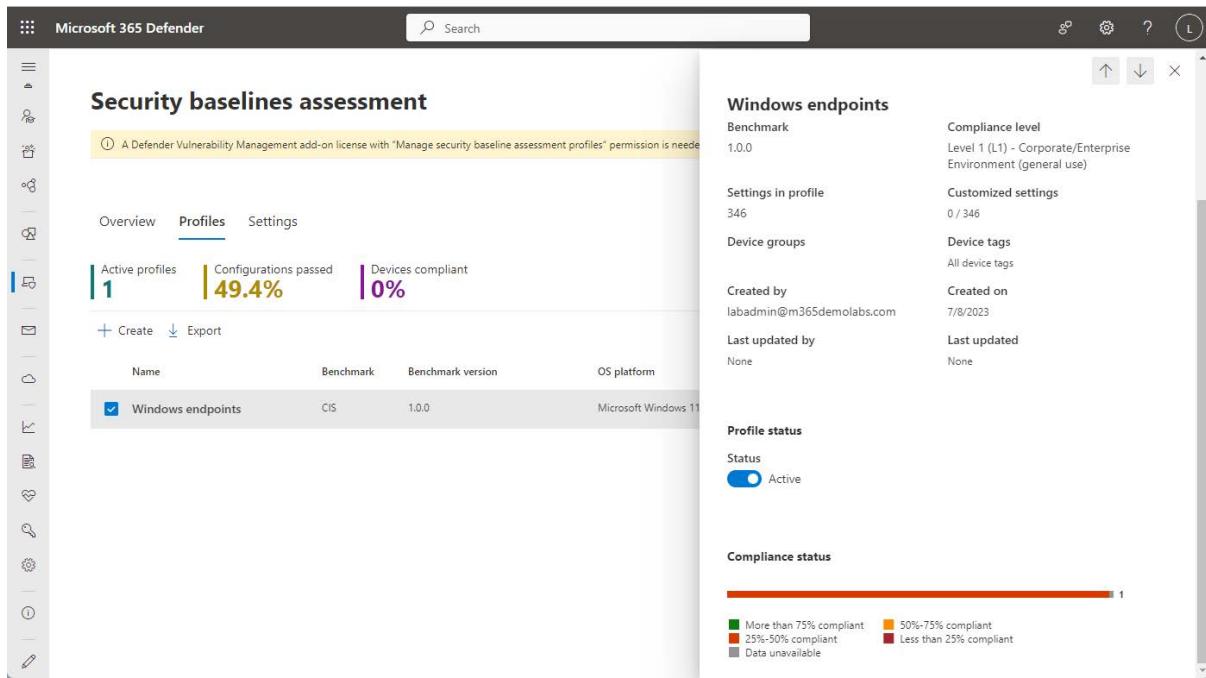


Figure 9.41 – Profile assessment

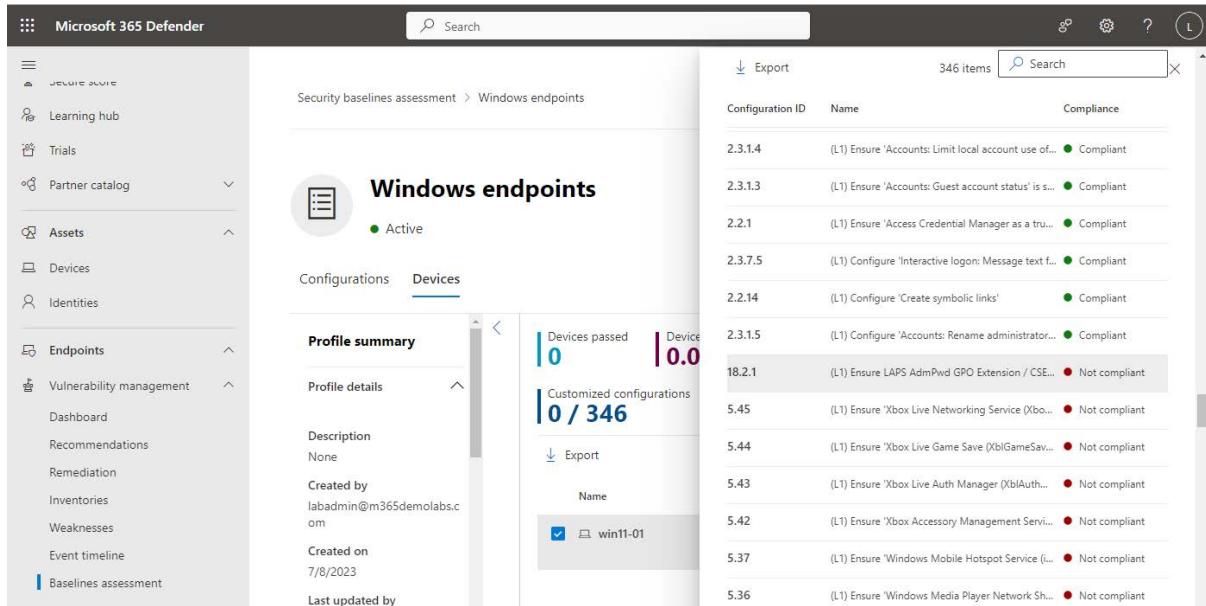


Figure 9.42 – Viewing an individual device's compliance against a baseline profile

The screenshot shows the Microsoft 365 Defender interface under the 'Incidents & alerts' section. The left sidebar includes options like Home, Incidents & alerts (selected), Alerts, Hunting, Actions & submissions, Threat intelligence, Secure score, Learning hub, Trials, Partner catalog, and Assets. The main area is titled 'Incidents' and displays 'Most recent incidents and alerts'. A red box highlights a specific incident entry: 'Multi-stage incident involving Initial access & Lateral... 2'. Below this, a list of alerts is shown, with another red box highlighting the first item: 'Suspicious process injection observed'. Other alert entries include 'Unexpected behavior observed by a process ran ...', 'Suspicious process injection observed', and 'Suspicious sequence of exploration activities'.

Figure 9.43 – Microsoft 365 Defender incidents and alerts

This screenshot shows the 'Attack story' for the incident from Figure 9.43. The left sidebar shows the navigation path: Incidents & alerts > Multi-stage incident involving Initial access & Lateral movement on one endpoint reported by multiple sources. The main area is titled 'Multi-stage incident involving Initial access & Later...'. It includes tabs for Attack story, Alerts (16), Assets (5), Investigations (1), Evidence and Response (23), and Summary. The 'Alerts' tab is selected, showing 16/16 Active alerts. A detailed incident graph is displayed, showing nodes for various system components and their interactions over time. A context menu is open over one of the nodes, listing actions such as 'Open file page', 'Pin related alerts', 'Hide related alerts', and 'Actions'. To the right, there's an 'Incident details' panel with information like 'Assigned to: Unassigned', 'Incident ID: 2', 'Classification: Not set', and 'Categories: Initial access, Execution, Persistence, Defense evasion, Discovery, Lateral movement'. The 'Evidence and Response' tab is expanded, showing a timeline of events with specific alert details like 'Suspicious behavior by Microsoft Word was observed' and 'Suspicious PowerShell download or encoded command execution'.

Figure 9.44 – Attack story

This screenshot provides a detailed view of an alert from the attack story. The left sidebar shows the navigation path: Incidents & alerts > Multi-stage incident involving Initial access & Lateral movement on one endpoint reported by multiple sources. The main area is titled 'Multi-stage incident involving Initial access & Later...'. The 'Alerts' tab is selected, showing 16/16 Active alerts. A specific alert entry is highlighted with a red box: 'Jul 6, 2023 2:45 PM • New Suspicious behavior by Microsoft Word was observed [win11-01] labadmin'. The timeline shows other alerts like 'Suspicious PowerShell download or encoded command execution' and 'PowerShell dropped a suspicious file on the machine'. The 'Evidence and Response' tab is expanded, showing a detailed timeline of events. A specific event is highlighted with a red box: '[10540] alexx 'B4F15...' [Lateral movement] [9948] WINWORD.EXE [/v...]' at 25349 PM. The right side of the screen displays 'Incident details' for this alert, including 'Integrity level: High', 'Token elevation: Invalid', 'User: labadmin', and 'Initiated by: [redacted]'. It also shows the 'Command line' for the highlighted event: 'powershell.exe -w Hidden -Exec B...'. The 'Detection' section indicates 'VirusTotal detection ratio: 0/71' and 'File verdict: unknown'. A summary at the bottom states '5 active alerts in 1 incidents'.

Figure 9.45 – Viewing an alert's details

The screenshot shows the Microsoft 365 Defender interface. On the left is a navigation sidebar with various security categories like Home, Incidents & alerts, Hunting, Threat intelligence, and more. The main area displays an 'Incidents' page for a specific 'Multi-stage incident involving Initial access & Lateral movement on one endpoint reported by multiple sources'. A modal window titled 'Manage alert' is open, showing alert details. The 'Status' field is set to 'In progress'. The 'Assign to' field contains 'labadmin@m365demolabs.com'. The 'Classification' field is set to 'Not set'. The 'Comment' field has 'Add comment' placeholder text. The alert itself is labeled 'True positive' and 'Multi staged attack'. It lists several findings, including 'Suspicious Application' (Low severity) which is selected. Other findings include 'Malware', 'Phishing', and 'False positive'. Buttons for 'Save' and 'Cancel' are at the bottom right of the modal.

Figure 9.46 – Manage alert details

This screenshot shows the Microsoft 365 Defender interface. The left sidebar is identical to Figure 9.46. The main area shows the same incident details. A new tab labeled 'Investigations (1)' is active. A modal window titled 'Powershell dropped a suspicious file on the machine' is open. It shows 'Triggering alert' details: ID 1, Status 'Partially investigated', and Service source 'Microsoft Defender for Endpoints'. To the right, the 'Investigation details' pane shows the alert was triggered by 'PowerShell dropped a suspicious file on the machine'. It includes fields for ID (1), Status (Partially investigated), Duration (35:08 minutes), Started (Jul 6, 2023, 2:55:19 PM), and Ended (Jul 6, 2023, 3:30:27 PM). Below this, 'Triggering alert details' are listed, including Incident (2), Detection source (EDR), Category (Execution), First activity (Jul 6, 2023, 2:54:08 PM), Last activity (Jul 6, 2023, 2:54:08 PM), and Generated on (Jul 6, 2023, 2:55:18 PM).

Figure 9.47 – Triggering alert investigation

This screenshot shows the Microsoft 365 Defender interface with the 'Investigations' page active. The left sidebar is consistent with previous figures. The main area displays the 'Powershell dropped a suspicious file on the machine' investigation. The 'Investigation Summary' section shows the status as 'Some findings might require review', alert severity as 'Medium', category as 'Execution', and detection source as 'EDR'. The 'Investigation Status Timeline' indicates the investigation started at 2:55:19 PM on July 6, 2023, and ended at 3:30:27 PM on July 6, 2023, totaling 35:08 minutes. The 'Investigation graph' on the right visualizes the investigation flow. It starts with an 'Alert received' node (PowerShell dropped a suspicious file on the machine) connected to a 'Device (1)' node (WN11-01). This device node is connected to an 'Evidence' node (7 entities found). The evidence node is connected to a 'Result' node (Partially investigated, Zenises remediated). A tooltip for the device node states '+ 3 correlated alerts'. The 'Entities analyzed (3083)' section lists various types of entities analyzed: 1926 Files, 190 Processes, 289 Services, 412 Drivers, 72 IP Addresses, and 294 Persistence Methods.

Figure 9.48 – Investigations page

The screenshot shows the Microsoft 365 Defender interface. On the left, the navigation menu includes Home, Incidents & alerts, Threat intelligence, Assets, Endpoints, and more. The main content area displays an investigation for a PowerShell dropped a suspicious file on the machine. It shows an investigation summary with a timeline from Jul 6, 2023, 2:55:19 PM to Jul 6, 2023, 3:30:27 PM, and a status of Complete (00:35:08). The investigation details section shows some findings might require review, alert severity (Medium), category (Execution), and detection source (EDR). The evidence tab is selected, showing a list of suspicious entities. One entity, 'winatp-intro-backdoor.exe', is highlighted as Remediated. The right pane provides file details for 'winatp-intro-backdoor.exe', including prevalence (21.5k worldwide, 1 in organization), active alerts (3), and a summary table of findings.

Figure 9.49 – Evidence details

The screenshot shows the Microsoft 365 Defender interface. The navigation menu is identical to Figure 9.49. The main content area displays an investigation for a multi-stage incident involving Initial access & Late... The evidence and response tab is selected. The files section shows four suspicious files: RS4_WinATP-Intro-Invoice.docm, C:\Users\labadmin\Desktop\WinATP-Intro-Backdoor.exe, powershell.exe, and C:\Users\labadmin\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\X365J57\RS4_WinATP-Intro-Invoice.docm. The right pane provides file details for 'RS4_WinATP-Intro-Invoice.docm', including its detection ratio (0/60), malware detection (None), and active alerts (6).

Figure 9.50 – Incident evidence

The screenshot shows the Microsoft 365 Defender interface. On the left, the navigation menu includes Home, Incidents & alerts (selected), Alerts, Hunting, Actions & submissions, Threat intelligence, Secure score, Learning hub, Trials, Partner catalog, Assets, Devices, Identities, Endpoints, Vulnerability management, Farmers and APIs, Evaluation & tutorials, Configuration management, Email & collaboration, and Investigations. The main pane displays a 'Multi-stage incident involving Initial access & Later...' with tabs for Attack story, Alerts (16), Assets (5) (selected), Investigations (1), Evidence and Response (23), and Summary. The Assets section shows 'All assets (5)' with categories: Devices (1), Users (3), Mailboxes (1), and Apps (0). A detailed view for 'win11-01' is shown on the right, listing device details like Device name (win11-01), Device id (7fe462eb87759ae3d3bb8ed349c8349c00dc41), Risk level (None), and logs for most logons (labadmin, labadmin). A context menu is open with options such as Report device inaccuracy, Run Antivirus Scan, Collect Investigation Package, Restrict App Execution, Initiate Automated Investigation, Initiate Live Response Session, Isolate Device, Ask Defender Experts, Action center, Download force release from isolation script, Go hunt, Turn on troubleshooting mode, and Policy sync.

Figure 9.51 – Device remediation actions

The screenshot shows the Microsoft 365 Defender interface. The navigation menu is identical to Figure 9.51. The main pane displays a 'Multi-stage incident involving Initial access & Lateral movement on one endpoint reported by multiple sources' with tabs for Attack story, Alerts (16), Assets (5), Investigations (1), and Evidence (23). The Evidence section shows 'All evidence (23)' with categories: URLs (1), Files (4) (selected), Processes (16), Verdict, Remediation, and Suspicious. A detailed view for 'WinATP-Intro-Backdoor.exe' is shown on the right, labeled as 'Suspicious'. It shows VirusTotal detection ratio (0/0), Malware detect (None), and File verdict (-). A context menu is open with options such as Stop and Quarantine File, Ask Defender Experts, Manual actions, Go hunt, and Submit to deep analysis.

Figure 9.52 – File actions

The screenshot shows the Microsoft 365 Defender interface. The navigation menu is identical to previous figures. The main pane displays an 'Incidents' section with a message about changing alert types. Below it is a table titled 'Most recent incidents and alerts' with columns: Incident name, Incident Id, Tags, Severity, Investigation state, and Category. One row is selected: 'Multi-stage incident involving Initial access & Lateral movement on one endpoint reported by multiple sources' (Severity: Medium, Investigation state: 2 investigation states, Category: Initial access). A context menu is open for this incident, showing options: Open incident page, Manage incident, and a detailed view of the incident details.

Figure 9.53 – Incident flyout

The screenshot shows the Microsoft 365 Defender interface. On the left is a navigation sidebar with sections like Home, Incidents & alerts (selected), Hunting, Actions & submissions, Threat intelligence, Secure score, Learning hub, Trials, Partner catalog, Assets, Devices, Identities, Endpoints, Vulnerability management, and Partners and APIs. The main area is titled 'Incidents' and shows 'Most recent incidents and alerts'. A flyout window titled 'Manage incident' is open, containing fields for Incident name (Multi-stage incident involving Initial access & Lateral movement on one endpoint...), Incident tags (SOC testing), Assign to (labadmin@m365demolabs.com), Status (Resolved), Classification (Informational: expected activity - Security testing), and Comment (Testing using the Document Drop simulation). At the bottom of the flyout are 'Save' and 'Cancel' buttons.

Figure 9.54 – Manage incident flyout

The screenshot shows the Microsoft 365 Defender interface. The navigation sidebar includes Alerts, Hunting, Actions & submissions, Threat intelligence, Secure score, Learning hub, Trials, Partner catalog, Assets, Endpoints, and Email & collaboration. The main area is titled 'Microsoft 365 Defender' and shows 'Settings > Microsoft 365 Defender > Alert tuning'. On the left, under 'General' settings, there are tabs for Account, Email notifications, Alert service settings, Permissions and roles, Streaming API, and Rules (with 'Alert tuning' selected). The main pane displays the 'Alert tuning' configuration, featuring a table header with columns for Rule name, Type, Service sources, and Scope. A button '+ Add new rule' is visible at the top of the table area.

Figure 9.55 – Microsoft 365 Defender rules

Tune alert

Set alert properties where the rule applies
New rules apply only to new alerts.
[Learn more about alert tuning](#)

AND

Entity Role: Trigger Equals Ip: Custom

OR

IP Equals 12.34.3.21

+ Add filter + Add subgroup

+ Add filter + Add subgroup

Action

Apply tuning for alerts that meet IOC conditions

Hide alert Resolve alert

Name *
Automatically resolve alerts for 12.34.3.21

Comment *
Alerts generated by test system

Save **Cancel**

Figure 9.56 – Alert condition parameters

Microsoft 365 Defender

Incidents & alerts

Multi-stage incident involving Initial access & Late...

Attack story Alerts (16) Assets (5) Investigations (1) Evidence and Response (23) Summary

All evidence (23)

Files (4)

Verdict	Remediation status	File Path
Suspicious		RS4_WinATP-Intro-Invoice.docm
Suspicious		C:\Users\labadmin\Desktop\WinATP-Intro-Backdoor.exe
Suspicious		powershell.exe
Suspicious		C:\Users\labadmin\AppData\Local\Microsoft\Windows\TempCache\Content.Outlook

RS4_WinATP-Intro-Invoice.docm

Open file page + Add indicator Download file ...

Detection

VirusTotal detection ratio 0/60 Malware detected None

File verdict

6 active alerts in 1 incidents

View all incidents & alerts in file page

Instance details

Created Device

File path RS4_WinATP-Intro-Invoice.docm

Object details SHA1

Open file page

Figure 9.57 – Selecting the evidence to be used as an indicator

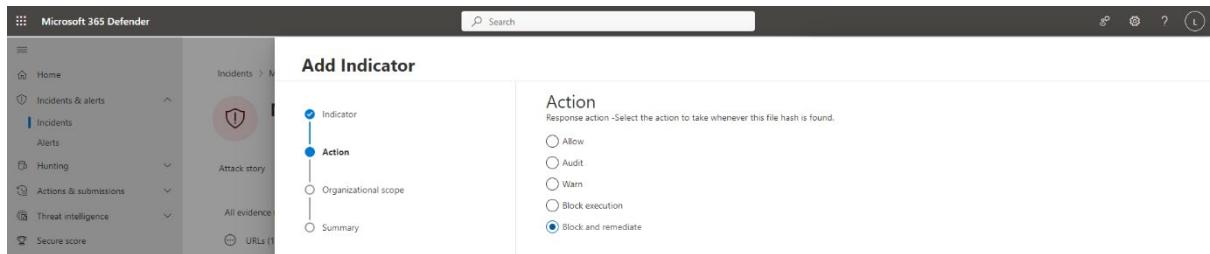


Figure 9.58 – Selecting the Block and remediate action

This screenshot shows a Microsoft 365 Defender dashboard for a 'Multi-stage incident involving Initial access & Late...'. The 'Evidence and Response' tab is active. On the right, a file named 'RS4_WinATP-Intro-Invoice.docm' is shown with a red 'Suspicious' status and a 'INDICATOR RULE' badge. Below the file are options to Open file page, Edit indicator, Download file, etc.

Figure 9.59 – Indicator rule has been created

This screenshot shows the 'Endpoints' settings page in Microsoft 365 Defender. The left sidebar includes sections like Campaigns, Threat tracker, Exchange message trace, Attack simulation training, Policies & rules, Cloud apps, Cloud discovery, Cloud app catalog, OAuth apps, Files, Activity log, Governance log, Policies, Reports, Audit, Health, Permissions, and Settings. The 'Device groups' section is currently selected. The main pane displays a table of device groups, with two entries visible: 'All devices' (rank 1) and 'Ungrouped devices (default)' (rank last). The table columns include Rank, Device group, Devices, Remediation level, Description, and User groups.

Figure 9.60 – Device groups

The screenshot shows the 'Practice Resources' section for Chapter 9. At the top, there's a 'DASHBOARD > CHAPTER 9' navigation bar and a 'SHARE FEEDBACK' button. The main content area is titled 'Implementing and Managing Endpoint Protection by Using Microsoft Defender for Endpoint'. It includes a 'Summary' section with text about the chapter's content and a 'Chapter Review Questions' section. The 'Chapter Review Questions' section is titled 'Chapter Review Questions' and includes a note about the Microsoft 365 Administrator MS-102 Exam Guide by Aaron Gulmette. It features a 'Select Quiz' button, a 'Quiz 1' section with a 'SHOW QUIZ DETAILS' link, and a 'START' button.

Figure 9.61 – Chapter Review Questions for Chapter 9

Chapter 10: Implementing Microsoft Purview Information Protection and Data Lifecycle Management

The screenshot shows the Microsoft Purview interface with the 'Classifiers' page open. The left sidebar includes links for Home, Compliance Manager, Data classification, Classifiers (which is selected), Content explorer, Activity explorer, Data connectors, Alerts, and Policies. The main content area is titled 'Classifiers' and has tabs for 'Trainable classifiers', 'Sensitive info types' (which is selected), and 'EDM classifiers'. A message states: 'The global & available to use in your security and compliance policies. These include a large collection of types we provide, spanning regions around the globe, and types you have created.' Below this are buttons for '+ Create sensitive info type', '+ Create Fingerprint based SIT', and a 'Refresh' button. A search bar shows '313 items' and a search icon. The table lists two entries: 'ABA Routing Number' (Entity, Microsoft Corporation) and 'ASRNET Machine Key' (Credential, Microsoft Corporation). The table has columns for Name, Type, and Publisher.

Figure 10.1 – Classifiers page with Sensitive info types tab selected

The screenshot shows the 'Create sensitive info type' wizard. The left sidebar shows steps: 'Name' (selected), 'Patterns' (selected), 'Recommended confidence level', and 'Finish'. The main content area is titled 'Define patterns for this sensitive info type' with a sub-instruction: 'Sensitive info types are defined by one or more patterns. Each pattern must contain a primary element and confidence level, but you can also include supporting elements and additional checks to further refine the evaluation and detection of matching items. [Learn about defining patterns](#)'. It includes a '+ Create pattern' button, a '0 patterns' count, and a note 'No patterns yet'. A red warning box says 'At least one pattern is required.' Below it is a blue 'Create one now' button. The right side of the screen shows a preview of the 'New pattern' configuration, which includes sections for 'Confidence level' (set to 'Regular expression'), 'Primary element' (set to 'Keyword list'), 'Supporting elements' (set to 'Keyword dictionary'), and 'Additional checks' (set to 'Functions').

Figure 10.2 – Define a pattern

This screenshot is identical to Figure 10.2, showing the 'Create sensitive info type' wizard at the 'Patterns' step. The left sidebar and main content area are the same. The right side shows a detailed view of the 'New pattern' configuration, specifically the 'Primary element' section. A dropdown menu is open under 'Primary element', showing options: 'Regular expression', 'Keyword list' (which is selected), 'Keyword dictionary', and 'Functions'. Below this is a '+ Add primary element' button.

Figure 10.3 – Primary element selection

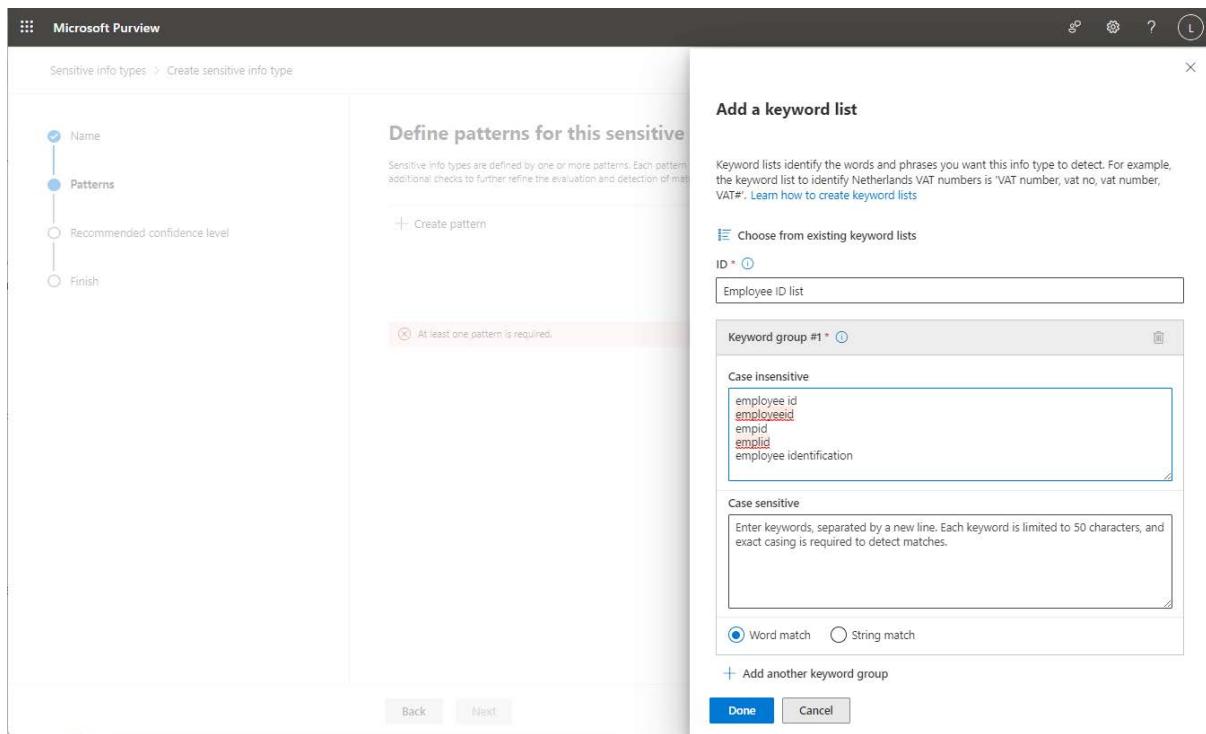


Figure 10.4 – Creating a keyword list

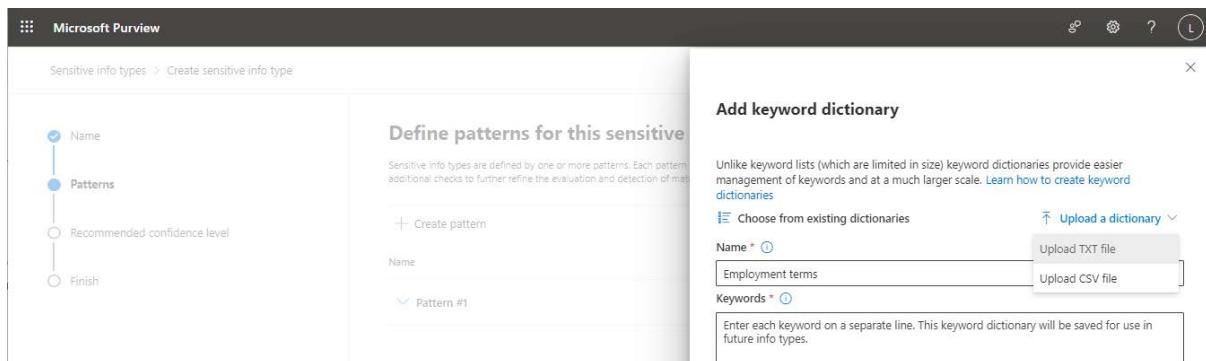


Figure 10.5 – Creating a keyword dictionary

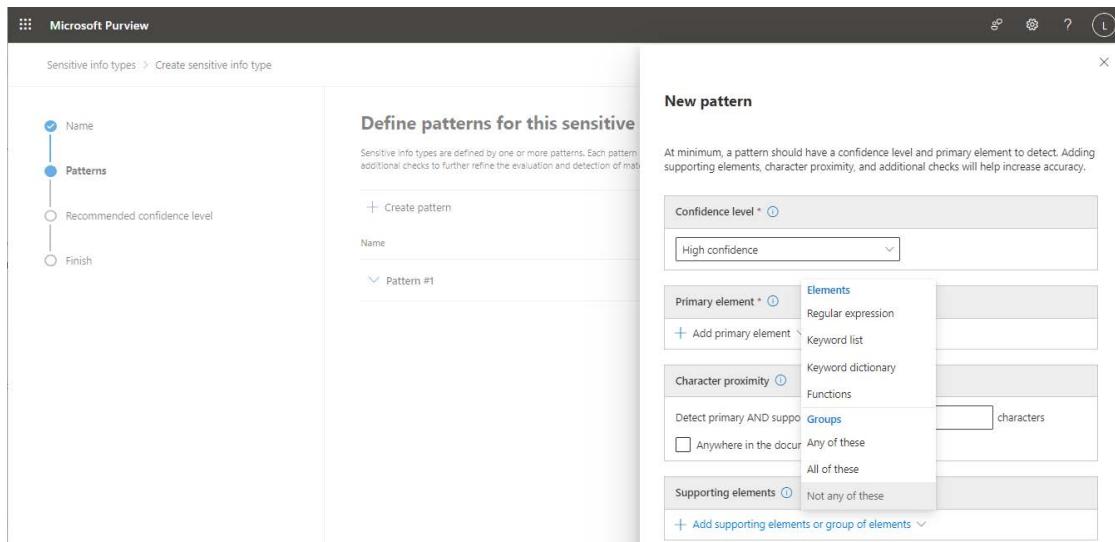


Figure 10.6 – Adding supporting elements

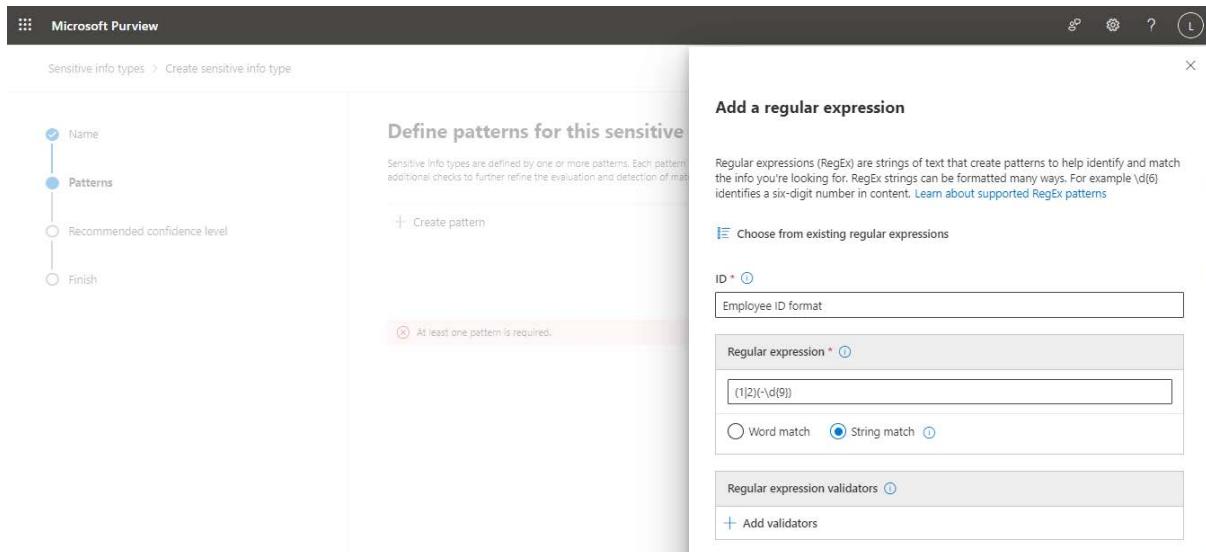


Figure 10.7 – Configuring a regular expression

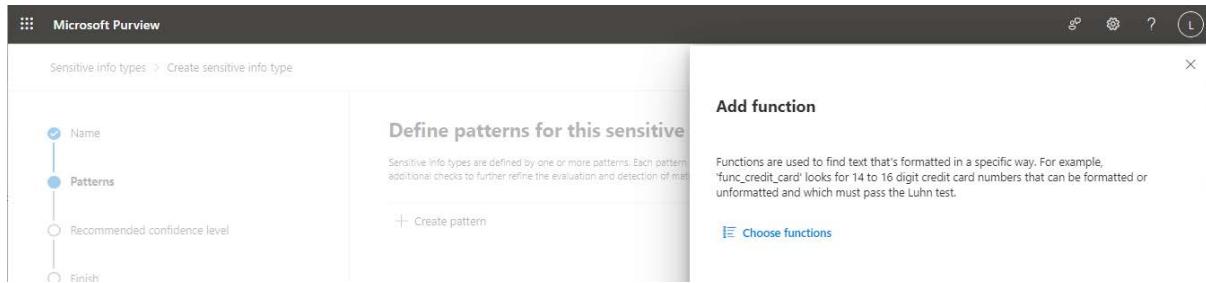


Figure 10.8 – Creating a function-based sensitive information type

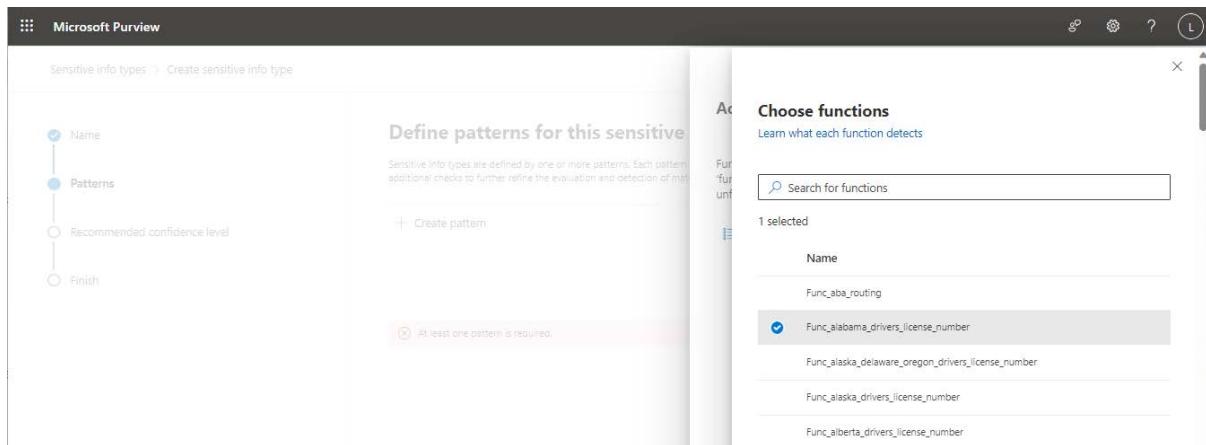


Figure 10.9 – Adding a function

The screenshot shows the Microsoft Purview interface for creating a fingerprint-based sensitive info type. On the left, a vertical navigation bar lists 'Name' (checked), 'Upload file' (selected), and 'Finish'. The main area is titled 'Upload a file to create a fingerprint for the file' with the sub-instruction: 'Fingerprint based SITs are based on the fingerprint of a file. Please upload file for which you would like to create a fingerprint.' A file input field contains 'W2.pdf'. Below it, there are dropdown menus for 'Confidence Level' set to 'Low' (30 & Above), 'Medium' (50 & Above), and 'High' (80 & Above).

Figure 10.10 – Uploading a form for a document fingerprint

The screenshot shows the Microsoft Purview interface for a 'Keyword example' classifier. The left sidebar includes 'Home', 'Compliance Manager', 'Data classification' (selected), 'Classifiers' (highlighted in blue), 'Content explorer', 'Activity explorer', 'Data connectors', 'Alerts', 'Policies', 'Roles & scopes', 'Trials', 'Solutions', and 'Catalog'. The main content area shows the 'Keyword example' classifier details. It includes tabs for 'Overview' (selected) and 'Matched items'. A 'Test' button is available. The 'Details' pane on the right provides information such as 'Description' (This is an example sensitive info type using keywords), 'Confidence level' (High), 'Created by' (M365 Demo Labs), 'Pattern #' (Primary element: Keyword list: Employee ID terms), and 'Character proximity' (Detect primary AND supporting elements within 300 characters). The 'Feedback results' section shows '0 Items with feedback', '0 Match', and '0 Not a match'.

Figure 10.11 – Classifier information page

The screenshot shows the Microsoft Purview interface for testing the 'Keyword example' classifier. The left sidebar is identical to Figure 10.11. The main content area is titled 'Upload file to test "Keyword example"'. It shows the uploaded file 'emplid.txt' and a 'Upload file' button. The 'Testing these sensitive info types' section lists '• Keyword example'.

Figure 10.12 – Uploading a sample file

The screenshot shows the Microsoft Purview interface. On the left, there's a navigation sidebar with various options like Home, Compliance Manager, Data classification, Classifiers, Content explorer, Activity explorer, Data connectors, Alerts, Policies, Roles & scopes, and Trials. The main area is titled 'Keyword example' under 'Classifiers > Sensitive info types'. It has tabs for 'Overview' (which is selected) and 'Matched items'. Below this is a 'Recommendation' section with a 'Provide feedback to improve' button. To the right, there's a 'Match results' panel with a heading 'We have detected the following in emplid.txt'. It lists two sections: '1. Keyword example' (Low - 2 unique matches) and '2. Keyword example' (Medium - 2 unique matches). Each section shows 'Matches' and 'Supporting elements' for terms like 'employee identification' and 'employee id'.

Figure 10.13 – Reviewing the match detections



Figure 10.14 – The principles of retention

The screenshot shows the Microsoft Purview interface with the 'Data lifecycle management' tab selected in the navigation bar. The left sidebar includes 'Solutions', 'Catalog', 'Audit', 'Content search', 'Communication compliance', 'Data loss prevention', 'eDiscovery', 'Data lifecycle management' (which is expanded to show 'Microsoft 365' and 'Exchange (legacy)'), and 'Microsoft 365'. The main area is titled 'Data lifecycle management' and has tabs for 'Overview', 'Retention policies' (which is selected), 'Labels', 'Label policies', 'Policy lookup', and 'Import'. A note says 'Your users create a lot of content every day, from emails to Teams and Yammer conversations. Use retention policies to keep the content you want and get rid of what you don't need.' Below this is a message about role group permissions. At the bottom, there's a table for 'Retention policies' with columns for 'Name', 'Created by', and 'Last modified'. One item is listed: '7 Year' created by 'MOD Administrator' on 'Jul 29, 2023 2:24 PM'.

Figure 10.15 – Retention policies tab

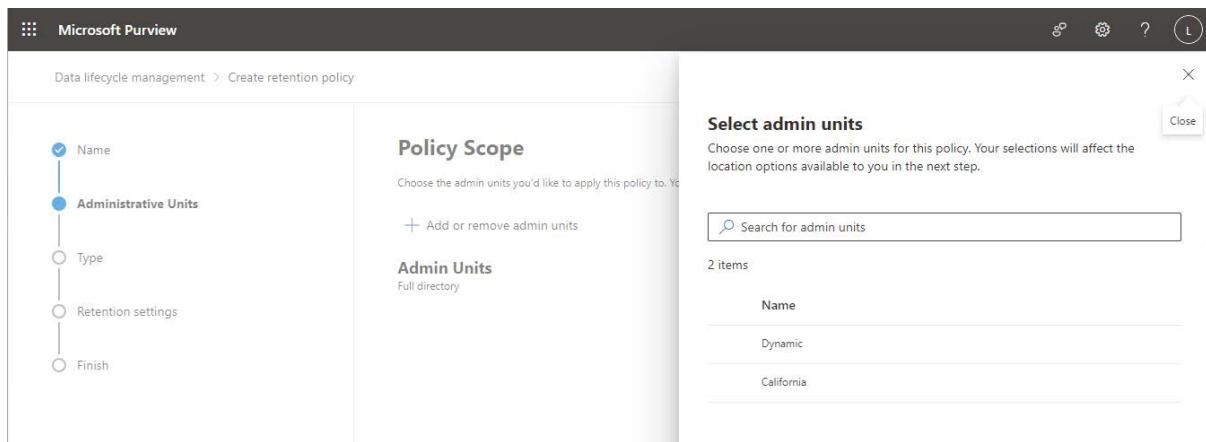


Figure 10.16 – Selecting administrative units

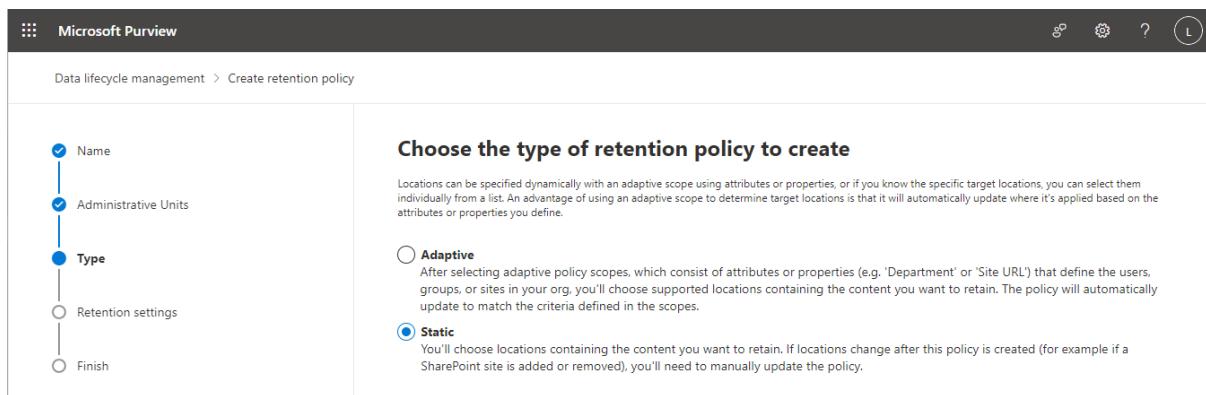


Figure 10.17 – Selecting the policy type

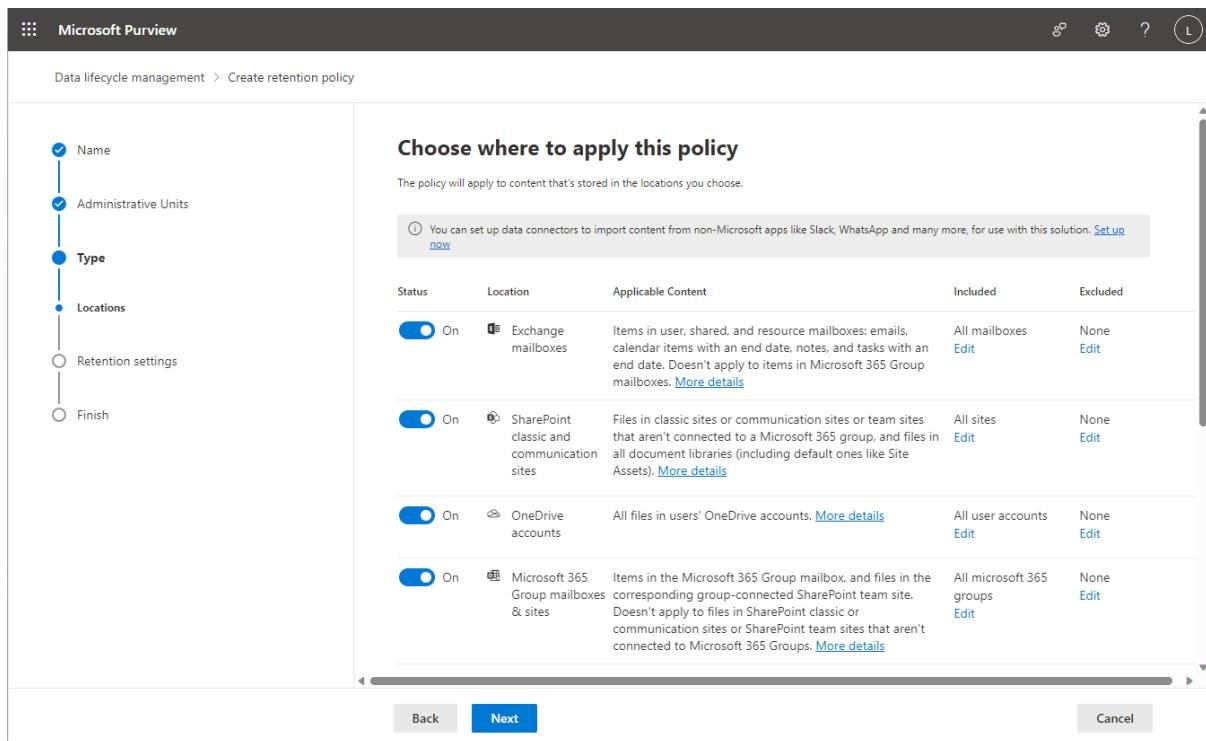


Figure 10.18 – Selecting workloads for policies

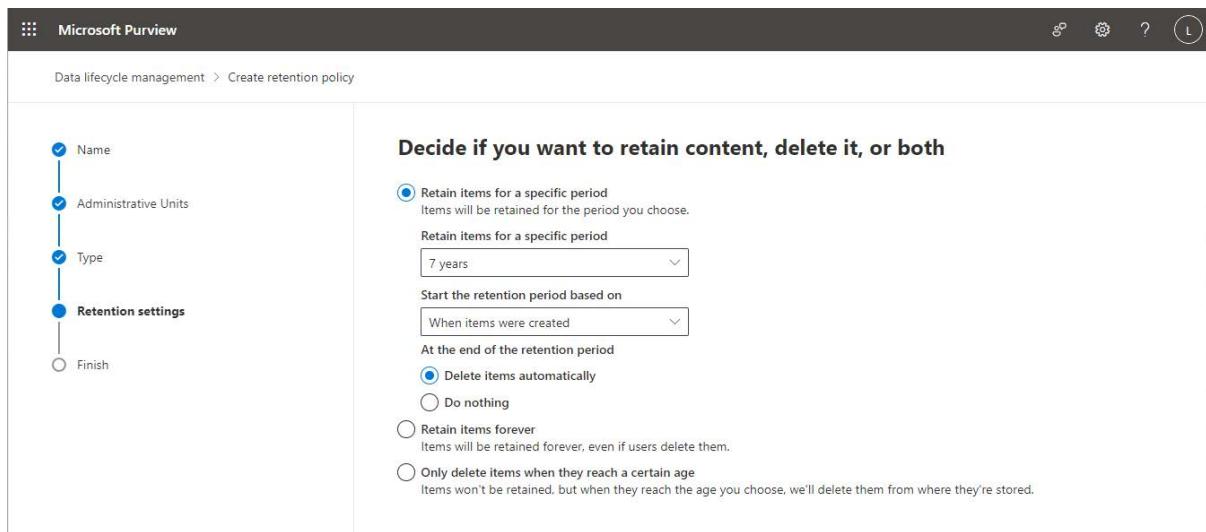


Figure 10.19 – Specifying the retention settings

Figure 10.20 – Using the Labels tab

Figure 10.21 – Selecting label settings

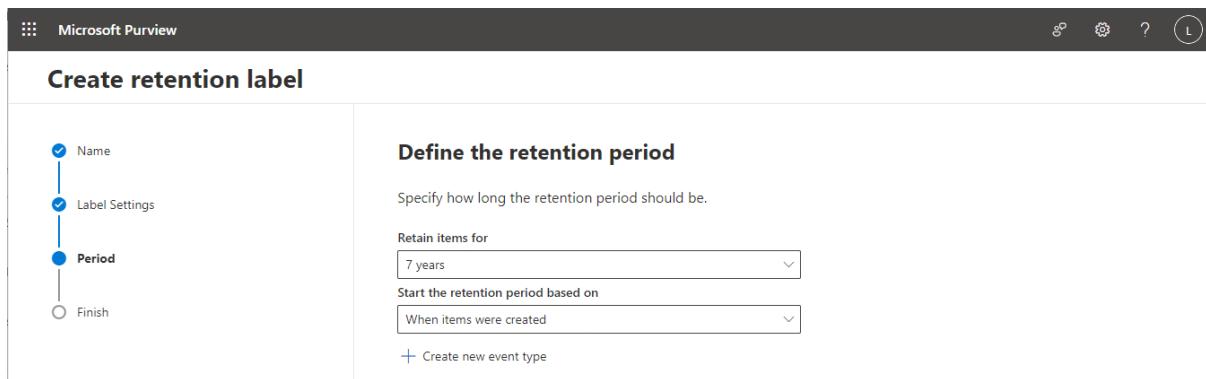


Figure 10.22 – Defining a retention period

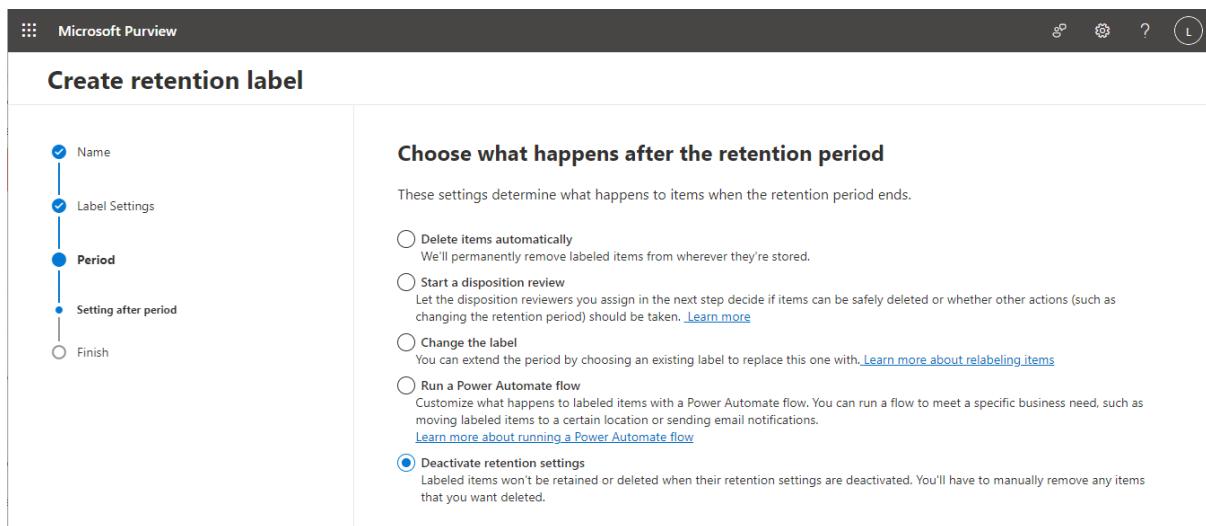


Figure 10.23 – Choosing what happens when the retention period expires

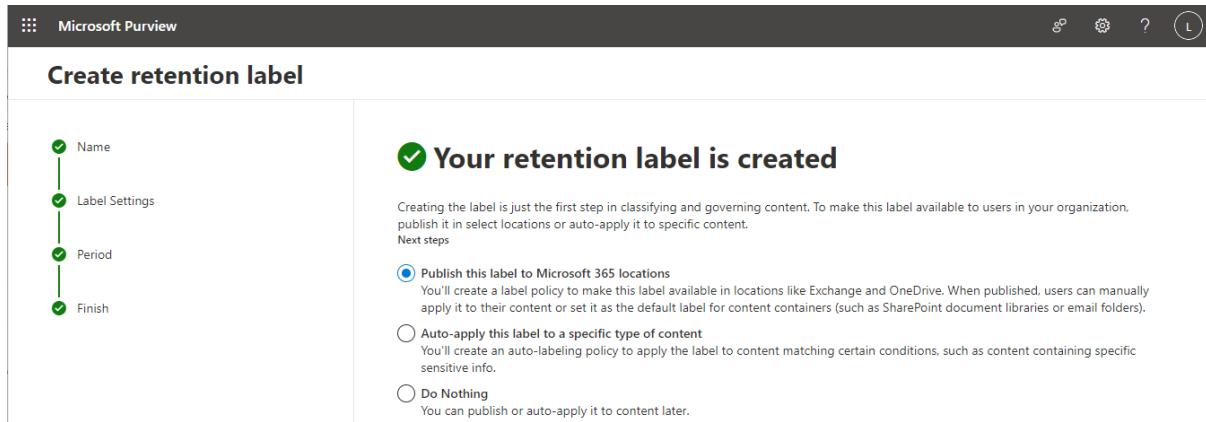


Figure 10.24 – Publishing options

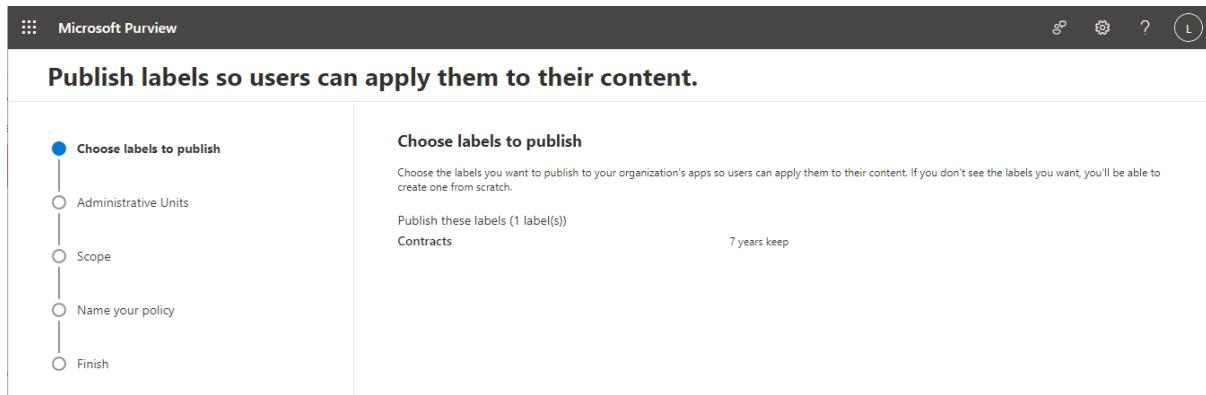


Figure 10.25 – Choosing a label to publish

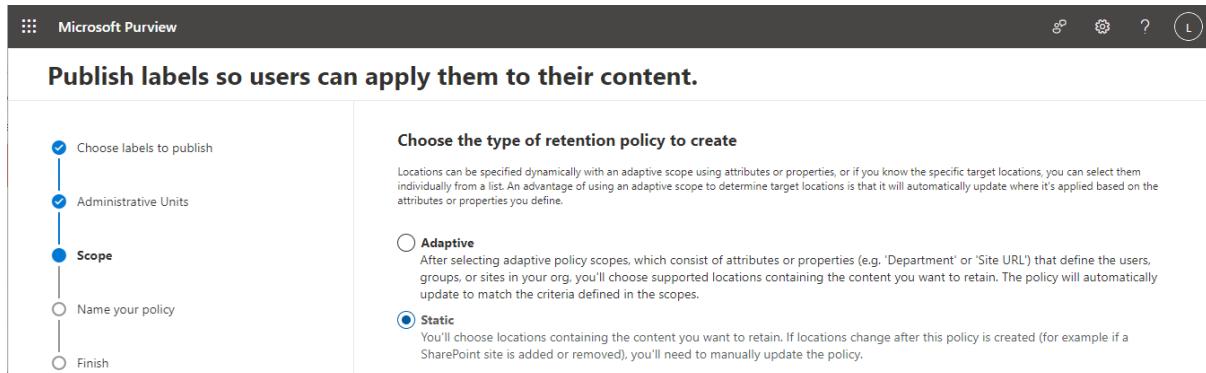


Figure 10.26 – Selecting a scope for the policy

Name	Status	Type	Created by	Last mod...	Last modified
Contracts	Enabled	Publish	labadmin	labadmin	10/18/2023

Figure 10.27 – Label policies tab

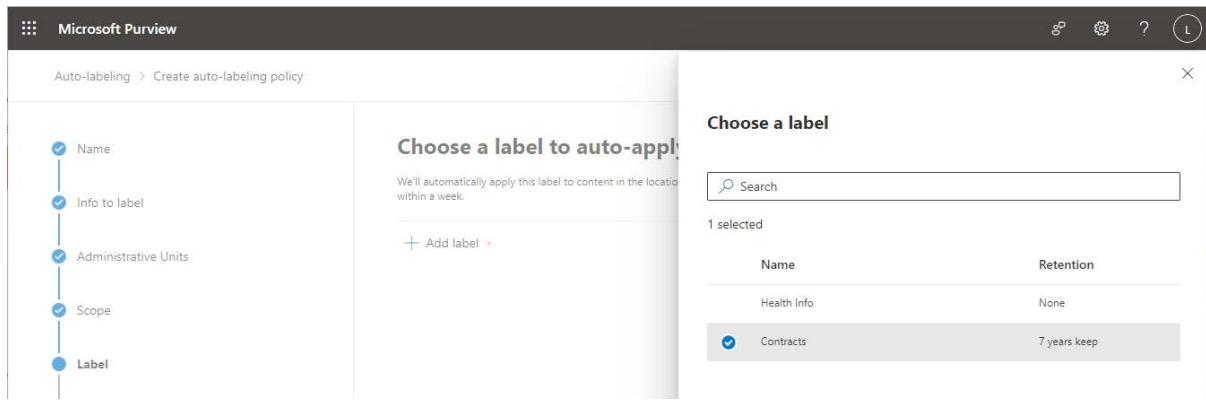


Figure 10.28 – Selecting a label

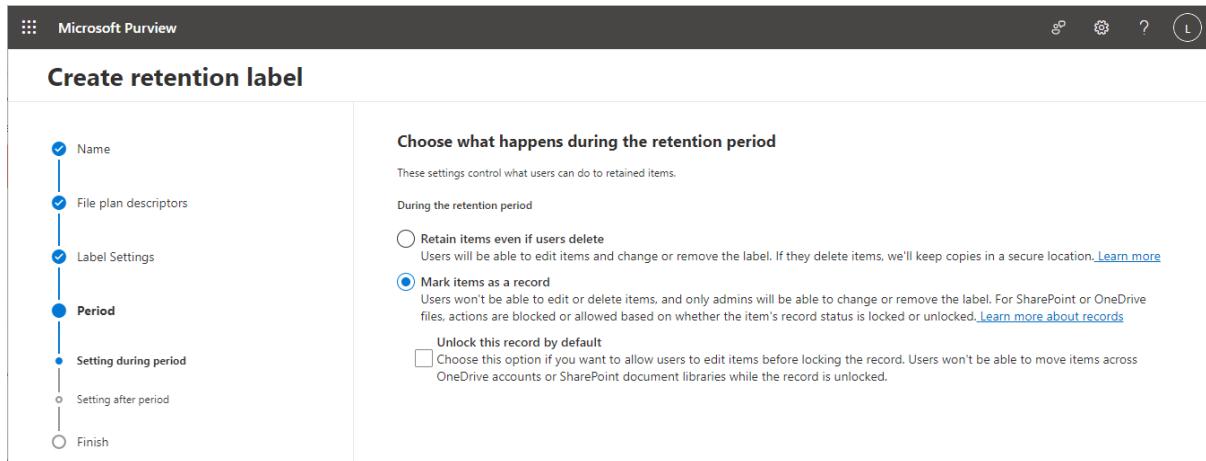


Figure 10.29 – Creating a retention label that marks items as a record

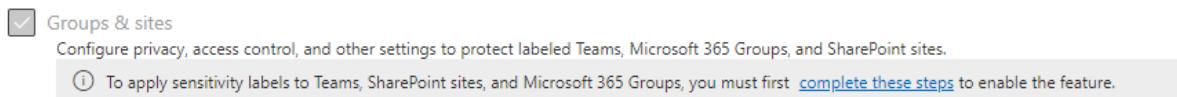


Figure 10.30 – Notice displayed when creating a sensitivity label

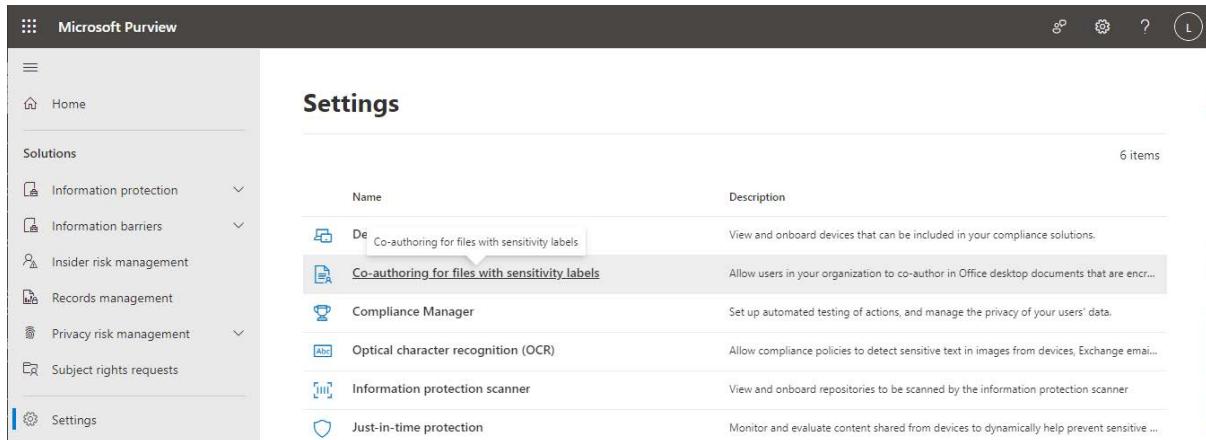


Figure 10.31 – Selecting the Co-authoring for files with sensitivity labels setting

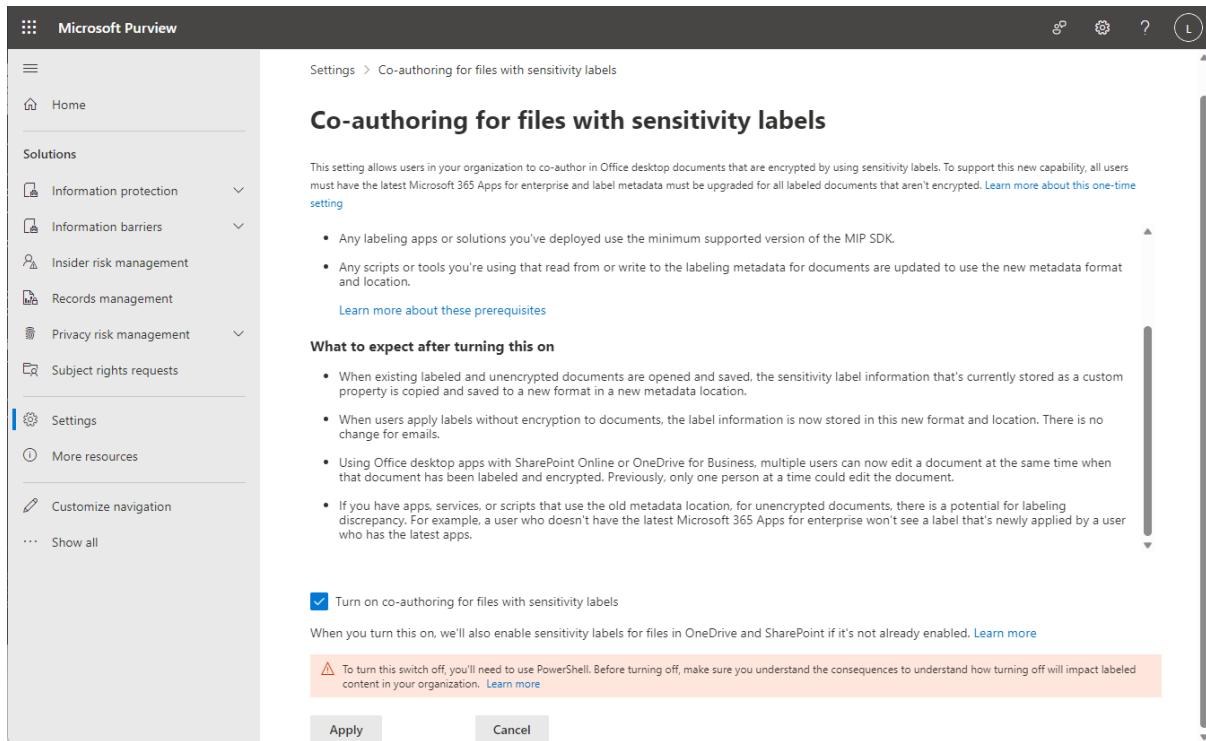


Figure 10.32 – Confirming co-authoring settings

The screenshot shows the Microsoft Purview Labels home page. The left sidebar has sections for Content search, Communication compliance, Data loss prevention, eDiscovery, Data lifecycle management (with sub-options Overview, Labels, Label policies, Auto-labeling), and Information protection. The main area is titled "Labels" and contains a note about creating sensitivity labels. It lists "Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is grouped based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites." Below this is a "Create a label" button and a table showing existing labels: Personal (Priority 0 - lowest, File, Email, Jan 21, 2023 6:52:33 AM), Public (Priority 1, File, Email, Jan 21, 2023 6:52:33 AM), and General (Priority 2, File, Email, Jan 21, 2023 6:52:34 AM). The table has columns for Name, Priority, Scope, Created by, and Last modified.

Figure 10.33 – Selecting Create a label from the Labels home page

New sensitivity label

protected wherever they go, whether they're saved in the cloud or downloaded to a computer.

Name and tooltip

- Name and tooltip
- Scope
- Items
- Groups & sites
- Schematized data assets (preview)
- Finish

Name * [?](#)
Public

Display name * [?](#)
Public

Description for users * [?](#)
Content is suitable for public distribution.

Description for admins [?](#)
Enter a description that's helpful for admins who will manage this label

Label color
The color selected below is currently applied to the parent label. As a result, all sublabels of the parent label will inherit the same color. If you want to use a different color, edit the parent label. [Learn more about label color](#)

Next **Cancel**

Figure 10.34 – Creating a new sensitivity label

New sensitivity label

Define the scope for this label

Labels can be applied directly to items (such as files, emails, meetings), containers like SharePoint sites and Teams, Power BI items, schematized data assets, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. [Learn more about label scopes](#)

Name and tooltip

Scope

Items
Be aware that restricting the scope to only files or emails might impact encryption settings and where the label can be applied. [Learn more](#)

- Files**
Protect files created in Word, Excel, PowerPoint, and more.
- Emails**
Protect messages sent from all versions of Outlook.
- Meetings**
Protect calendar events and meetings scheduled in Outlook and Teams.

Parent label will automatically inherit meeting scope from sub labels

Groups & sites
Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

Schematized data assets (preview)
Apply labels to files and schematized data assets in Microsoft Purview Data Map. Schematized data assets include SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and more.

Figure 10.35 – Defining the scope of the label

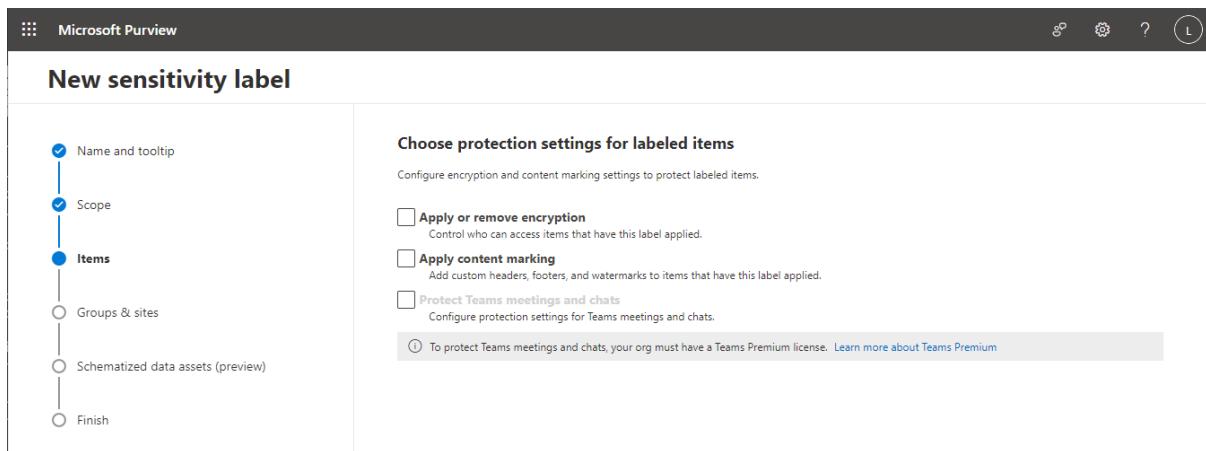


Figure 10.36 – Choosing protection settings

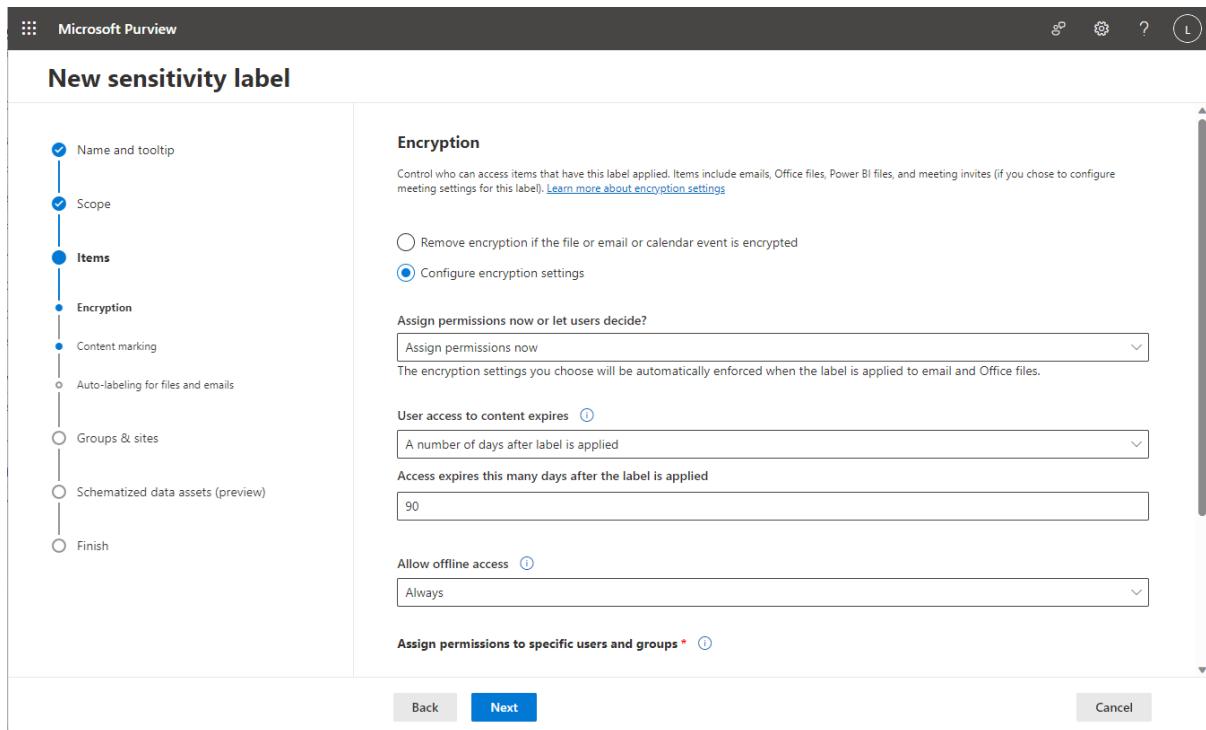


Figure 10.37 – Choosing encryption settings

New sensitivity label

Content marking

Add custom headers, footers, and watermarks to content that has this label applied. [Learn more about content marking](#)

All content marking will be applied to documents but only the header and footer will be applied to email messages. If you chose to configure meeting settings for this label, the header and footer will also be applied to meeting invites.

Content marking

Add a watermark

Customize text
Private

Add a header

Add a footer

Customize text
This is private content.

Figure 10.38 – Applying content marking settings

New sensitivity label

Auto-labeling for files and emails

When users edit Office files or compose, reply to, or forward emails from Outlook that contain content matching the conditions you choose here, we'll automatically apply this label or recommend that they apply it themselves. [Learn more about auto-labeling for Microsoft Purview](#)

We'll also apply this label to files that match the same conditions in Azure Blob Storage, Azure Files, Azure Data Lake Storage, and Amazon S3. [Learn more about auto-labeling in Microsoft Purview Data Map](#)

To automatically apply this label to files that are already saved (in SharePoint and OneDrive) or emails that are already processed by Exchange, you must create an auto-labeling policy. [Learn more about auto-labeling policies](#)

Auto-labeling for files and emails

Since encryption is turned on, a large amount of content might be automatically encrypted when this label is applied. Turning on encryption impacts Office files (Word, PowerPoint, Excel) and PDF files that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. [Learn more](#)

Detect content that matches these conditions

Add condition

Recommended labeling and displaying a message to users is supported only for Office apps. This label will be automatically applied to files in Microsoft Purview Data Map, but no message will be displayed.

When content matches these conditions

Back **Next** **Cancel**

Figure 10.39 – Enabling auto-labeling

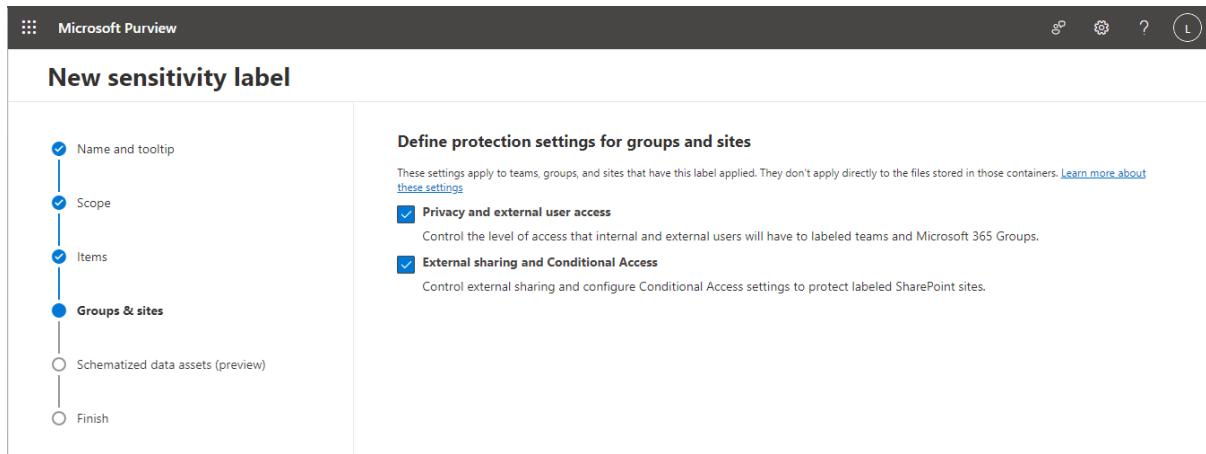


Figure 10.40 – Defining protections for groups and sites

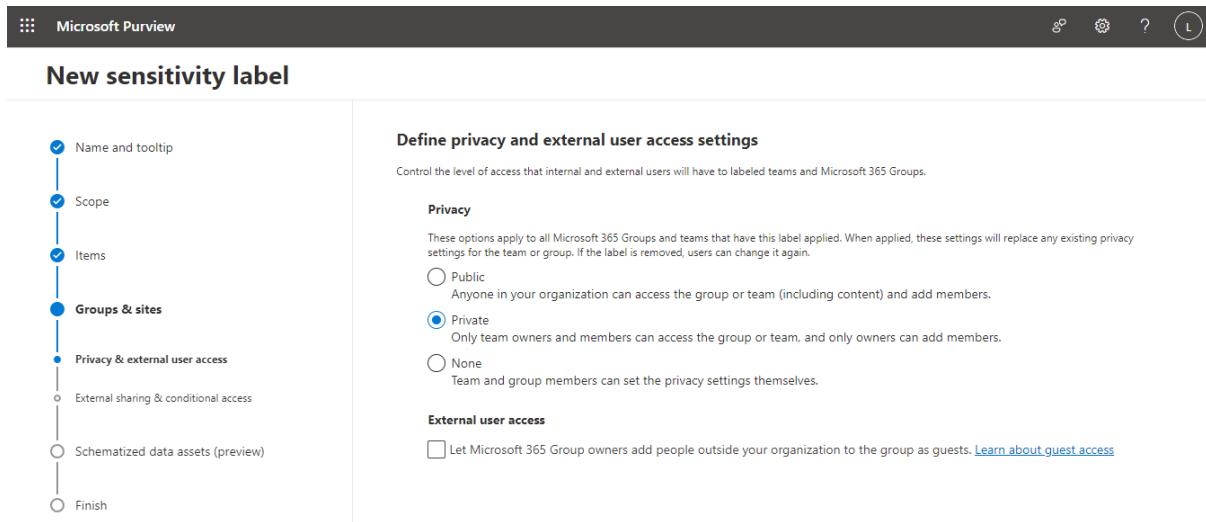


Figure 10.41 – Configuring privacy and external access settings

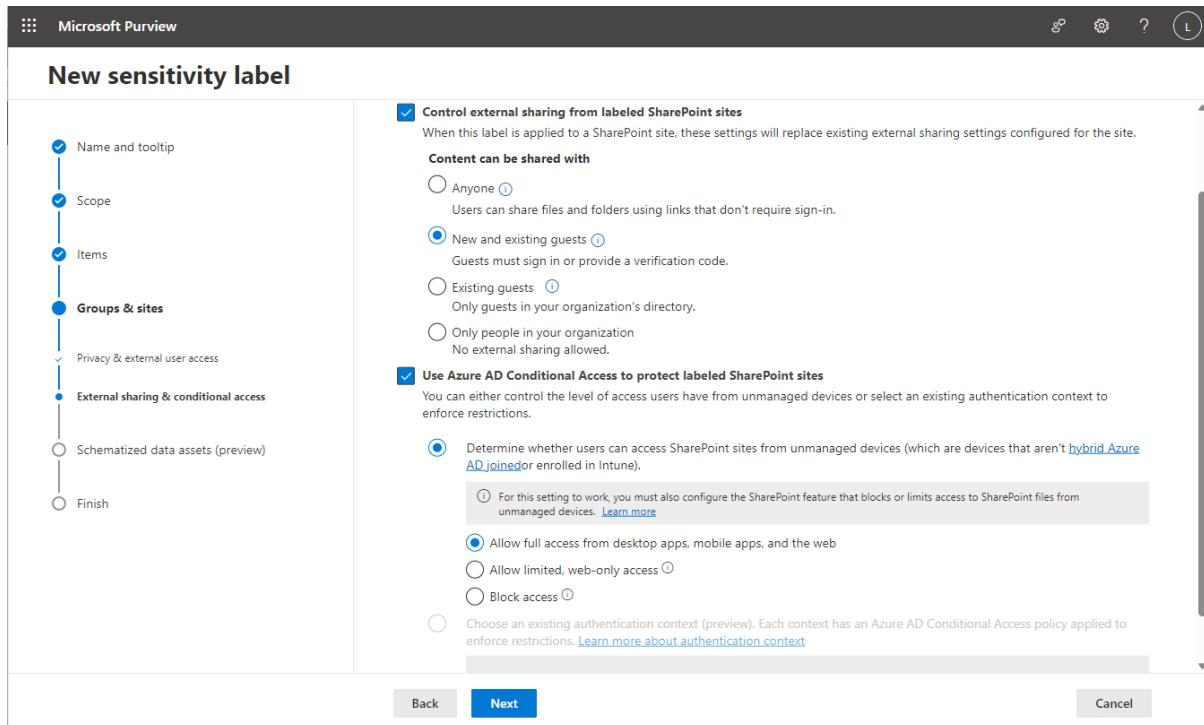


Figure 10.42 – Configuring external sharing and Conditional Access controls

Name	Priority	Scope	Created by	Last modified
Personal	0 - lowest	File, Email	Jan 21, 2023 6:52:33 AM	
Public	1	File, Email	Jan 21, 2023 6:52:33 AM	
General	2	File, Email	Jan 21, 2023 6:52:34 AM	
Anyone (unrestricted)	3	File, Email	Jan 21, 2023 6:52:34 AM	
All Employees (unrestricted)	4	File, Email	Jan 21, 2023 6:52:35 AM	

Figure 10.43 – Sublabel example

Figure 10.44 – Creating a sublabel

New sensitivity label

- Name and tooltip
- Scope
- Items
- Groups & sites
- Schematized data assets (preview)
- Finish

Parent label

Name * (Required)

Display name * (Required)

Description for users * (Required)

Description for admins (Optional)

Label color
The color selected below is currently applied to the parent label. As a result, all sublabels of the parent label will inherit the same color. If you want to use a different color, edit the parent label. [Learn more about label color](#)

Next
Cancel

Figure 10.45 – Reviewing name and tooltip settings

Label policies

If your role group permissions are restricted to a specific set of users or groups, you'll only be able to manage policies for those users or groups. [Learn more about role group permissions](#)

Publish label **Refresh** 3 items

Name	Priority	Created by	Last modified
<input type="checkbox"/> Global sensitivity label policy	0 - lowest	Jan 21, 2023 6:52 AM	
<input type="checkbox"/> Confidential-Finance Policy	1	MOD Administrator	Jan 21, 2023 7:31 PM
<input type="checkbox"/> Highly Confidential Policy	2 - highest	MOD Administrator	Jan 21, 2023 7:31 PM

Figure 10.46 – Publishing a label

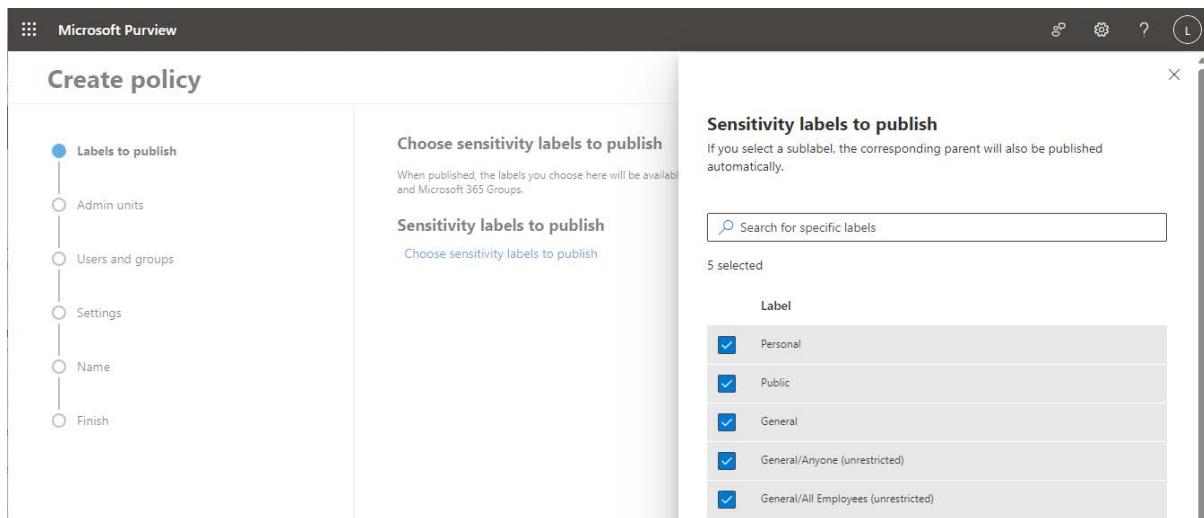


Figure 10.47 – Selecting labels to publish

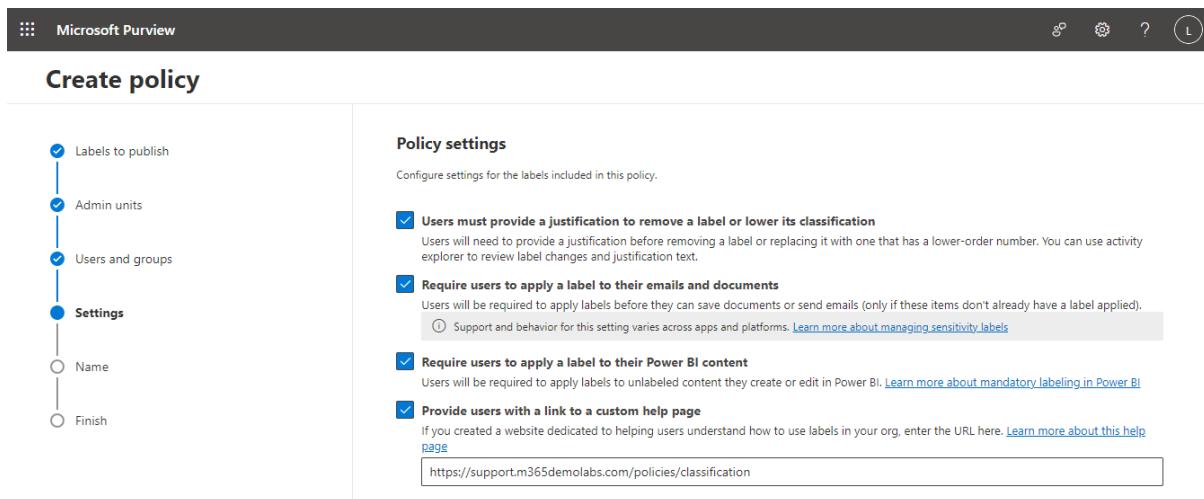


Figure 10.48 – Configuring policy settings

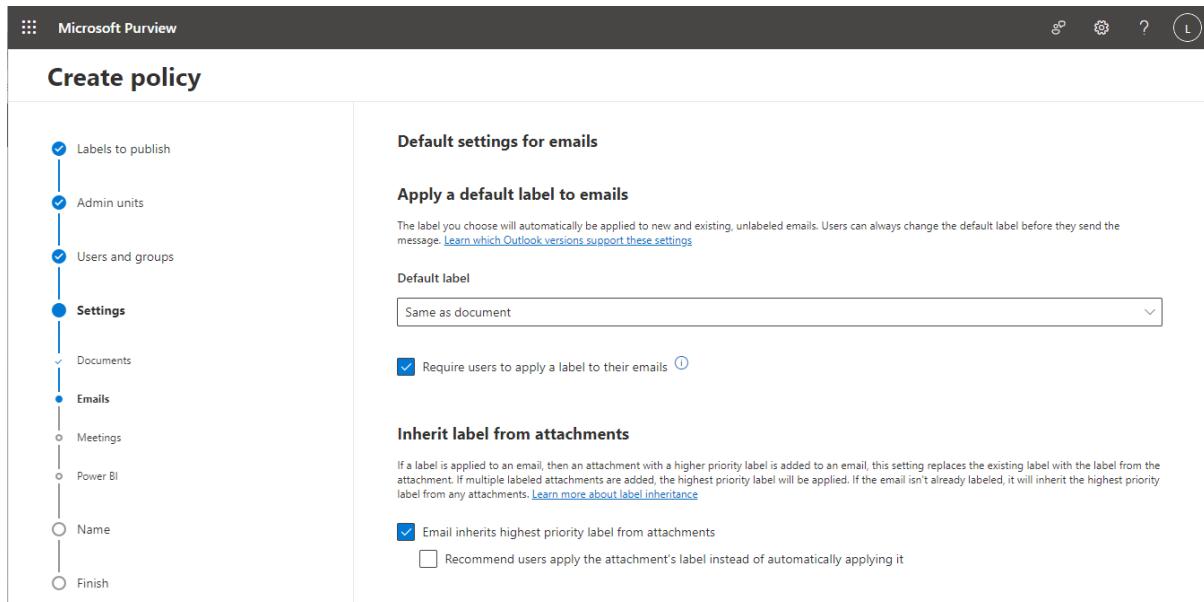
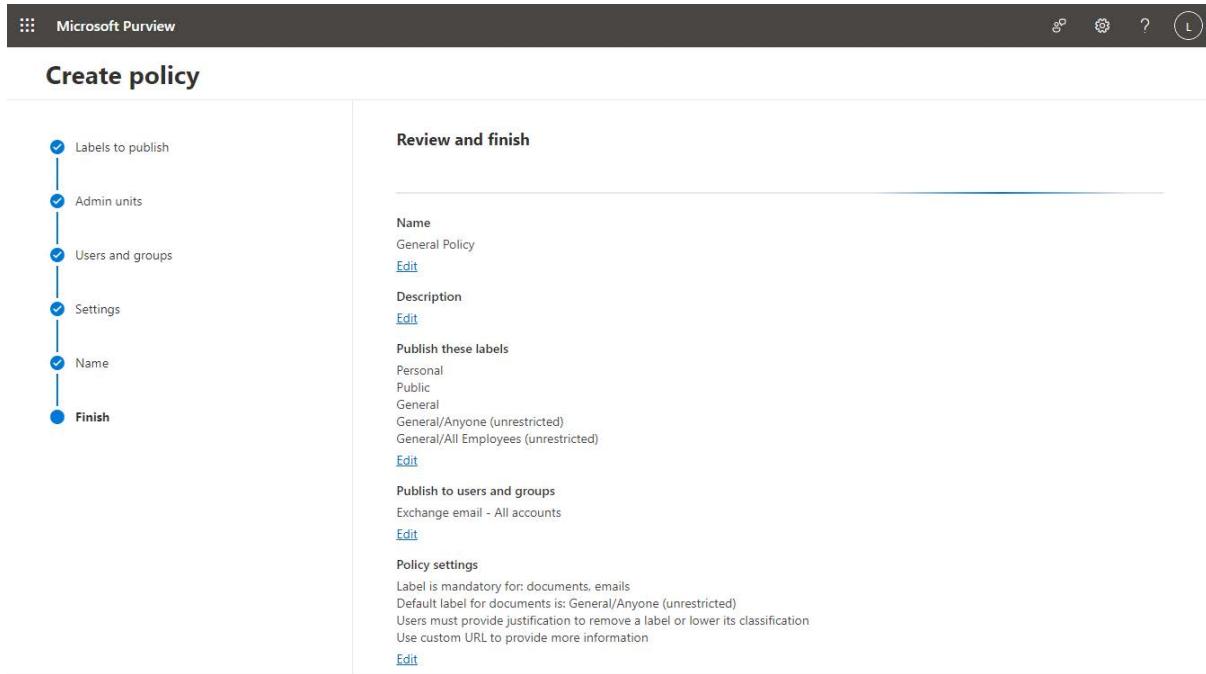


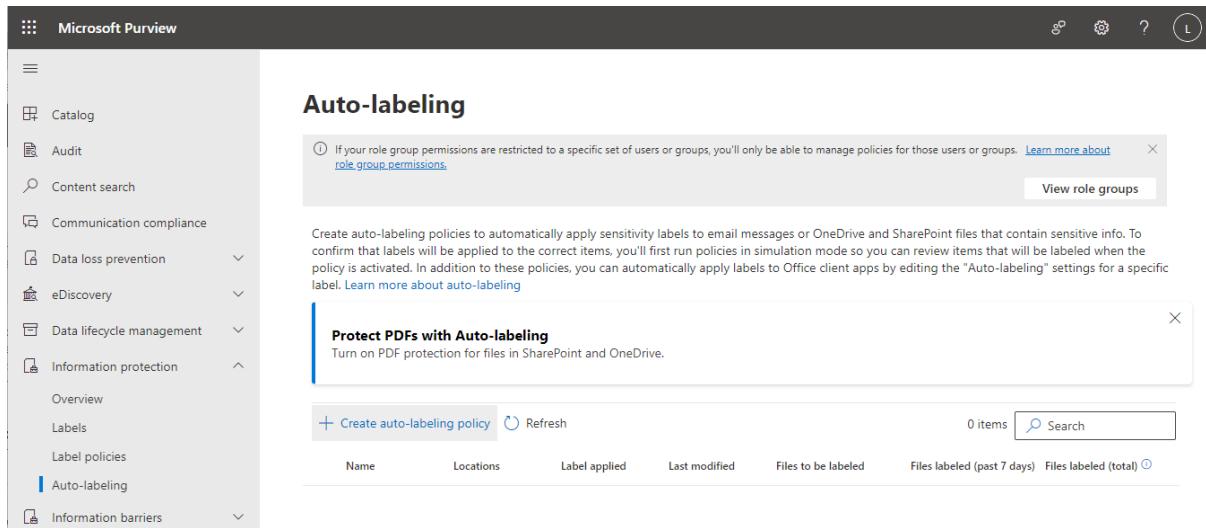
Figure 10.49 – Configuring email settings



The screenshot shows the 'Create policy' process in Microsoft Purview. On the left, a vertical checklist shows steps completed: 'Labels to publish', 'Admin units', 'Users and groups', 'Settings', 'Name', and 'Finish'. The 'Finish' step is highlighted with a blue circle. On the right, the 'Review and finish' section displays the final settings:

- Name:** General Policy
- Description:**
- Publish these labels:** Personal, Public, General, General/Anyone (unrestricted), General/All Employees (unrestricted)
- Publish to users and groups:** Exchange email - All accounts
- Policy settings:** Label is mandatory for: documents, emails; Default label for documents is: General/Anyone (unrestricted); Users must provide justification to remove a label or lower its classification; Use custom URL to provide more information

Figure 10.50 – Reviewing the final settings



The screenshot shows the 'Auto-labeling' page in Microsoft Purview. The left sidebar includes options like Catalog, Audit, Content search, Communication compliance, Data loss prevention, eDiscovery, Data lifecycle management, Information protection, Labels, Label policies, Auto-labeling (which is selected and highlighted in blue), and Information barriers.

The main area is titled 'Auto-labeling' and contains the following content:

- A note: "If your role group permissions are restricted to a specific set of users or groups, you'll only be able to manage policies for those users or groups." with a link to "role group permissions". A "View role groups" button is also present.
- A description: "Create auto-labeling policies to automatically apply sensitivity labels to email messages or OneDrive and SharePoint files that contain sensitive info. To confirm that labels will be applied to the correct items, you'll first run policies in simulation mode so you can review items that will be labeled when the policy is activated. In addition to these policies, you can automatically apply labels to Office client apps by editing the 'Auto-labeling' settings for a specific label." with a link to "Learn more about auto-labeling".
- A sub-section titled "Protect PDFs with Auto-labeling" with the sub-instruction "Turn on PDF protection for files in SharePoint and OneDrive."
- A button to "+ Create auto-labeling policy".
- A refresh button.
- A table header with columns: Name, Locations, Label applied, Last modified, Files to be labeled, Files labeled (past 7 days), and Files labeled (total).
- A search bar with placeholder "Search".

Figure 10.51 – Selecting Create auto-labeling policy

The screenshot shows the Microsoft Purview Auto-labeling interface for creating a new policy. On the left, a sidebar lists steps: Info to label (selected), Name, Admin units, Locations, Policy rules, Label, Policy mode, and Finish. The main area is titled "Choose info you want this label applied to". It includes a search bar, a dropdown for "All countries or regions", and a table with "Categories" (Enhanced, Financial, Medical and health, Privacy, Custom) and "Templates" (Australia Privacy Act Enhanced, Australia Personally Identifiable Information (PII) Data, Canada Personally Identifiable Information (PII) Data, Canada Personal Information Protection Act (PIPA), Canada Personal Information Protection Act (PIPEDA), France Data Protection Act). A note about "U.S. State Breach Notification Laws Enhanced" is present, along with a list of protected information types.

Figure 10.52 – Selecting a category template

The screenshot shows the Microsoft Purview Auto-labeling interface for creating a new policy. The sidebar shows steps: Info to label, Name, Admin units, Locations, Policy rules (selected), Label, and Policy mode. The main area is titled "Set up common or advanced rules". It explains that rules define what content the label is applied to. It offers two options: "Common rules" (selected) and "Advanced rules". "Common rules" details include Credit Card Number, U.S. Bank Account Number, U.S. Driver's License Number, U.S. Social Security Number (SSN), All Full Names, U.S. / U.K. Passport Number, and All Medical Terms And Conditions. "Advanced rules" is described as defining specific rules for each location.

Figure 10.53 – Selecting policy rules

The screenshot shows the Microsoft Purview Auto-labeling interface for creating a new policy. The sidebar shows steps: Info to label, Name, Admin units, Locations, Policy rules, Label (selected), and Policy mode. The main area is titled "Choose a label to auto-apply". It notes that users will see this label applied to files that match rules and conditions. A note cautions that turning on encryption impacts Office files and PDF files. It shows the selected label "Highly Confidential/All Employees" and a "Change" link.

Figure 10.54 – Selecting the label to apply

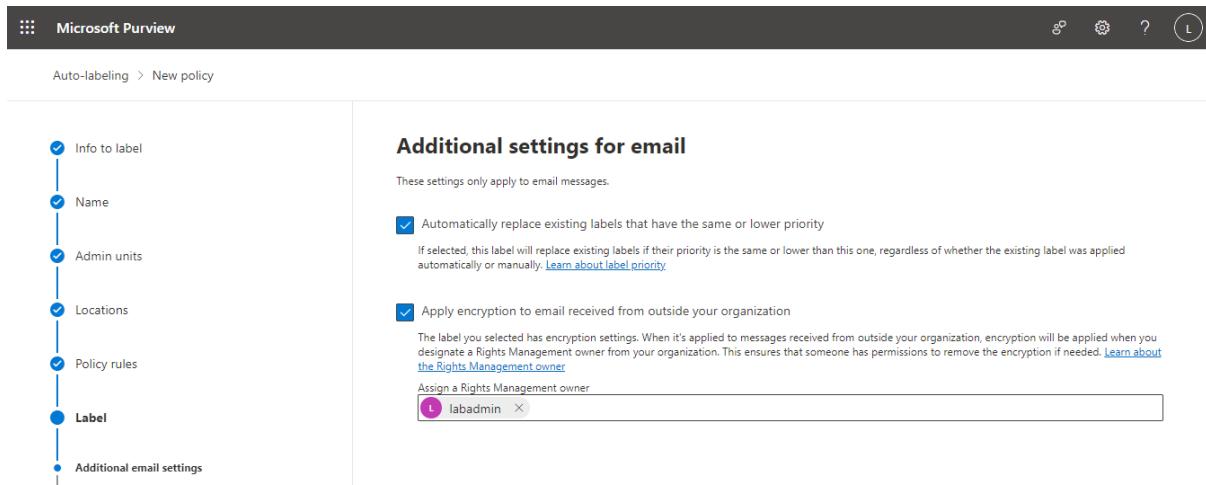


Figure 10.55 – Specifying additional settings for email

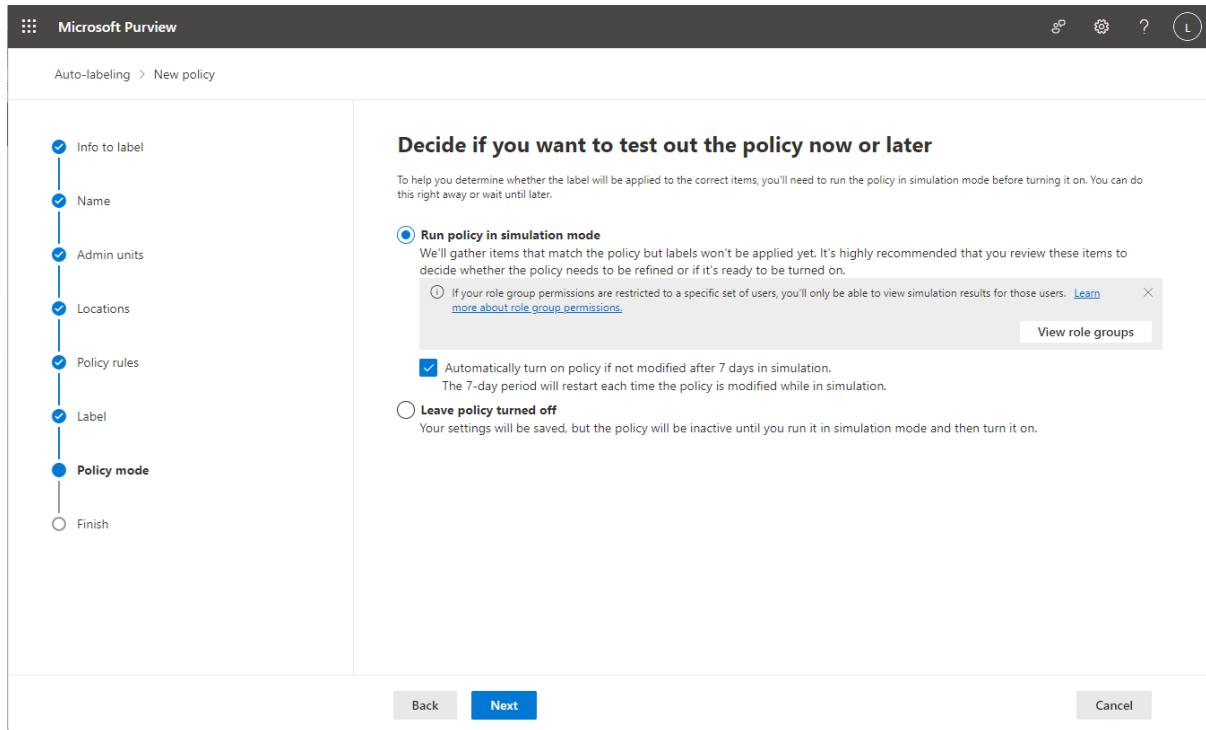


Figure 10.56 – Choosing the policy mode

DASHBOARD > CHAPTER 10

Implementing Microsoft Purview Information Protection and Data Lifecycle Management

Summary

Implementing Microsoft Purview Information Protection and Data Lifecycle Management

Summary: In this chapter, you learned about some of the important compliance tasks that many organizations face, such as content classification and retention. You learned about the foundational technical concepts around **sensitive information types (SITs)**. SITs are used to classify content and can be used in the Microsoft Purview solutions including labeling and retention.

In the next chapter, you'll apply the SIT knowledge learned here to another compliance concept: data loss prevention.

Chapter Review Questions

The Microsoft 365 Administrator MS-102 Exam Guide
by Aaron Guilmette

Select Quiz

Quiz 1

[SHOW QUIZ DETAILS](#) ▾

START

Figure 10.57 – Chapter Review Questions for Chapter 10

Chapter 11: Implementing Microsoft Purview Data Loss Prevention

The screenshot shows the Microsoft Purview Policies page. On the left, there's a navigation sidebar with categories like Data loss prevention, eDiscovery, Data lifecycle management, etc. The main area is titled 'Policies' and contains a table of existing policies:

Name	Order	Last modified	Status
Default Office 365 DLP policy	0	Jan 21, 2023 6:52 AM	On
Default policy for Teams	1	Jan 21, 2023 6:52 AM	On
Privacy Policy	2	Jan 21, 2023 7:29 PM	On
Financial Policy	3	Jan 21, 2023 7:29 PM	On
Medical and health Policy	4	Jul 19, 2023 12:50 PM	On

Figure 11.1 – Microsoft Purview compliance policies page

This screenshot shows the 'Create policy' wizard, step 1: 'Template or custom policy'. The left sidebar lists steps: Name, Admin units (preview), Locations, Policy settings, Policy mode, and Finish. The 'Template or custom policy' option is selected. The main pane shows a search bar and a list of categories and templates. A callout box highlights the 'U.S. Health Insurance Act (HIPAA) Enhanced' template.

Categories	Templates	U.S. Health Insurance Act (HIPAA) Enhanced
Enhanced	Australia Health Records Act (HRIP Act) Enhanced	Helps detect the presence of information subject to United States Health Insurance Portability and Accountability Act (HIPAA). This enhanced template extends the original by also detecting people's full names, medical terms and conditions, and U.S. physical addresses. We have also enhanced this template with Trainable Classifier "Business-Healthcare" which can detect healthcare and medical content in your tenant such as Medical records, Health benefits documents, Insurance forms, Prior authorizations and referral forms.
Financial	Canada Health Information Act (HIA)	
Medical and health	Canada Personal Health Information Act (PHIA) - Manitoba	
Privacy	Canada Personal Health Act (PHIPA) - Ontario	
Custom	U.K. Access to Medical Reports Act	
	U.S. Health Insurance Act (HIPAA) Enhanced	

Figure 11.2 – Selecting a template or policy type

This screenshot shows the 'Create policy' wizard, step 2: 'Assign admin units (preview)'. The left sidebar continues from step 1. The main pane is titled 'Assign admin units (preview)' and contains instructions about assigning admin units. It includes a 'Admin units' section with a 'Full directory' link and a '+ Add or remove admin units' button.

Figure 11.3 – Assigning an administrative unit

Locations

Status	Location	Included	Excluded
On	Exchange email	All Choose distribution group	None Exclude distribution group
On	SharePoint sites	All Choose sites	None Exclude sites
On	OneDrive accounts	All Choose account or distribution group	None Exclude account or distribution group
On	Teams chat and channel messages	All Choose account or distribution group	None Exclude account or distribution group
On	Devices	All Choose user or group	None Exclude user or group
On	On-premises repositories	All Choose repositories	None Exclude repositories
Off	Power BI		

Back **Next** **Cancel**

Figure 11.4 – Adding workloads and locations to the policy

Info to protect

This policy will protect content that matches these conditions. Review them and make any necessary changes. For example, you can edit the conditions to detect additional sensitive info or content that has specific sensitivity or retention labels applied.

Content contains any of these sensitive info types:
 U.S. Social Security Number (SSN)
 Drug Enforcement Agency (DEA) Number
 U.S. Physical Addresses
 And
 Content contains any of these sensitive info types:
 International Classification of Diseases (ICD-9-CM)
 International Classification of Diseases (ICD-10-CM)
 All Medical Terms And Conditions
 And
 Content contains all of these sensitive info types:
 All Full Names
 And
 Content contains any of these sensitive info types:
 Business - Healthcare
 Employee Insurance Files
 Healthy/Medical Forms
 Edit
 Detect when this content is shared from Microsoft 365: With people outside my organization Only with people inside my organization

User's risk level for Adaptive Protection is

Risk levels for Adaptive Protection are defined in insider risk management. They determine how risky a user's activity is and can be based on conditions such as:

Back **Next** **Cancel**

Figure 11.5 – Reviewing the Info to protect page

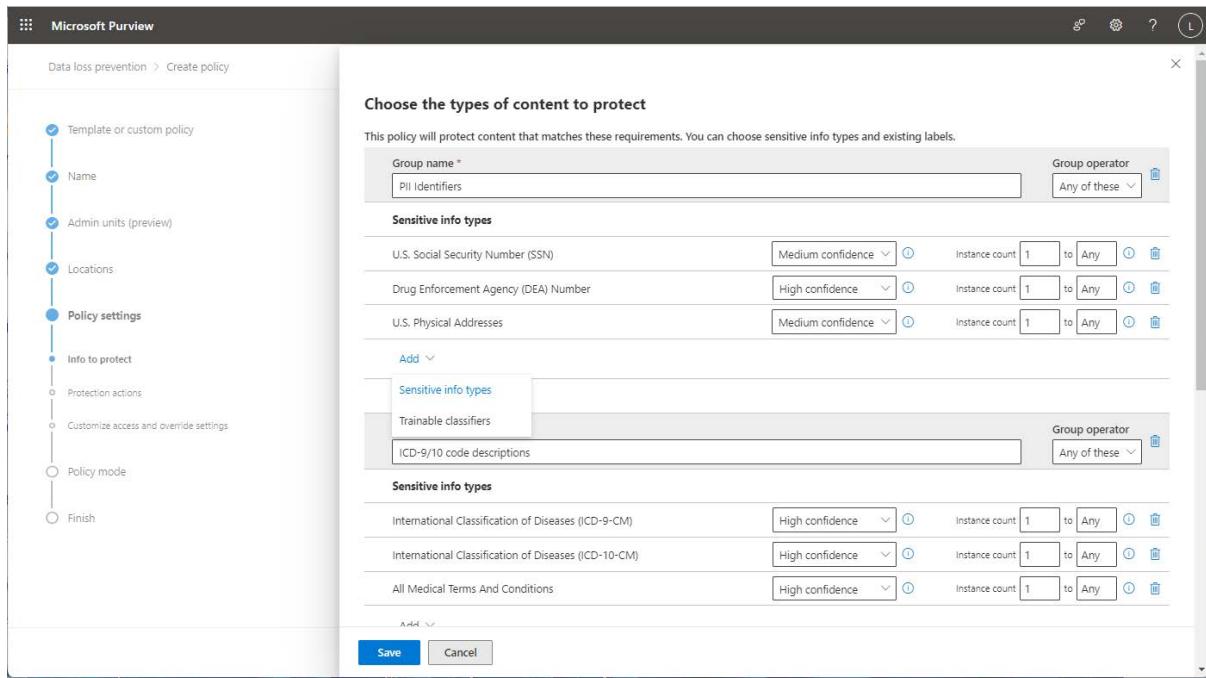


Figure 11.6 – Editing a DLP match rule

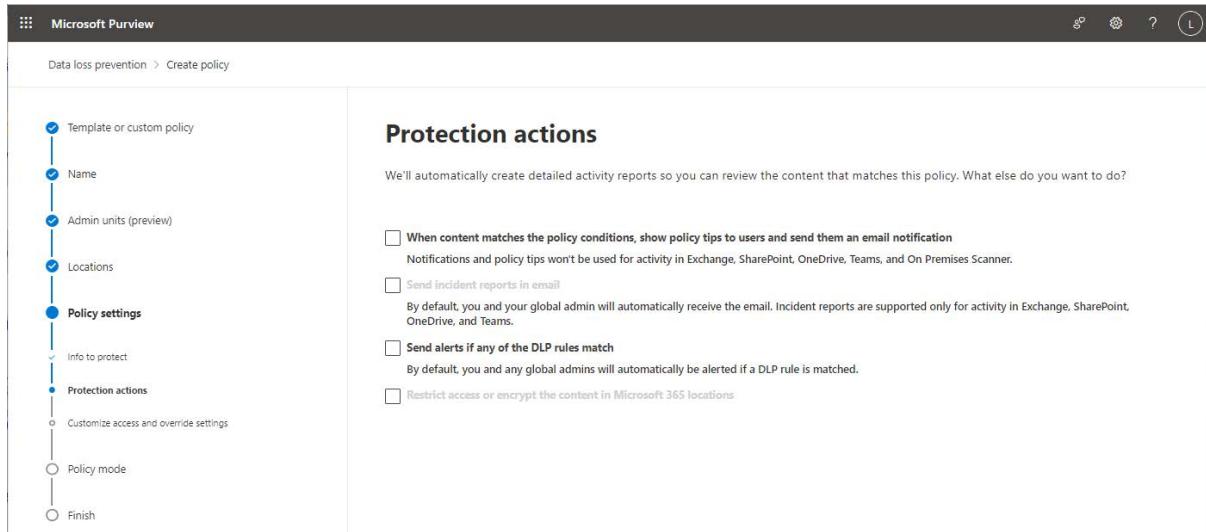


Figure 11.7 – Configuring protection actions

Microsoft Purview

Data loss prevention > Create policy

Template or custom policy

Name

Admin units (preview)

Locations

Policy settings

- ✓ Info to protect
- ✓ Protection actions
- Customize access and override settings
- Policy mode
- Finish

Customize access and override settings

By default, users are blocked from sending email and Teams chats and channel messages that contain the type of content you're protecting. But you can choose who has access to shared SharePoint and OneDrive files. You can also decide if you want to let people override the policy's restrictions.

Restrict access or encrypt the content in Microsoft 365 locations
 Block users from receiving email or accessing shared SharePoint, OneDrive, and Teams files.

Audit or restrict activities on devices
 When specified activities are detected on devices for files containing the sensitive info you're protecting, you can choose to only audit the activity, block it entirely, or block it but allow users to override the restriction.
[Learn more restricting device activity](#)

Service domain and browser activities
 Detects when protected files are blocked or allowed to be uploaded to cloud service domains based on the 'Allow/Block cloud service domains' list in endpoint DLP settings.

Upload to a restricted cloud service domain or access from an unallowed browsers
 Audit only

Choose different restrictions for sensitive service domains

Paste to supported browsers
 Audit only

Choose different restrictions for sensitive service domains

Back Next Cancel

Figure 11.8 – Customize access and override settings

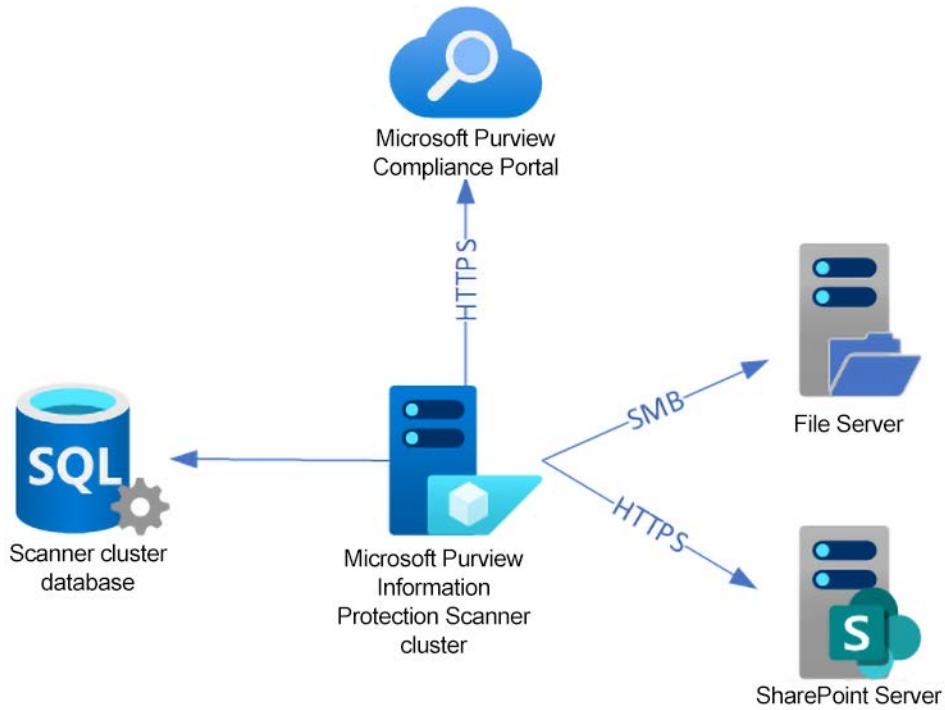


Figure 11.9 – On-premises DLP architecture

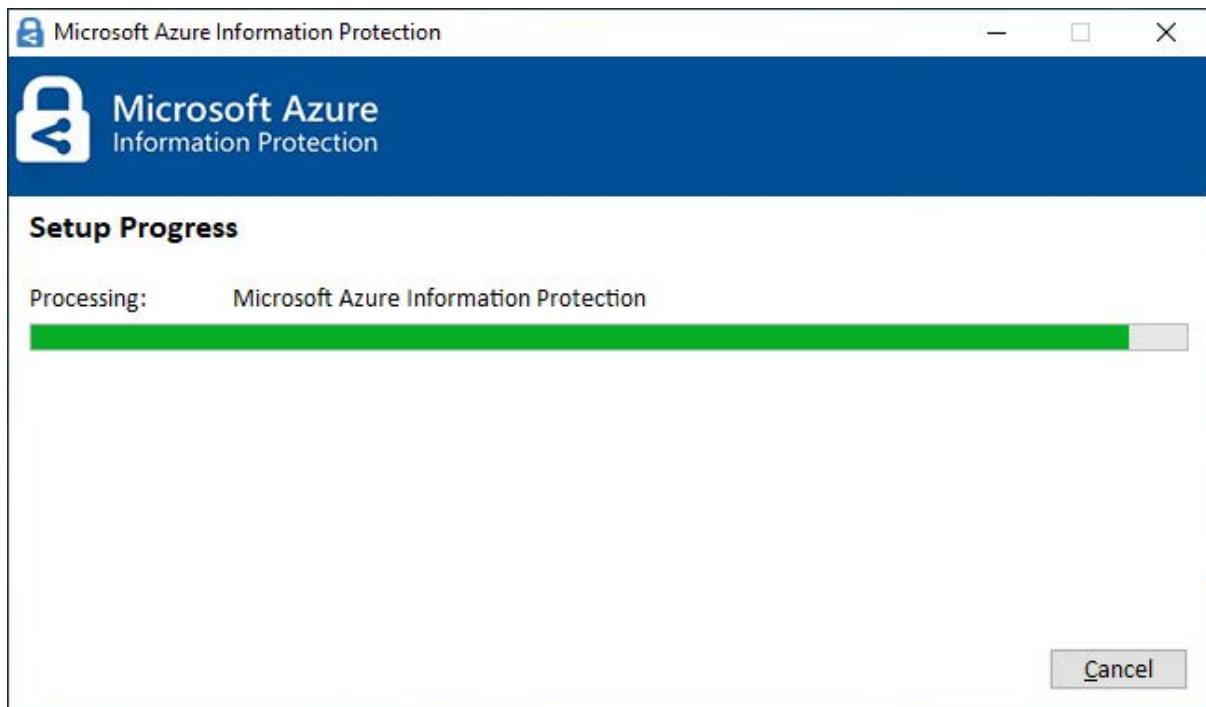


Figure 11.10 – AIP UI client installation

A screenshot of the Microsoft Purview Information protection scanner page. The left sidebar shows "Trials", "Solutions", "Catalog", "Audit", "Content search", "Communication compliance", "Data loss prevention", "eDiscovery", and "Data lifecycle management". The main content area is titled "Information protection scanner" and includes a note about discovering, classifying, and protecting files. It shows a table with one item: a Content scan job named "Content scan job" with 1 node. There are tabs for "Clusters", "Nodes", and "Content scan jobs", and buttons for "+ Add" and "Refresh". A search bar at the top right shows "1 item" and "Search".

Figure 11.11 – AIP clusters page

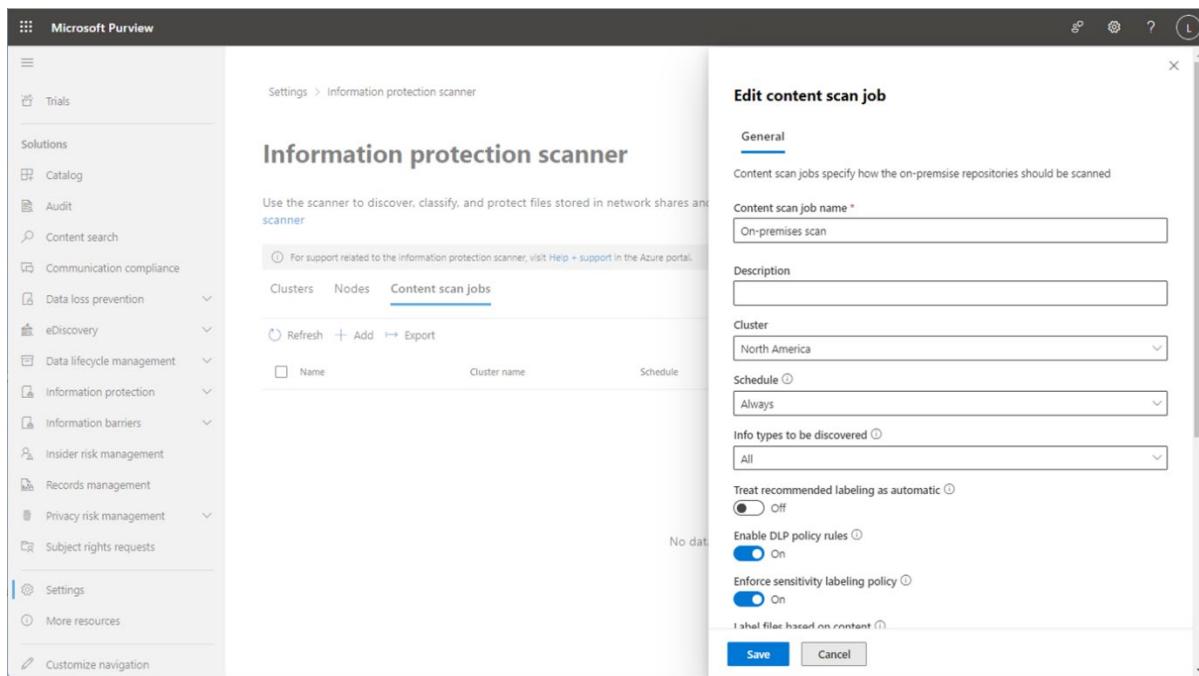


Figure 11.12 – Configuring content scan job settings

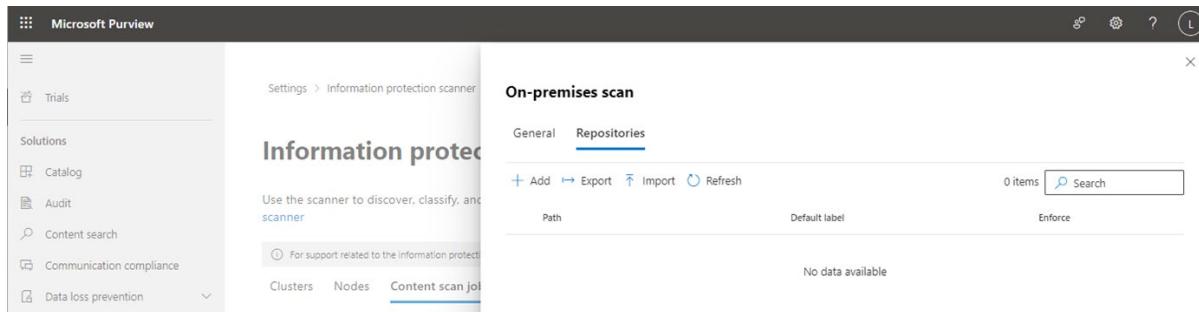


Figure 11.13 – Configuring repositories for the scan

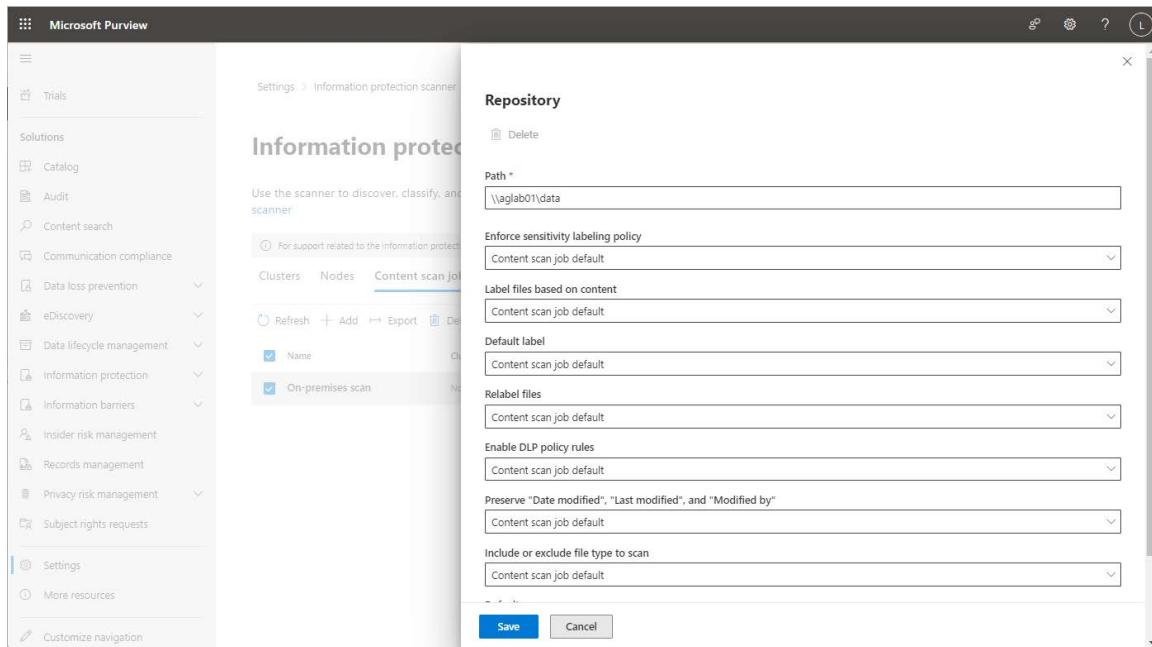


Figure 11.14 – Configuring repository settings

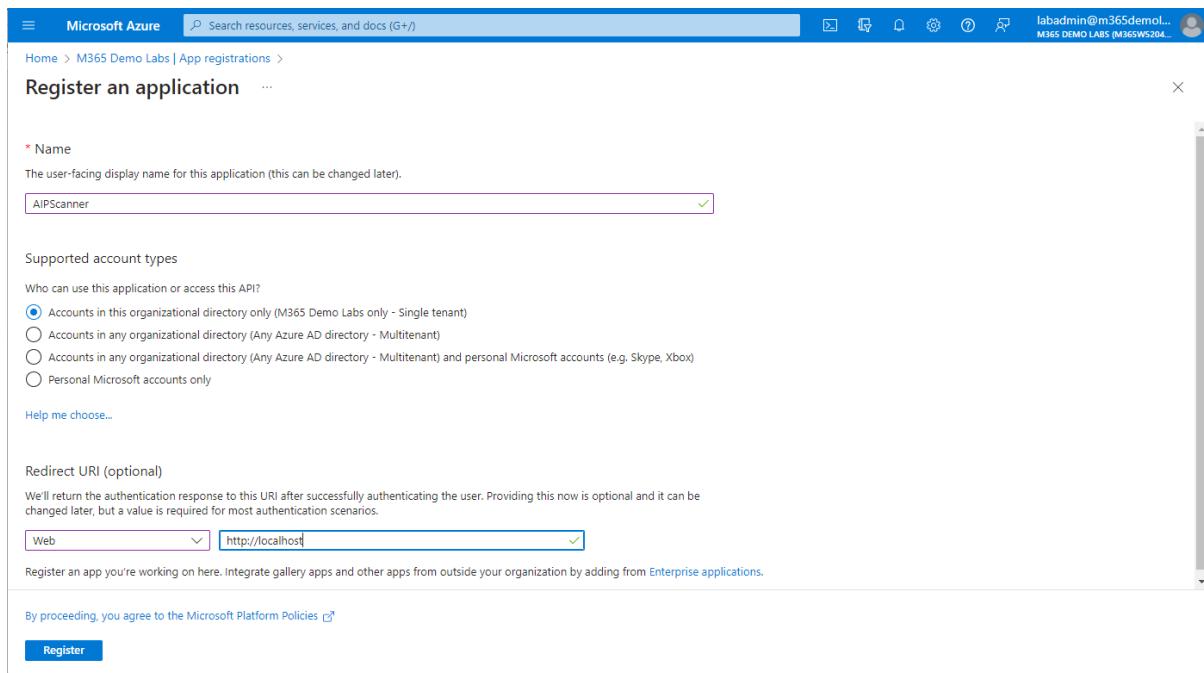


Figure 11.15 – Configuring an app registration

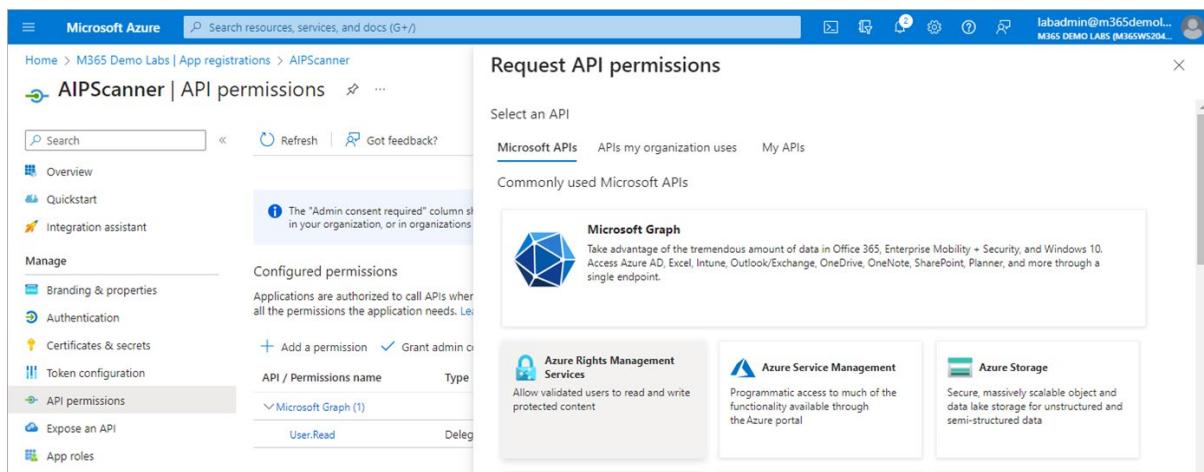


Figure 11.16 – Adding permissions on the Request API permissions flyout

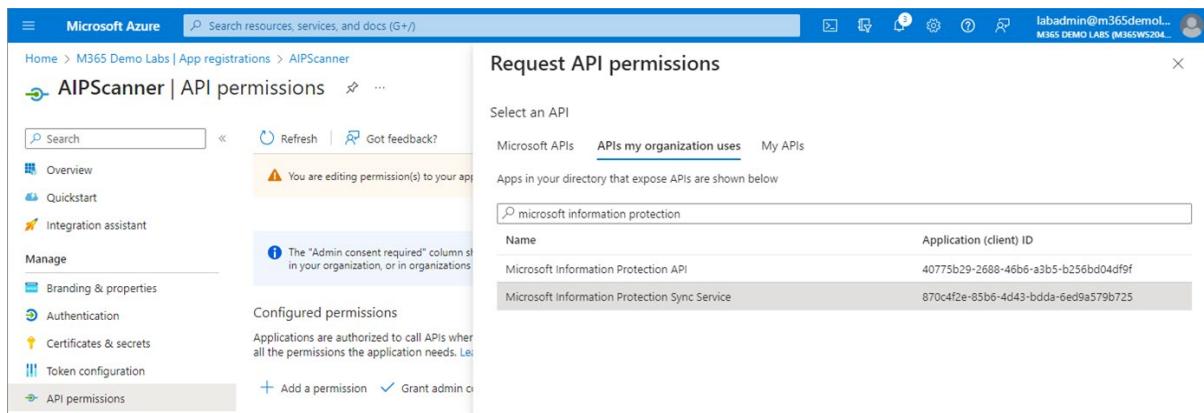


Figure 11.17 – Choosing the Microsoft Information Protection Sync Service API

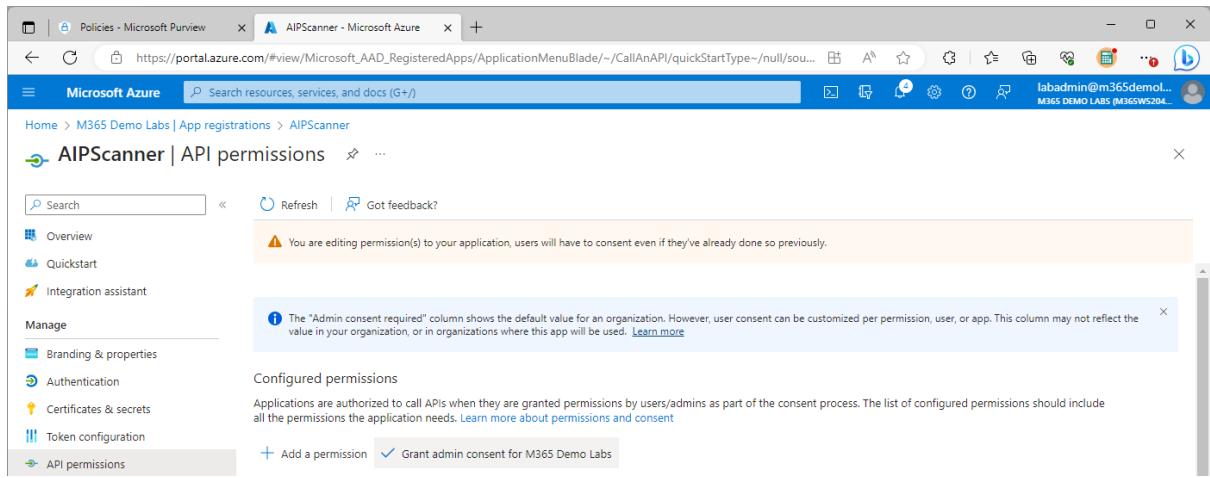


Figure 11.18 – Granting admin consent

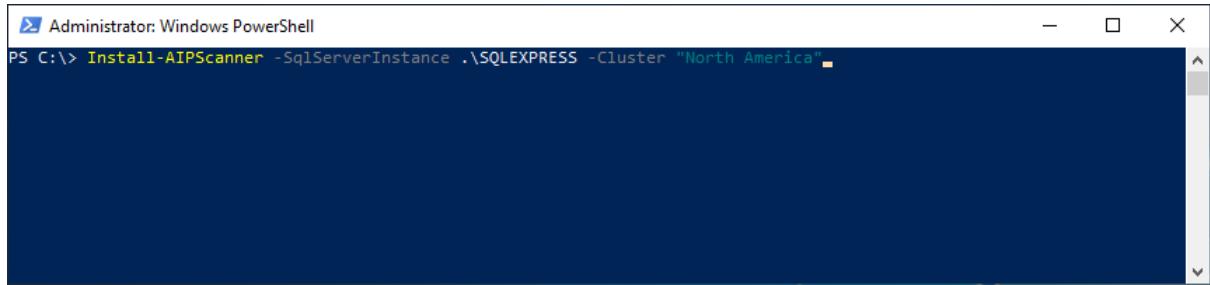


Figure 11.19 – Starting the AIP scanner installation

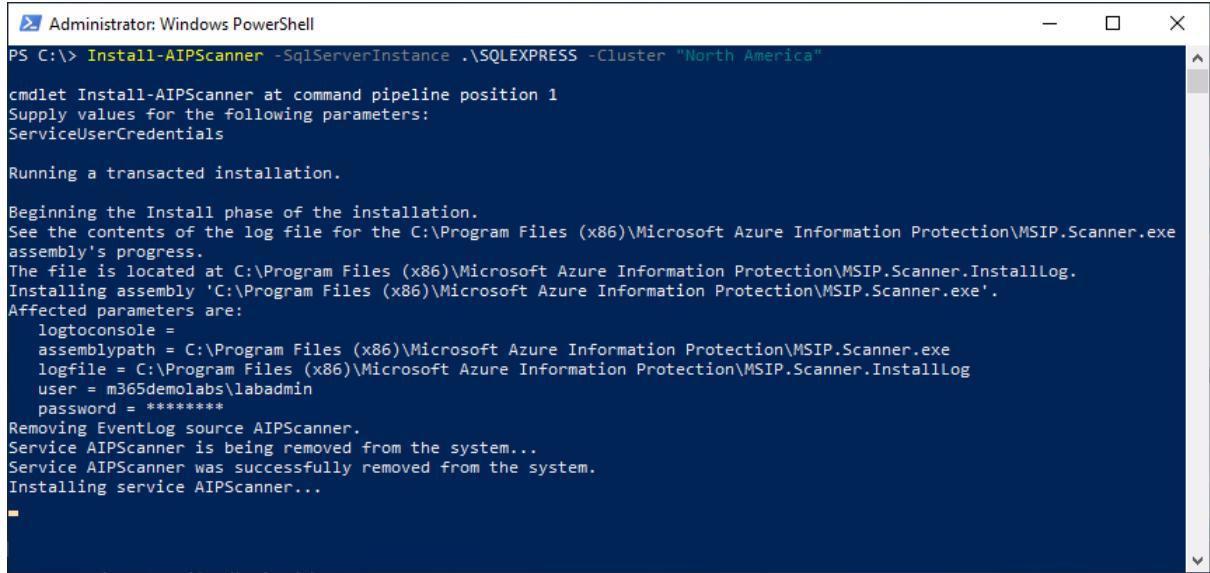


Figure 11.20 – Installing the AIP scanner

The screenshot shows the Microsoft Purview interface with the 'Settings' tab selected. On the left, a sidebar lists various compliance solutions like Catalog, Audit, and Device onboarding. The main content area is titled 'Settings' and contains a table with four items:

Name	Description
Device onboarding	View and onboard devices that can be included in your compliance solutions.
Co-authoring for files with sensitivity labels	Allow users in your organization to co-author in Office desktop documents that are encrypted by using sensitivity labels.
Compliance Manager	Set up automated testing of actions, and manage the privacy of your users' data.
Information protection scanner	View and onboard repositories to be scanned by the information protection scanner

Figure 11.21 – Device onboarding

The screenshot shows the 'Device onboarding' page under 'Settings'. The sidebar includes 'Device onboarding' in the 'Catalog' section. The main content area has tabs for 'Devices', 'Onboarding', and 'Offboarding'. A message states 'No devices onboarded yet' with a link to 'Turn on device onboarding'.

Figure 11.22 – Turning on device onboarding

The screenshot shows the 'Device onboarding' page with the 'Devices' tab selected. It displays a table of onboarded devices with columns for Device name, Configuration status, Policy sync status, and Last sync. Two devices are listed: 'win11-01' and 'labadmin_iphone 7'.

Device name	Configuration status	Policy sync status	Last sync
win11-01	Updated	Updated	Aug 1
labadmin_iphone 7	Not available	Not available	Jul 6

Figure 11.23 – List of onboarded devices

The screenshot shows the Microsoft Purview Device onboarding interface. On the left, a navigation menu includes 'Trials', 'Solutions' (Catalog, Audit, Content search, Communication compliance, Data loss prevention, eDiscovery, Data lifecycle management, Information protection, Information barriers, Insider risk management, Records management, Privacy risk management, Subject rights requests), and 'Settings'. The main area is titled 'Device onboarding' and shows a 'Devices' tab with sections for 'Onboarding' and 'Offboarding'. A table lists a single device: 'win11-01' (Device name) and 'labadmin_iPhone 7' (Device type). To the right, a detailed view for 'win11-01' shows configuration status (Real time protection/RTP Enabled, Behavior monitoring/BM Enabled), DLP policy sync details (Policy updates can take up to 2 hours), and device details (Last seen: Aug 1, 2023 2:03 PM, OS: Windows11, OS version: 21H2, Last policy sync time: Aug 1, 2023 1:42 PM).

Figure 11.24 – Viewing synchronized DLP policies

The screenshot shows an Outlook inbox. The 'Focused' folder contains 56 messages. One message from 'Microsoft AD Identity Protection' is highlighted, with a subject line 'Azure AD Identity Protec... 10:26 AM'. The message body contains a policy tip: 'Policy tip: Ooops, you may be sending something you shouldn't Show details'. Another message from 'Office365Alerts@microsoft.com' is also visible, with a subject line 'Medium-severity alert... Mon 8:05 PM'.

Figure 11.25 – Policy tip test

The screenshot shows the Microsoft Purview Alerts interface. The left sidebar includes 'Audit', 'Content search', 'Communication compliance', 'Data loss prevention' (Overview, Policies, Alerts selected), 'eDiscovery', 'Data lifecycle management', 'Information protection', 'Information barriers', 'Insider risk management', 'Records management', 'Privacy risk management', 'Subject rights requests', 'Settings', and 'More resources'. The main area is titled 'Alerts' and shows a list of alerts. One alert is selected: 'DLP policy match for email with subject 'Fw: Policy Tip Test''. The alert details pane on the right shows: Alert ID: ca8a2f06-35b3-1812-5a00-08db9308551c, Alert status: Active, Alert severity: High, Time detected: Aug 1, 2023 11:29 PM, Number of events: 1, DLP policy matched: Privacy Policy, Locations: Exchange, Users who performed the event: labadmin (labadmin@m365demolabs.com), and Assigned to: No one is assigned.

Figure 11.26 – Viewing a DLP alert

The screenshot shows the Microsoft Purview interface for managing alerts. On the left, a navigation sidebar includes Home, Compliance Manager, Data classification, Data connectors, Alerts, Policies, Roles & scopes, Trials, Solutions, Catalog, Audit, Content search, Communication compliance, Data loss prevention, eDiscovery, Data lifecycle management, Information protection, Information barriers, and Insider risk management. The main content area displays an alert titled 'DLP policy match for email with subject 'Fw: Policy Tip Test''. It shows a summary: 'labadmin sent an email with subject "Fw: Policy Tip Test" with sensitive content.' Below this, it details the event on Aug 1, 2023, at 11:26 PM, where labadmin sent an email which violated the DLP policy 'Privacy Policy'. The event table includes columns for Name, User, and Location. To the right, a 'Manage alert' panel allows for assignment and logging, with tabs for Assign and Management log. The status is set to Active, and the assignee is Start typing to find users. A comments section is also present.

Figure 11.27 – Alert detail page

This screenshot shows the Microsoft Purview interface for viewing event details. The left sidebar is identical to Figure 11.27. The main content area shows the same alert summary: 'DLP policy match for email with subject 'Fw: Policy Tip Test''. Below the summary, an event table lists one selected item: 'Sensitive info in email with subj...'. The right side provides detailed information about the event, including the source (Privacy Policy), detected sensitive info types (U.S. Social Security Number (SSN)), actions taken (User overrode policy), and other conditions matched (Content is shared from Microsoft 365). An 'Actions' button is located at the bottom of the details pane.

Figure 11.28 – Event detail view of an alert

The screenshot shows the Microsoft Purview interface for handling a DLP policy match. The main title is "DLP policy match for email with subject 'Fw: Policy Tip Test'". A sidebar on the left includes icons for Home, Compliance Manager, Data classification, Activity explorer (selected), Data connectors, Alerts, Policies, Roles & scopes, Trials, Catalog, Audit, Content search, Communication compliance, and Data loss prevention. The main content area has tabs for "Overview" and "Events", with "Events" selected. It displays a single event: "Sensitive info in email with subj...". The event details show the source as "labadmin" and the location as "Exchange". The event timestamp is "Aug 1, 2023 11:26 PM". The right side of the screen is a "Help Microsoft improve the accuracy of its built-in classifiers" panel. It contains a redacted preview of the email with the subject "Policy Tip Test" and a message body containing "This is a policy tip test for SSN" followed by several redacted SSNs. Below this is a checkbox for "I agree to provide a copy of this file to Microsoft" and a "Submit to Microsoft" button.

Figure 11.29 – Submitting a redacted false positive sample to Microsoft

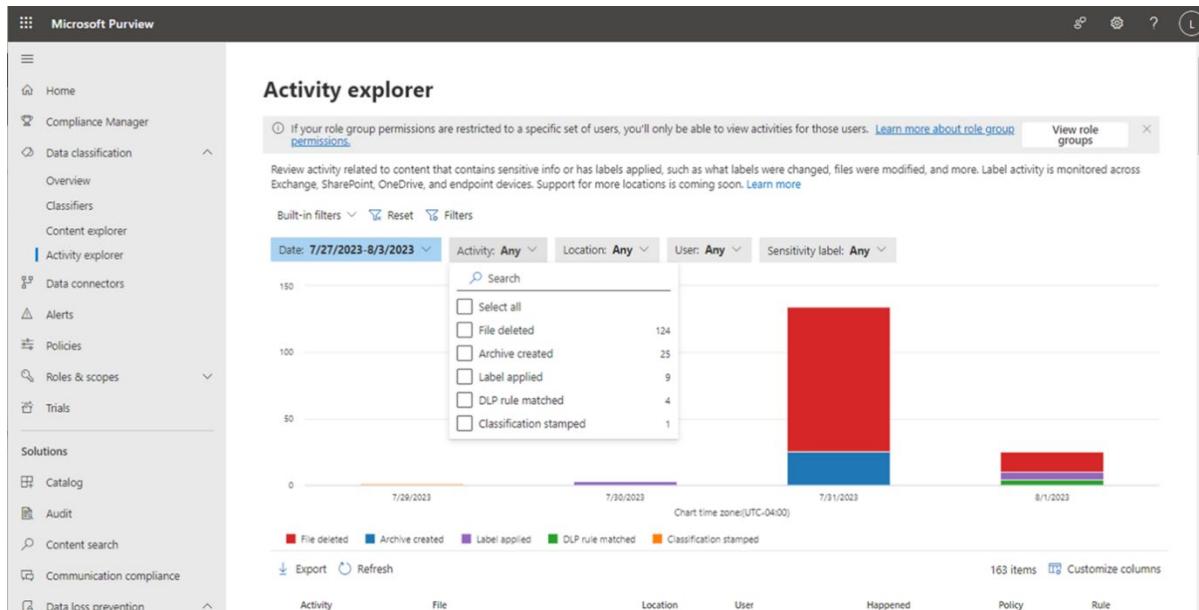


Figure 11.30 – Activity explorer dashboard

The screenshot shows the Microsoft Purview Activity explorer interface. On the left, there's a navigation sidebar with various options like Home, Compliance Manager, Data classification, Content explorer, Activity explorer (which is selected), Data connectors, Alerts, Policies, Roles & scopes, Trials, Solutions, Catalog, Audit, Content search, Communication compliance, and Data loss prevention (with Overview and Policies sub-options). The main area has a title bar with 'DLP rule matched' and a date range from '7/27/2023-8/3/2023'. Below this are filter buttons for 'Activity: Any', 'Location: Any', and 'User: Any'. A timeline chart shows activity counts from 0 to 100 over time, with a specific event highlighted on Aug 1, 2023, at 11:26 PM. A legend indicates event types: File deleted (red), Archive created (blue), Label applied (purple), DLP rule matched (green), and Classification stamp (orange). Below the chart is a table of events:

Activity	File	Location	User
<input type="checkbox"/> Label applied	Fw: Policy Tip Test	Exchange	labadmin
<input checked="" type="checkbox"/> DLP rule matched	Message Body	Exchange	labadmin
<input type="checkbox"/> Label applied	Re: Policy Tip Test	Exchange	labadmin
<input type="checkbox"/> DLP rule matched	Message Body	Exchange	labadmin
<input type="checkbox"/> DLP rule matched	Message Body	Exchange	labadmin
<input type="checkbox"/> Label applied	Re: Policy Tip Test	Exchange	labadmin
<input type="checkbox"/> Label applied	Policy Tip Test	Exchange	labadmin

To the right, there's a detailed view of the selected 'DLP rule matched' event. It includes sections for 'Activity details' (Activity: DLP rule matched, Happened on Aug 1, 2023 at 11:26 PM), 'About this item' (File: Message Body, User: labadmin@m365demolabs.com, File size: 15 KB, Sensitive info type: U.S. Social Security Number (SSN), Policy: Privacy Policy, Rule: High volume of content detected U.S. PII, Policy mode: Enable, Rule actions: GenerateAlert, GenerateIncidentReport), 'Email subject' (Fw: Policy Tip Test), 'Email recipient' (labadmin@m365demolabs.com), 'Other conditions matched' (Condition: Content is shared from Microsoft 365, Matched value: InternalUsersOnly), and 'Location details'.

Figure 11.31 – Viewing details of an event in Activity explorer

The screenshot shows the Microsoft 365 Defender Alerts dashboard. The left sidebar includes Home, Incidents & alerts (selected), Alerts, Hunting, Actions & submissions, Threat intelligence, Secure score, Learning hub, Trials, and Partner catalog. The main area has a title bar with 'Search' and a button to 'Customize columns'. Below is a table of alerts:

Alert name	Tags	Severity	Investigation state	Status	Category	Detection source	Impacted assets
DLP policy (Privacy...)	■■■ High	High	Resolved	●	Exfiltration	Microsoft Data Loss Pr...	labadmin
DLP policy (Privacy...)	■■■ High	High	Resolved	●	Exfiltration	Microsoft Data Loss Pr...	labadmin
Suspicious Process...	■■■■ Low	Low	Resolved	●	Discovery	EDR	win11-01
Attempt to stop M...	■■■■ Medium	Medium	Resolved	●	Defense evasion	EDR	win11-01
Compliance Mana...	■■■■ Medium	Medium	Queued	●	ComplianceManager	MDO	
Compliance Mana...	■■■■ Medium	Medium	Queued	●	ComplianceManager	MDO	
eDiscovery search ...	■■■■ Informational	Informational	Queued	●	Threat management	MDO	labadmin

Figure 11.32 – Microsoft 365 Defender Alerts dashboard

The screenshot shows the Microsoft 365 Defender interface with the 'Alerts' section selected in the sidebar. A detailed view of a single alert is displayed on the right. The alert is titled 'DLP policy (Privacy Policy) matched for email with subject (Fw: Policy Tip Test)'. It is categorized as 'High' severity. The alert details pane shows the classification as 'Automation' and the assigned to field as 'Automation'. The evidence section indicates the entity name is undefined and the verdict is 'Suspicious'. The alert policy ID is listed as 39e45806-6358-4e4e-8c23-6836119b05fe.

Figure 11.33 – Alert detail flyout

The screenshot shows the Microsoft 365 Defender interface with the 'Incidents & alerts' section selected in the sidebar. The main area displays a list of 'Most recent incidents and alerts'. The table includes columns for Incident name, Incident Id, Tags, Severity, Investigation state, and Categories. Several incidents are listed, including 'Exfiltration incident involving one user' (High severity, Exfiltration category), multiple entries for 'DLP policy (Privacy Policy) matched for email...' (High severity, Exfiltration category), and 'Multi-stage incident involving Defense evasion ...' (Medium severity, Defense evasion, Disc... category).

Figure 11.34 – Microsoft 365 Defender Incidents dashboard

Figure 11.35 – Viewing the user actions in a DLP incident

Figure 11.36 – Microsoft 365 Defender incident evidence

Figure 11.37 – Advanced hunting results

The screenshot shows the Microsoft 365 Defender interface. On the left, the navigation menu includes Home, Incidents & alerts, Hunting (selected), Advanced hunting, Custom detection rules, Actions & submissions, Threat intelligence, Secure score, Learning hub, Trials, Partner catalog, Assets, and Devices. The main area is titled "Advanced hunting" and contains a "Schema" section with "Search" and "Query" tabs. The "Query" tab shows a search result for "EmailEvents" with one item. To the right, a detailed view for an email event titled "Re: Policy Tip Test" is shown, with sections for "Delivery details" (Threats: None, Delivery action: Blocked; Original location: Dropped, Latest delivery location: Dropped; Detection technologies: Primary Override: Source) and "Email details" (Sender display name: labadmin, Sender address: labadmin@m365demolabs.com; SMTP mail from address: labadmin@m365demolabs.com, Sent on behalf of: -).

Figure 11.38: Advanced hunting item details

The screenshot shows the "Take actions" dialog box. The left sidebar lists the same navigation items as Figure 11.38. The main area has a "Choose actions" section with three options: "Choose target entities" (radio button selected), "Review and submit" (radio button unselected), and "Choose response actions" (radio button unselected). The "Choose response actions" section contains several sections: "Move or delete" (checkbox for Move to another mailbox folder, radio buttons for Junk, Inbox, Deleted items, checked for Delete email, radio buttons for Soft deleted items, Hard deleted items); "Submit to Microsoft" (radio buttons for Report as clean, phishing, junk, malware); "Tenant level block" (radio buttons for Sender, Sender domain); "Initiate automated investigation" (radio buttons for Investigate, Contact); and "Next" and "Cancel" buttons at the bottom.

Figure 11.39 – Initiating remediation tasks

DASHBOARD > CHAPTER 11

Implementing Microsoft Purview Data Loss Prevention (DLP)

Summary

In this chapter, you learned about the capabilities of Microsoft DLP. Building on the knowledge you previously gained about classifiers such as sensitive information types, DLP policies can be used to detect sensitive information as it moves throughout your organization.

DLP policies can target workloads such as Exchange Online or SharePoint as well as endpoint devices such as on-premises file servers and client computers. Each layer helps provide additional protection against data leakage and compromise.

You also learned about the alerting and troubleshooting tools available in the platform, including the DLP Alerts dashboard and the Microsoft 365 Defender Incidents dashboard, and the capabilities of incident management to further remediate issues with users and data.

Chapter Review Questions

The Microsoft 365 Administrator MS-102 Exam Guide
by Aaron Guimette

Select Quiz

Quiz 1

[SHOW QUIZ DETAILS](#) ▾

START

Figure 11.40 – Chapter Review Questions for Chapter 11