Microsoft 365 Administrator MS-102 Exam Guide

Preface:

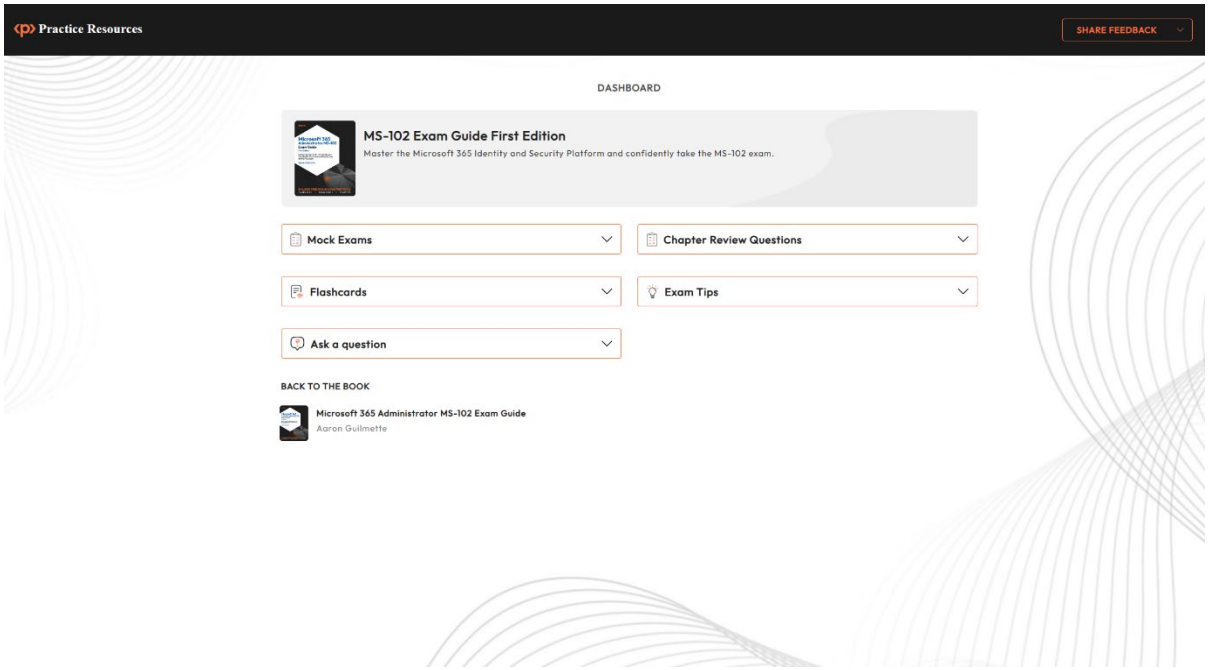

Figure 0.1 – Dashboard interface on a desktop device

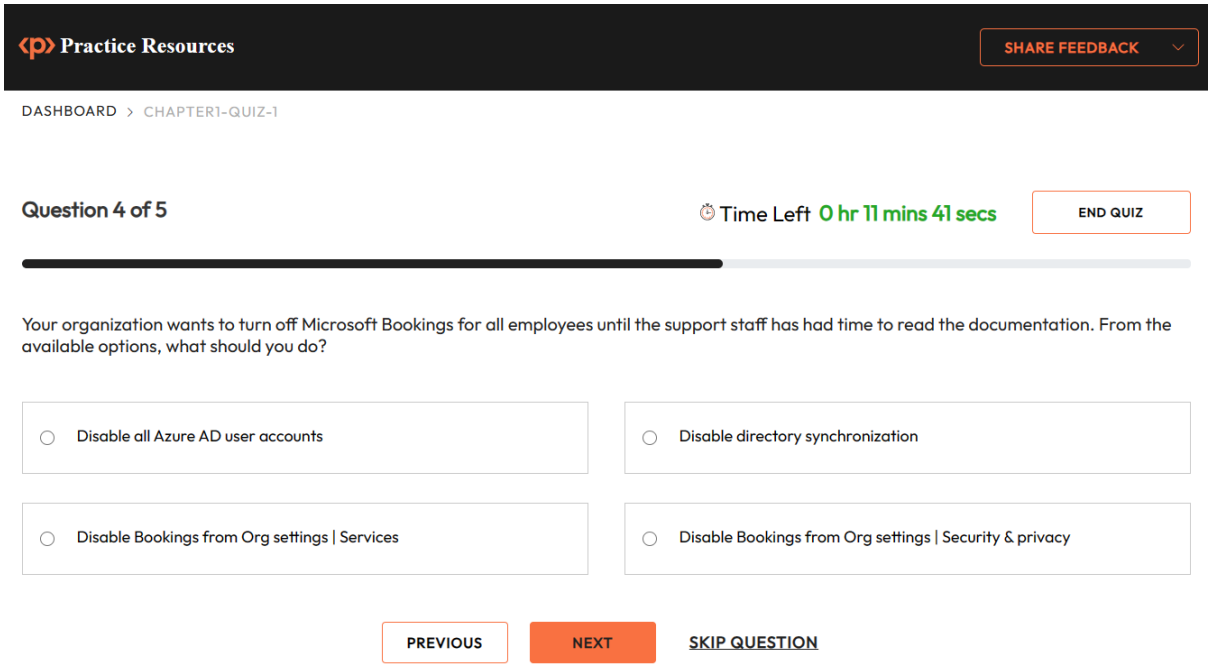

Figure 0.2 – Practice Questions Interface on a desktop device

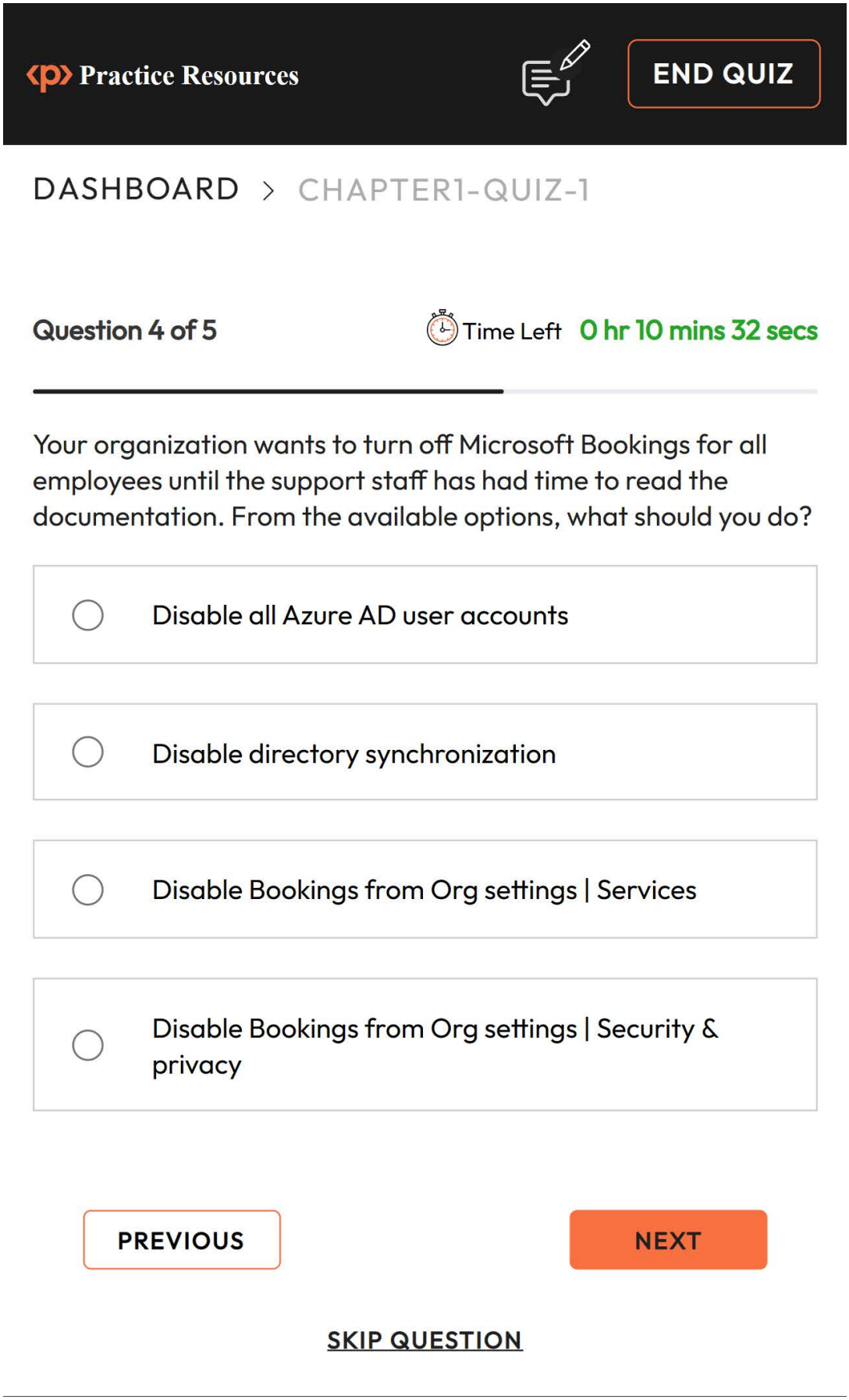

Figure 0.3 – Quiz interface on a mobile device

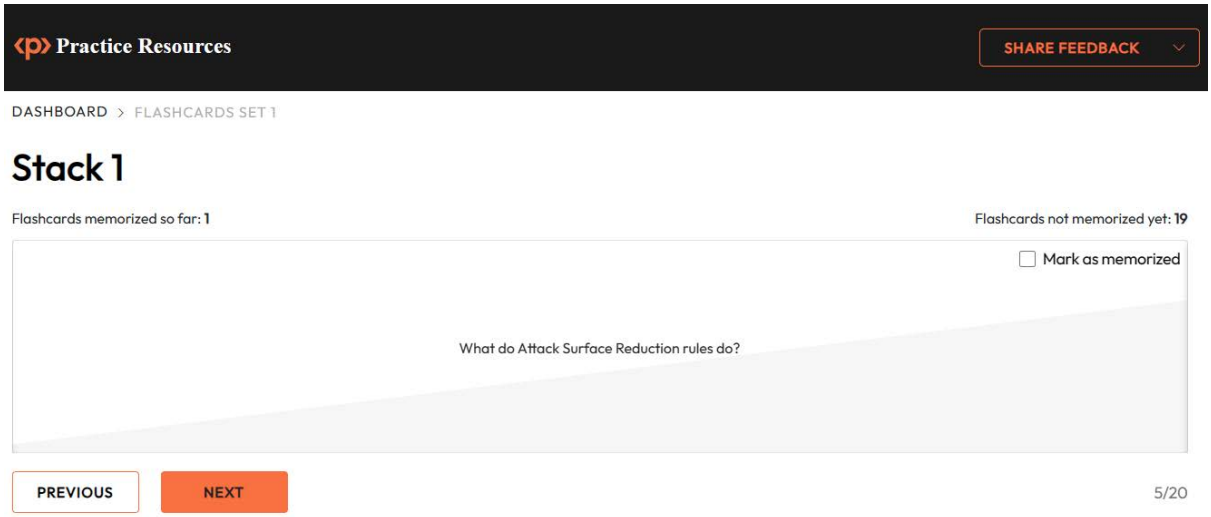

Figure 0.4 – Flashcards interface

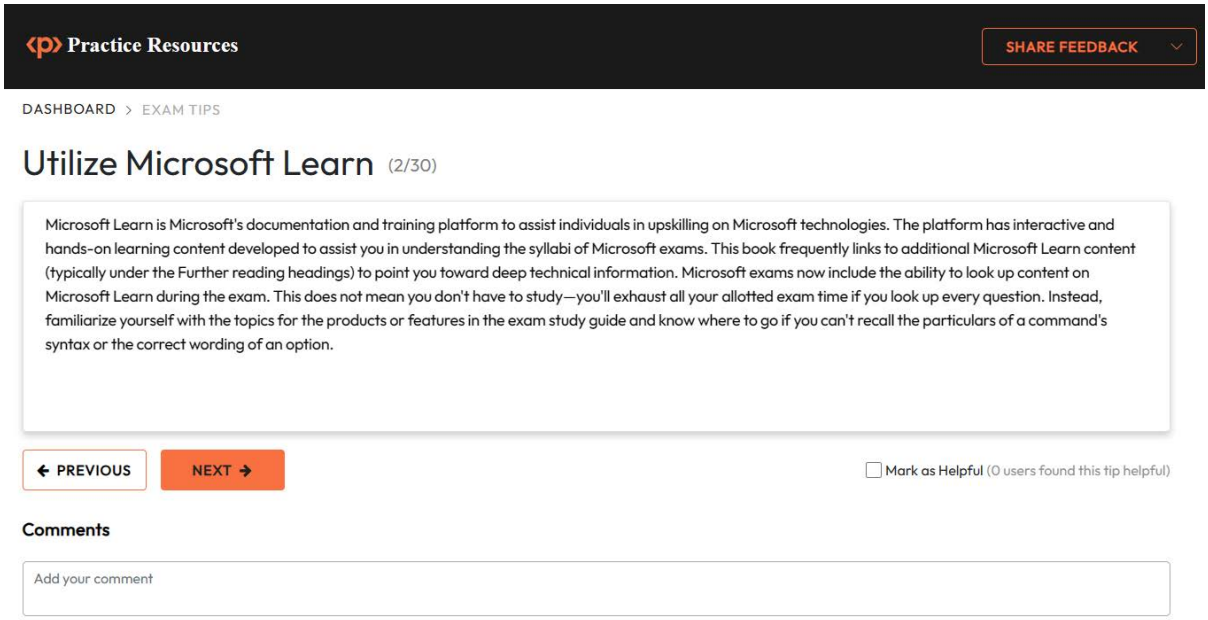

Figure 0.5 – Exam Tips Interface

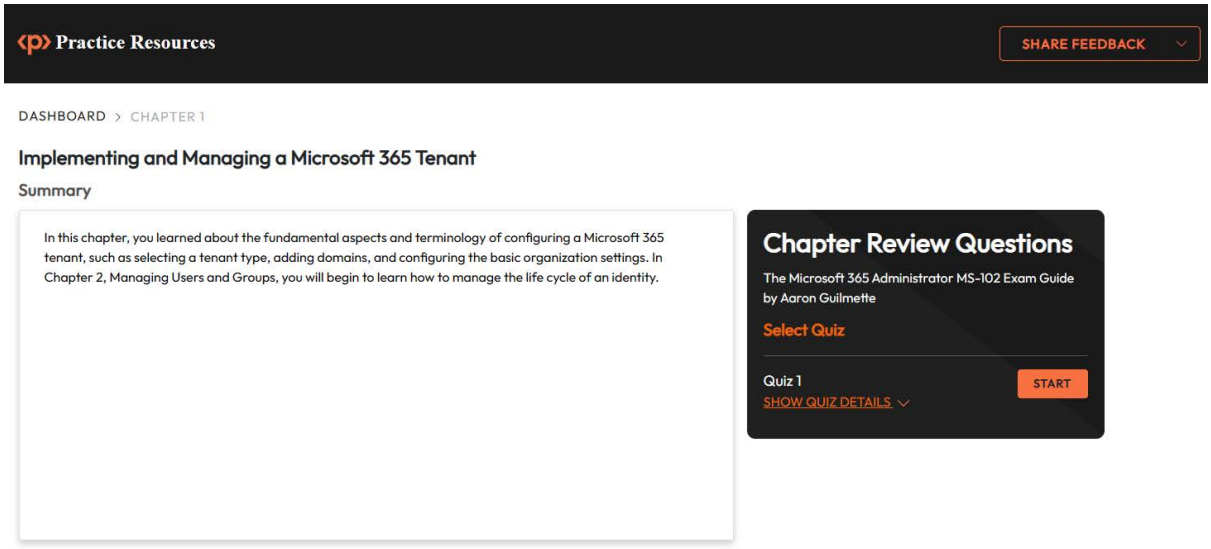

Figure 0.6 – Chapter Review Questions Page

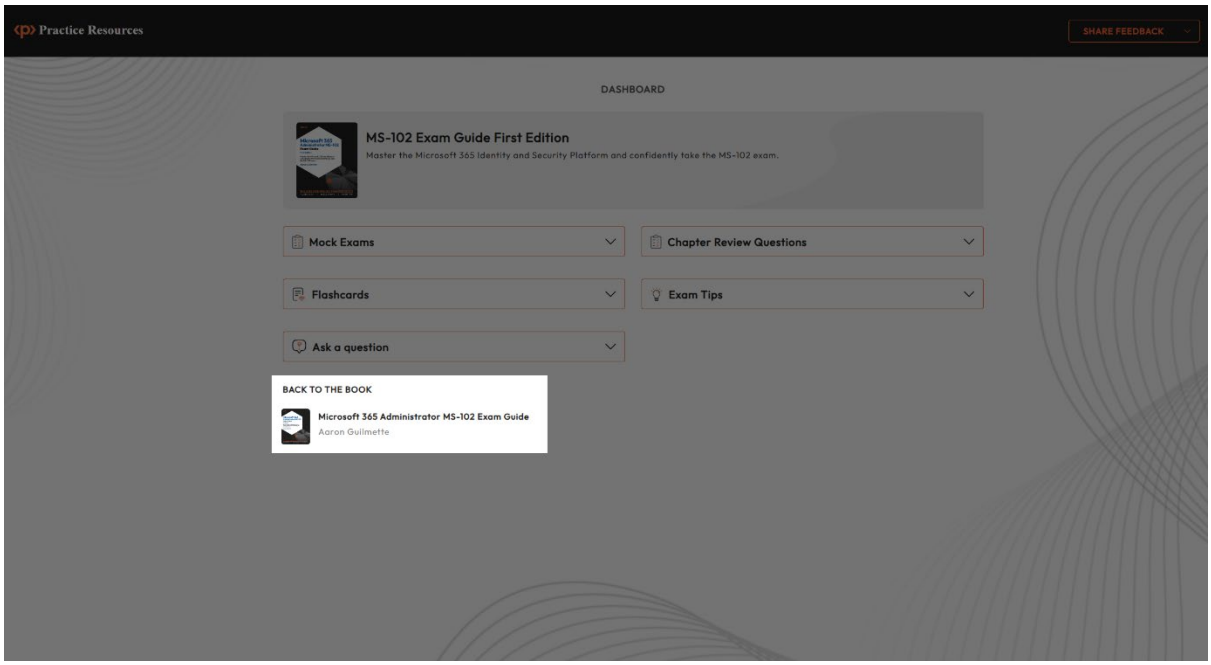

Figure 0.7 – Jump back to the book from the dashboard

Chapter 1: Implementing and Managing a Microsoft 365 Tenant

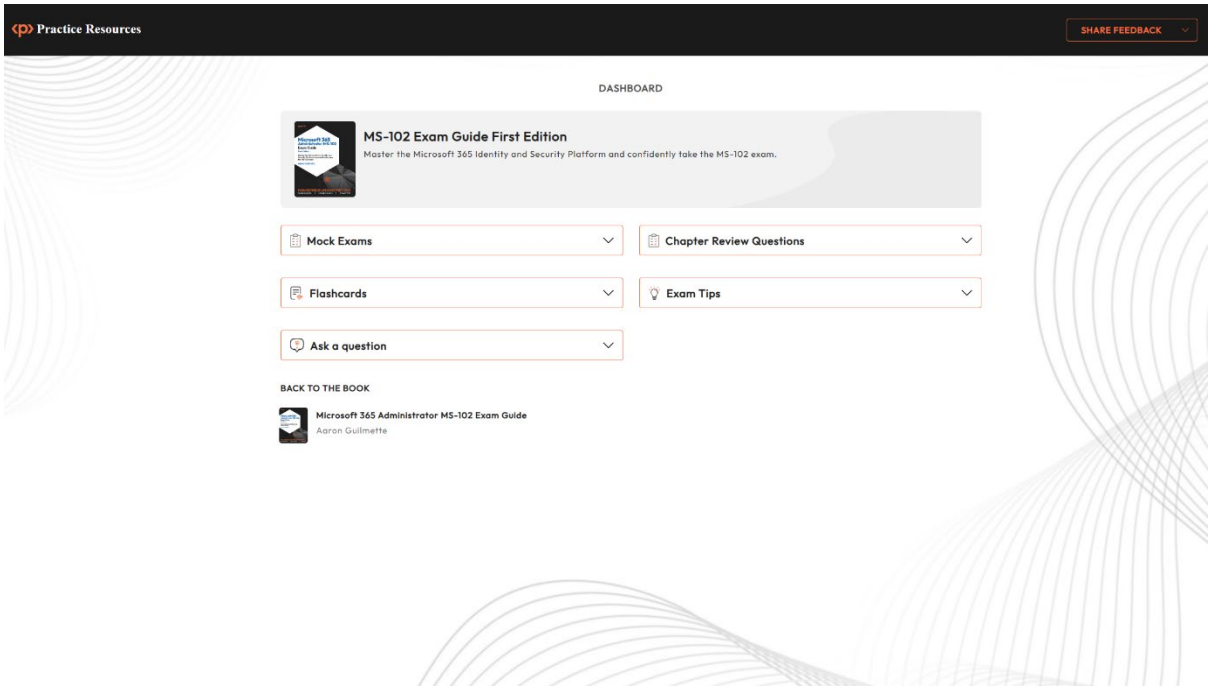

Figure 1.1 – Dashboard Interface Of MS-102 Practice Resources

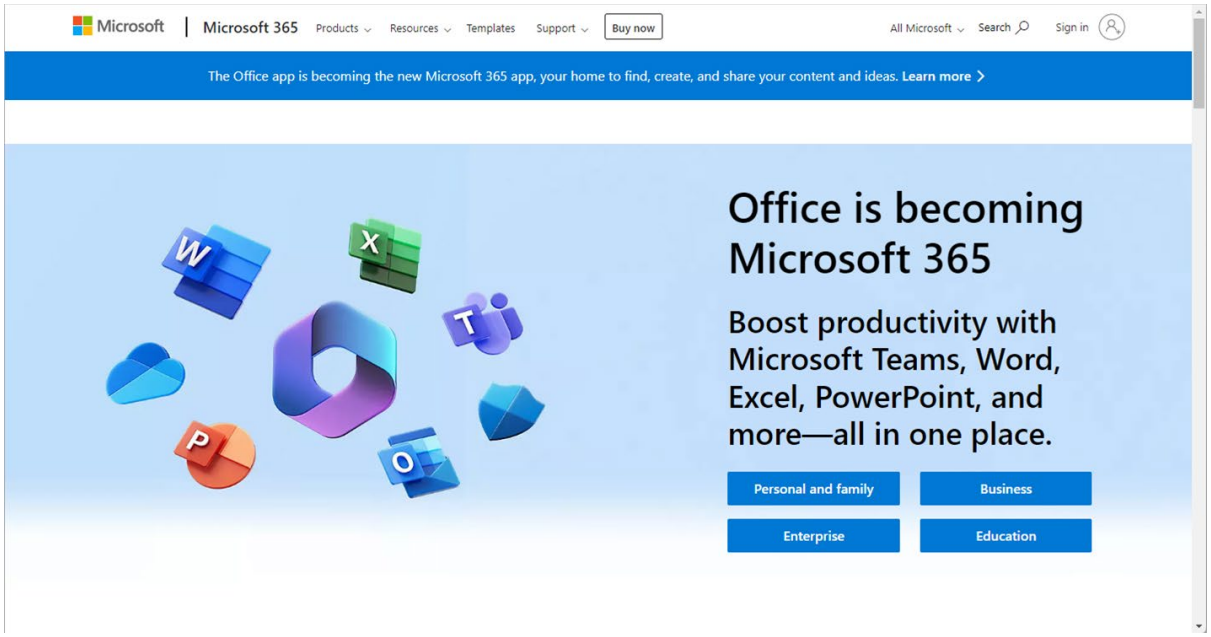

Figure 1.2 – Types of tenants

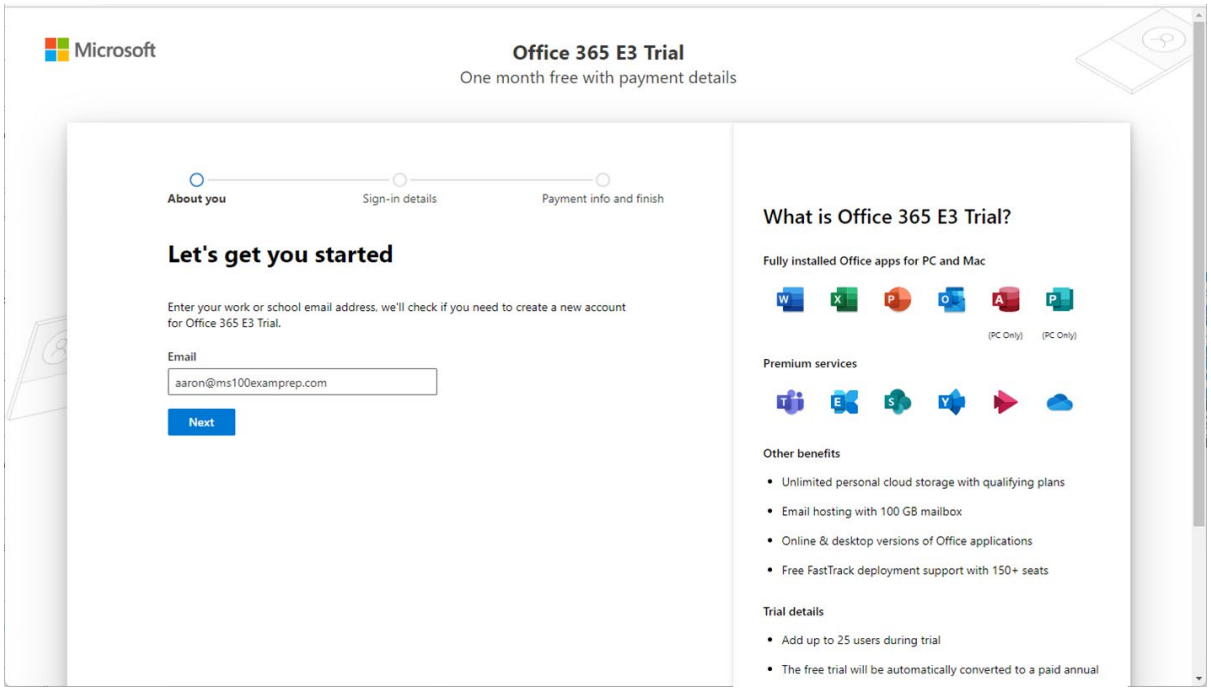

Figure 1.3 – Starting a trial subscription

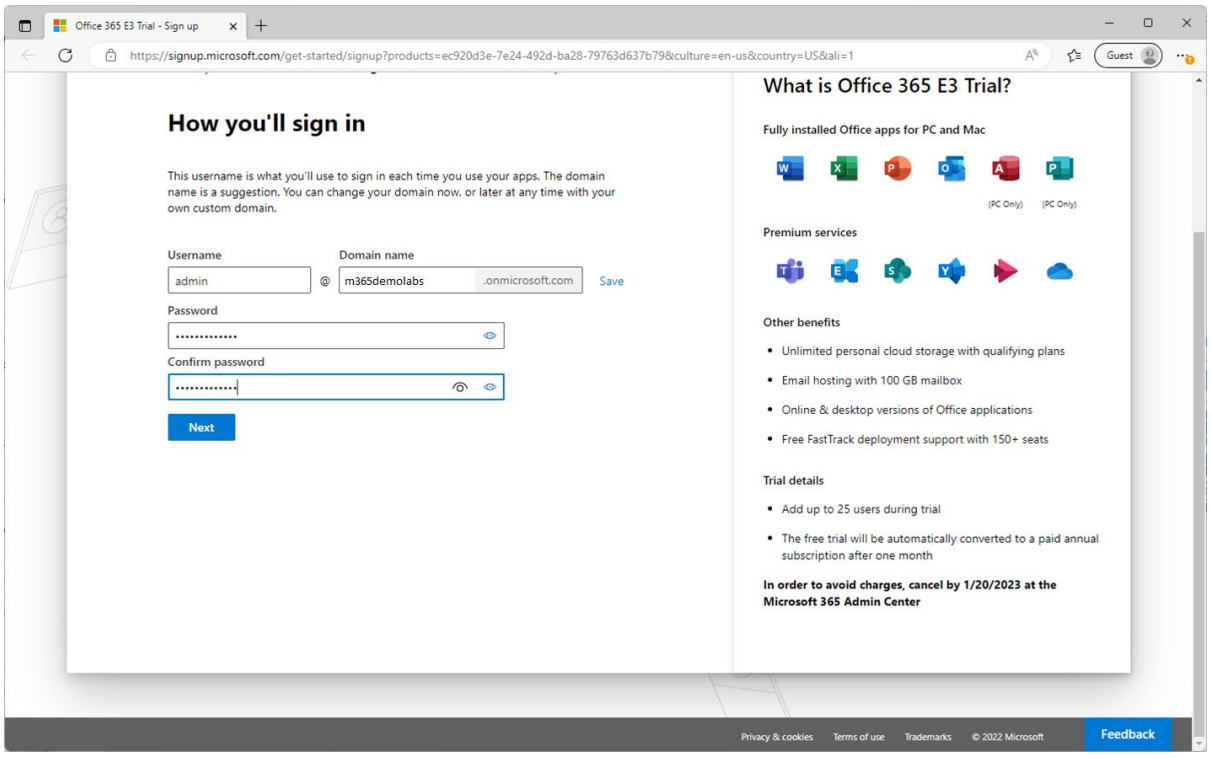

Figure 1.4 – Choosing a managed domain

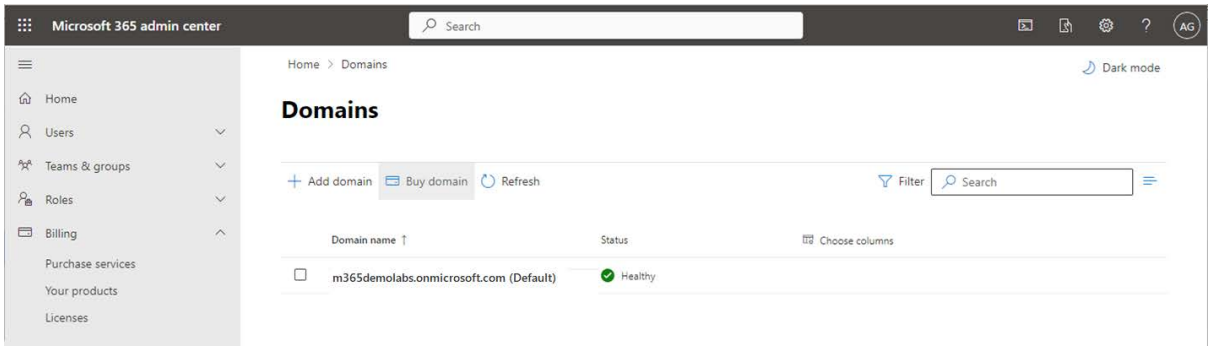

Figure 1.5 – Purchasing a domain through the Microsoft 365 admin center

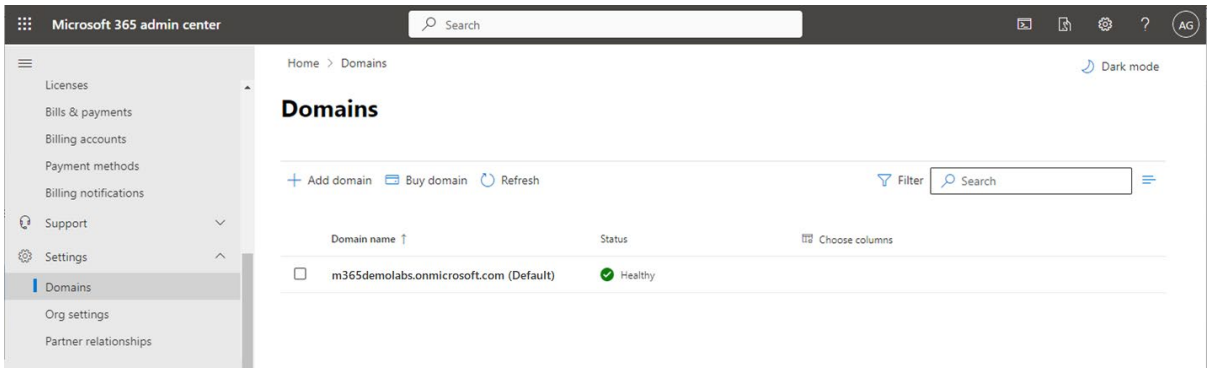

Figure 1.6 – Domains page of the Microsoft 365 admin center

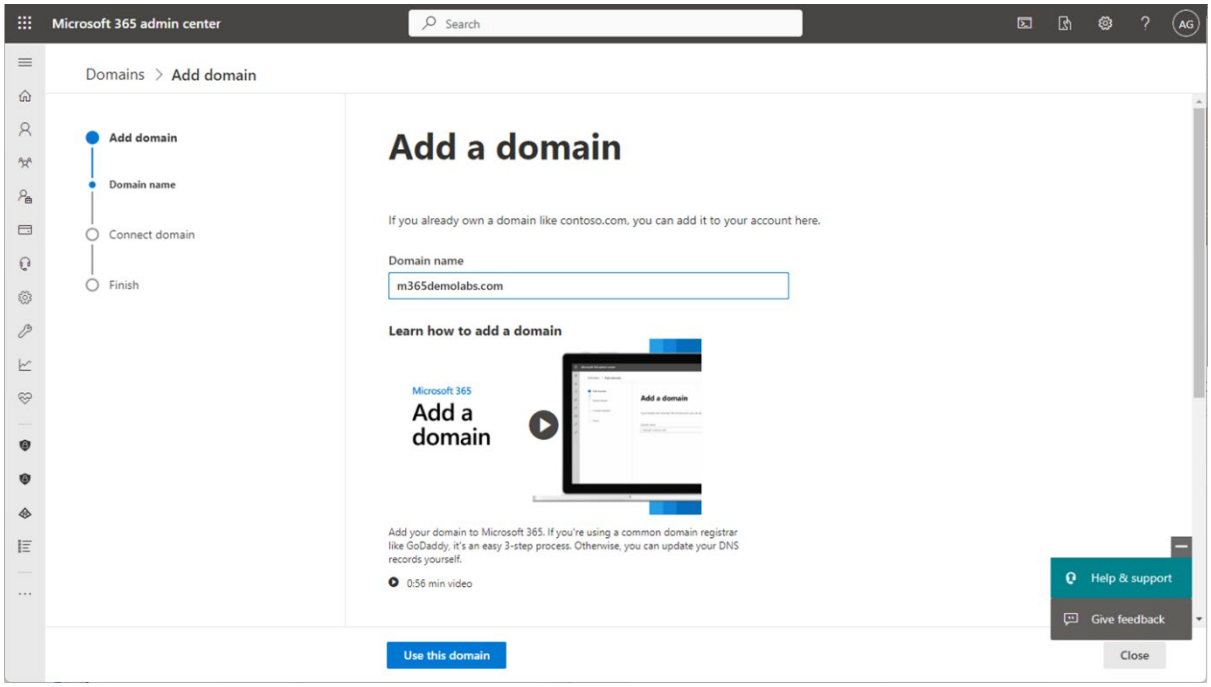

Figure 1.7 – Add domain page

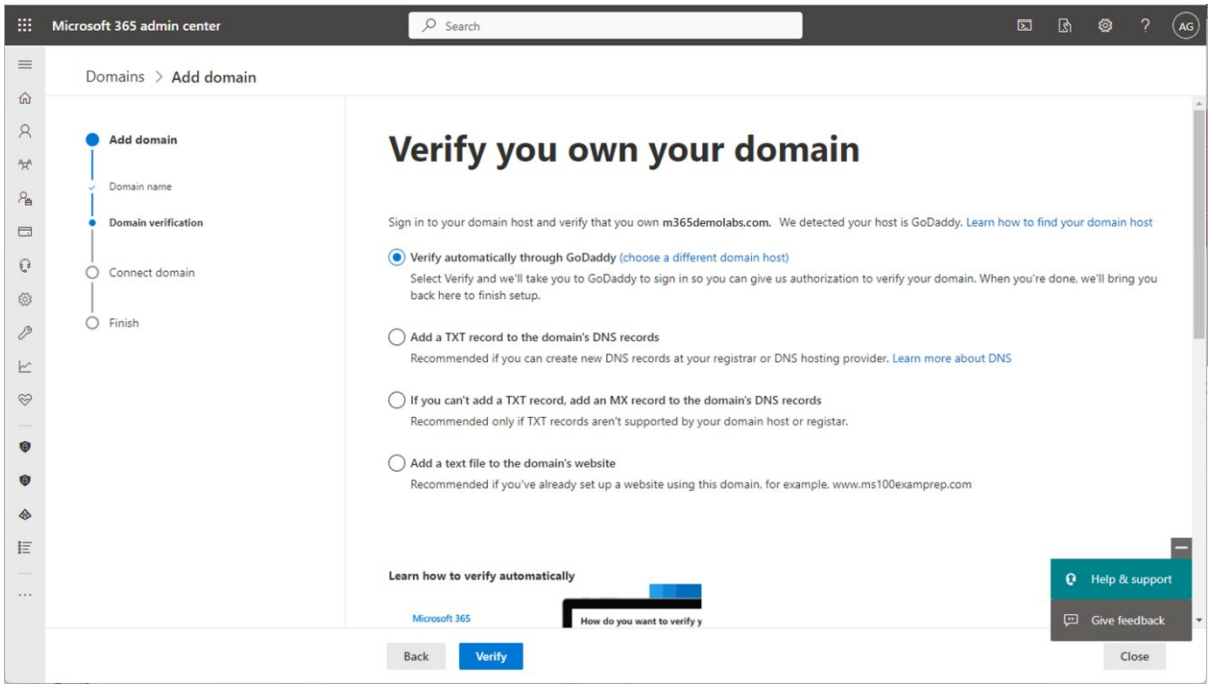

Figure 1.8 – Verify domain ownership

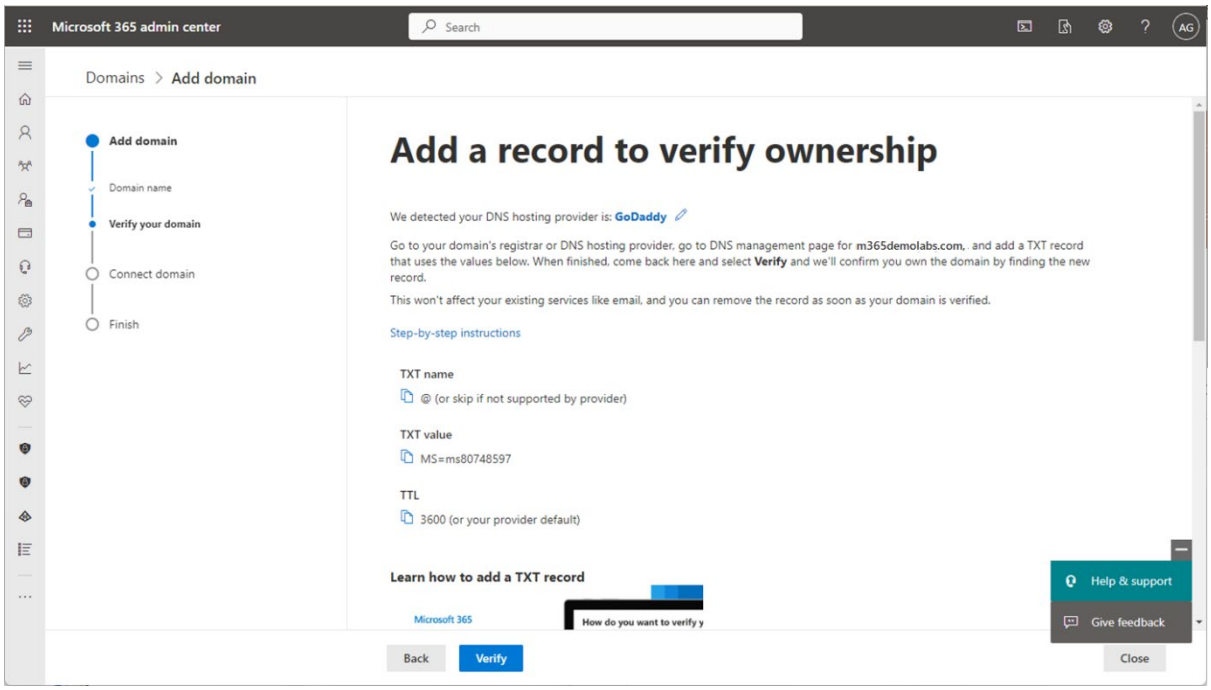

Figure 1.9 – Completing verification records manually

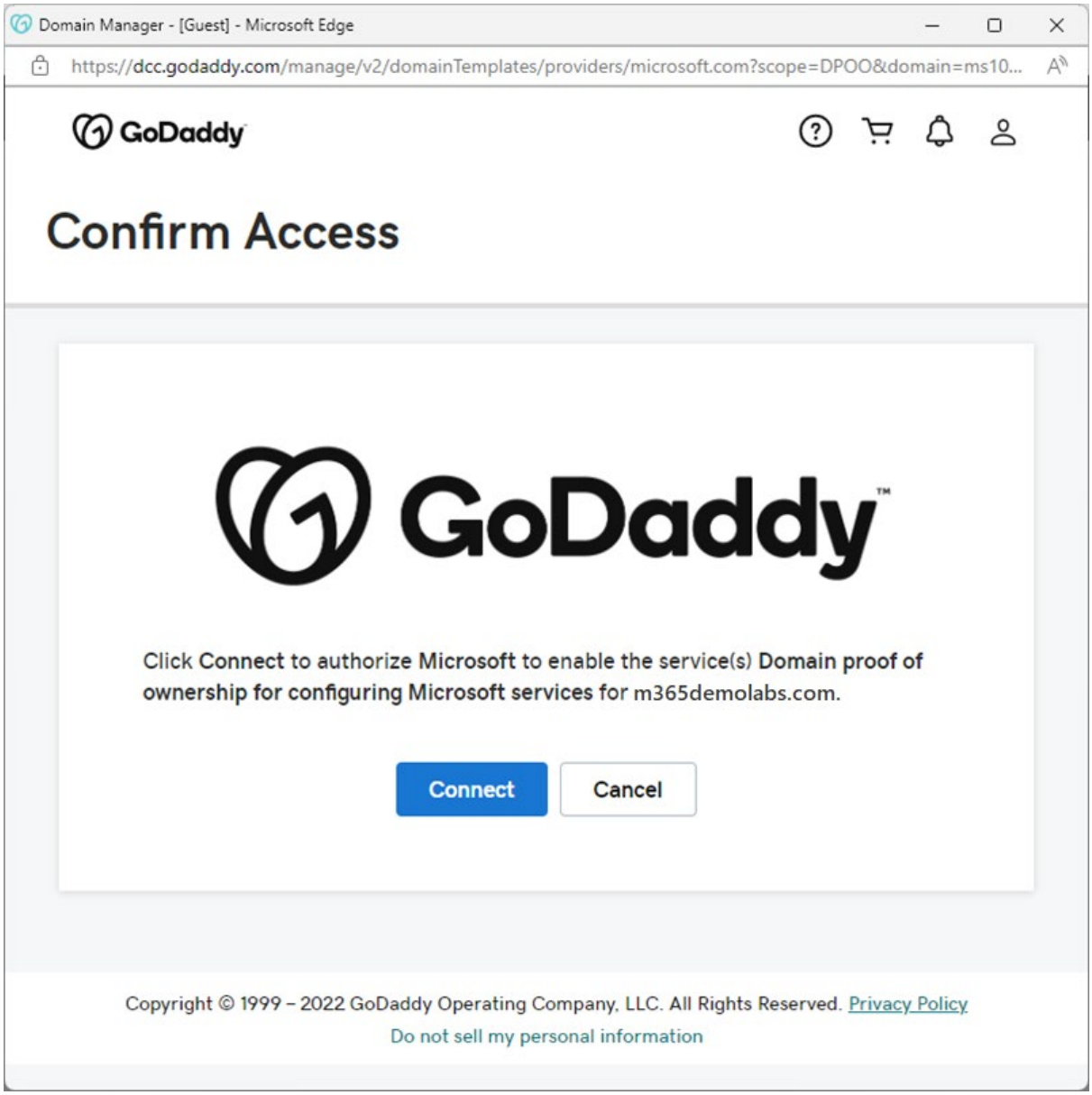

Figure 1.10 – Authorizing Domain Connect with GoDaddy to update DNS records

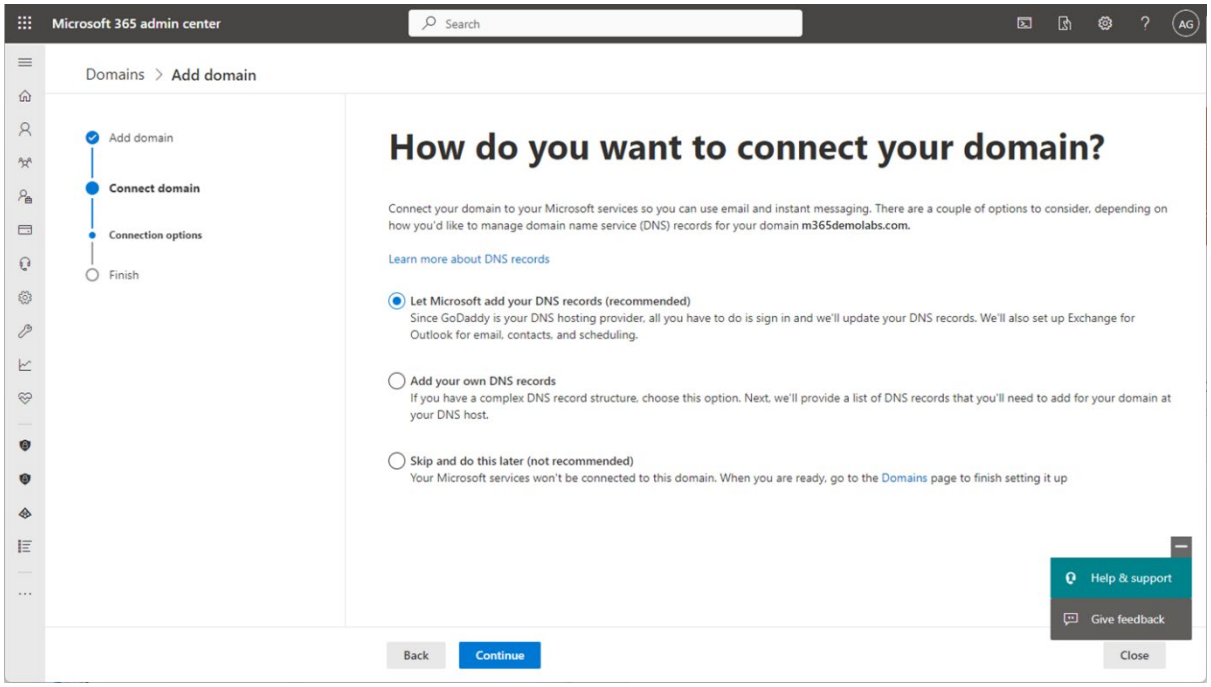

Figure 1.11 – Connecting domain to Microsoft 365

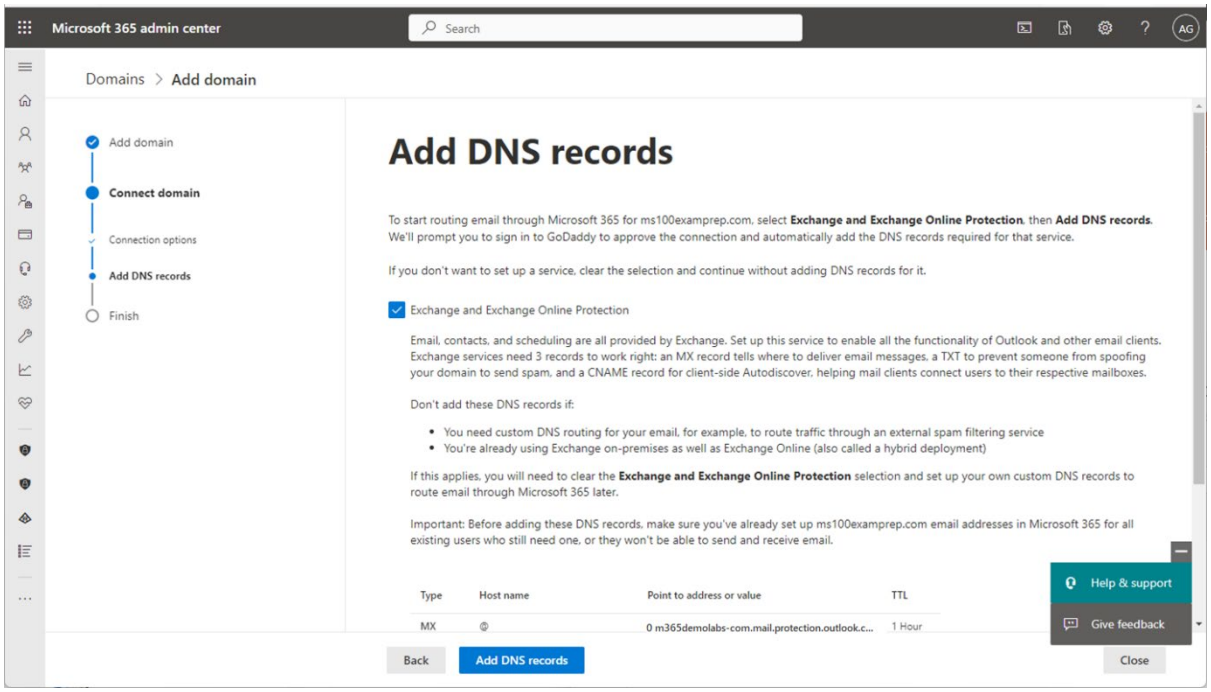

Figure 1.12 – Adding DNS records

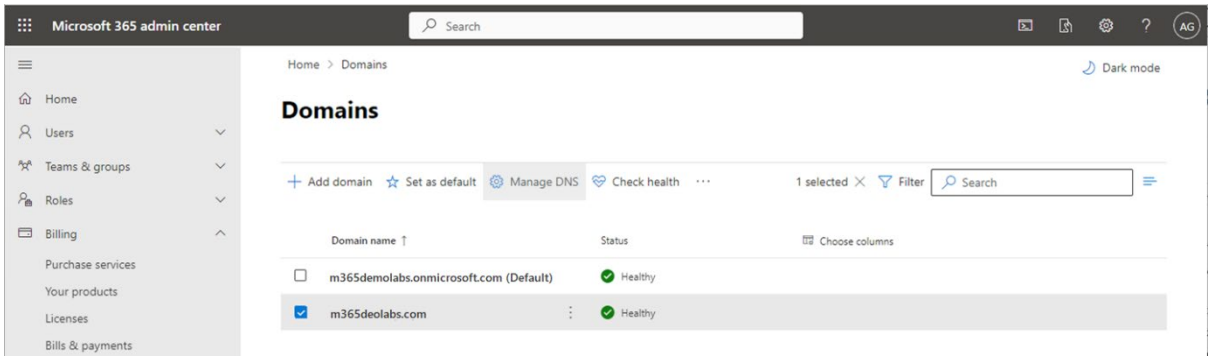

Figure 1.13 – Managing DNS settings for a domain

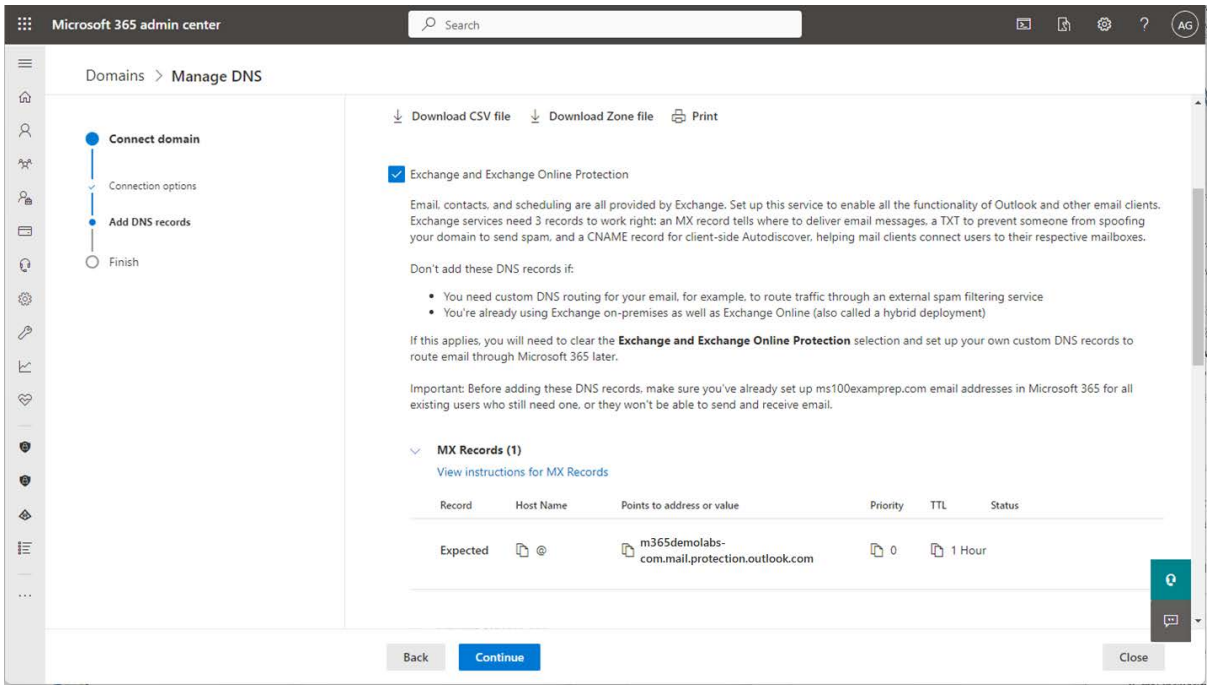

Figure 1.14 – Viewing DNS settings

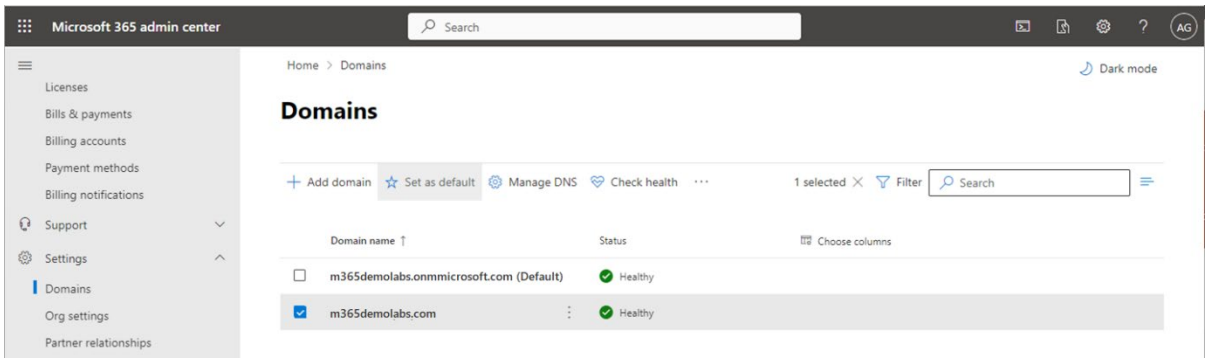

Figure 1.15 – Setting the default domain

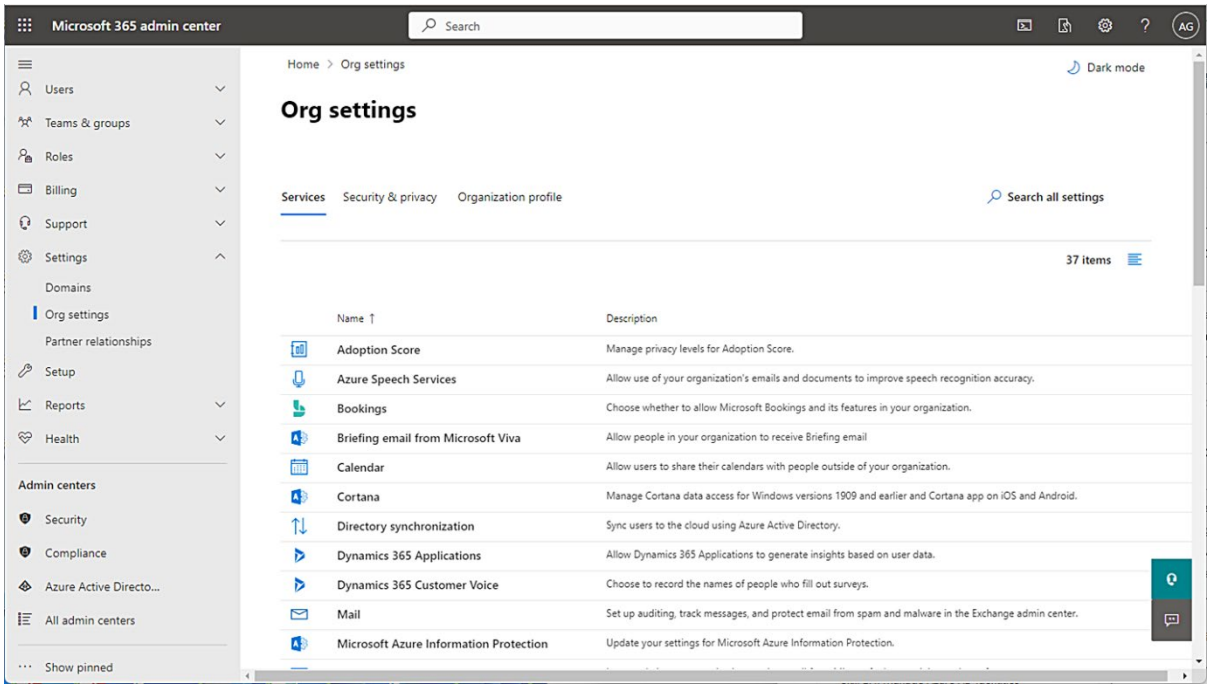

Figure 1.16 – Org settings in the Microsoft 365 admin center

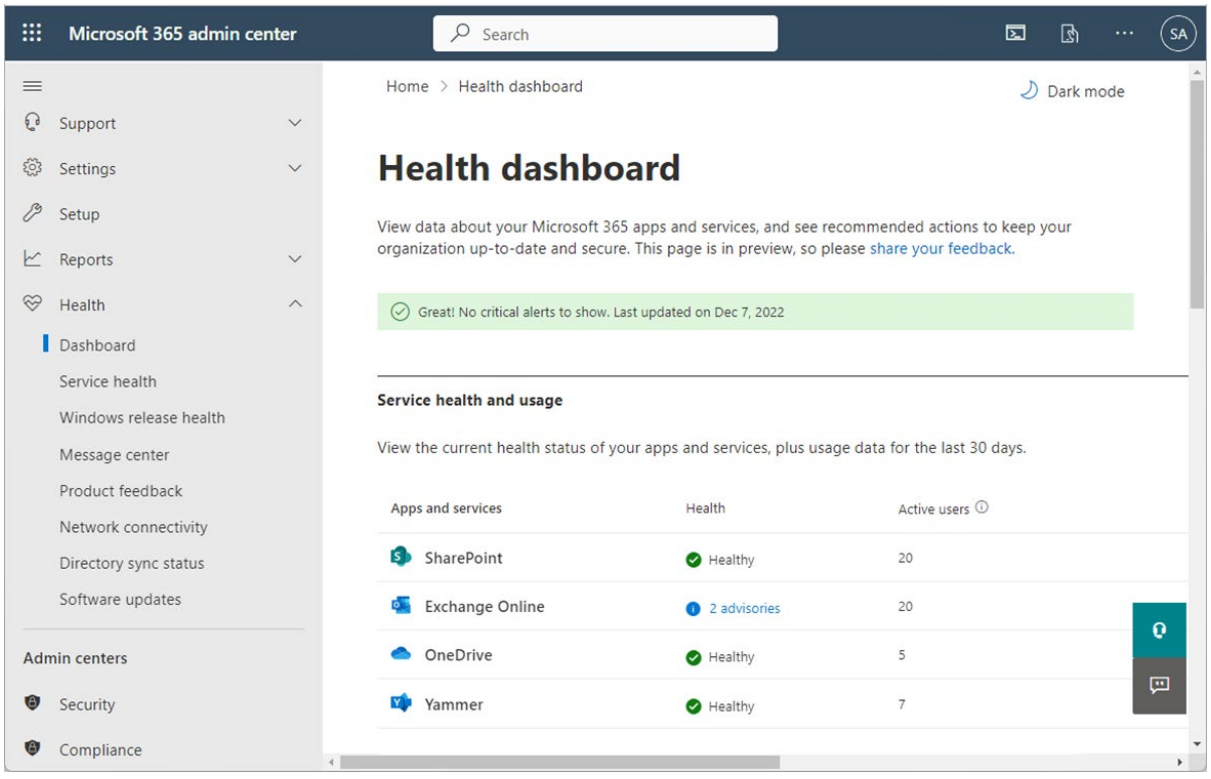

Figure 1.17 – Service health dashboard

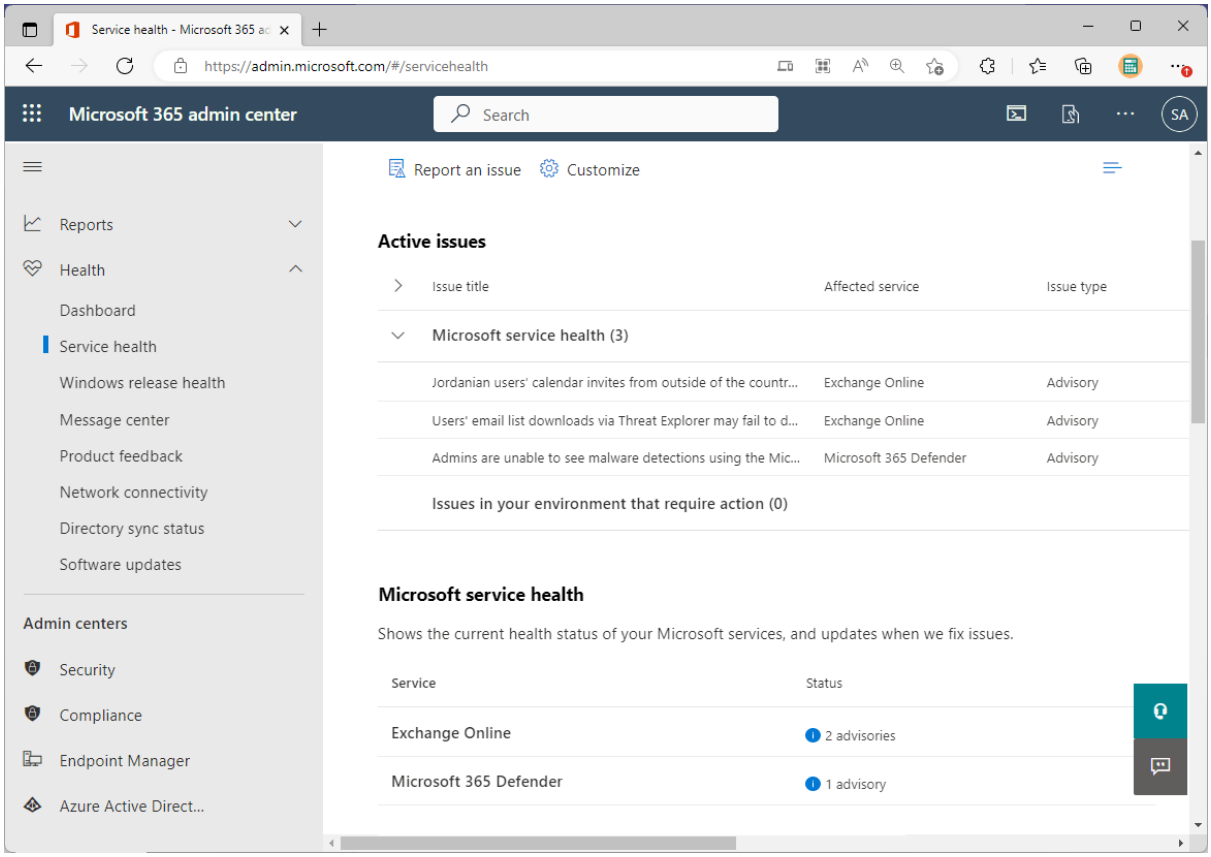

Figure 1.18 – Service health page

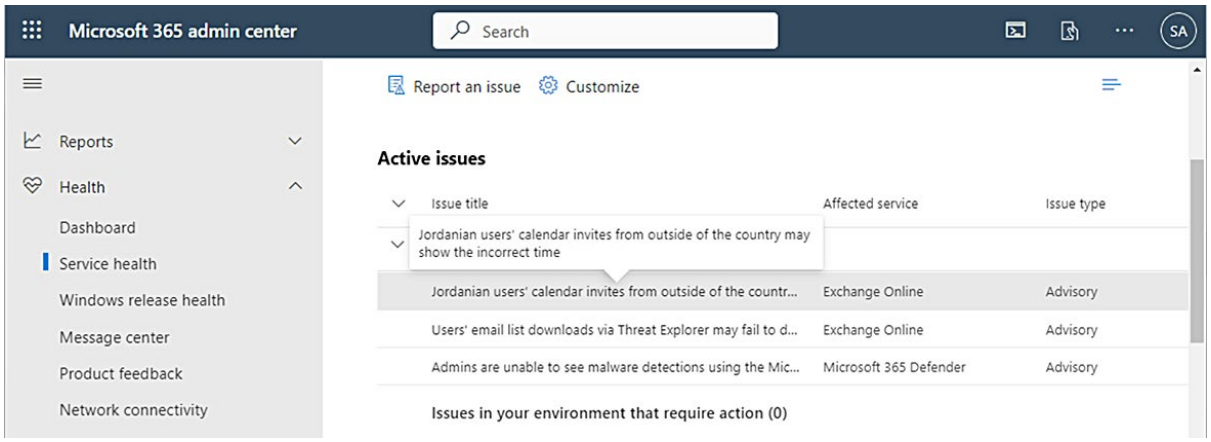

Figure 1.19 – Service health active issues

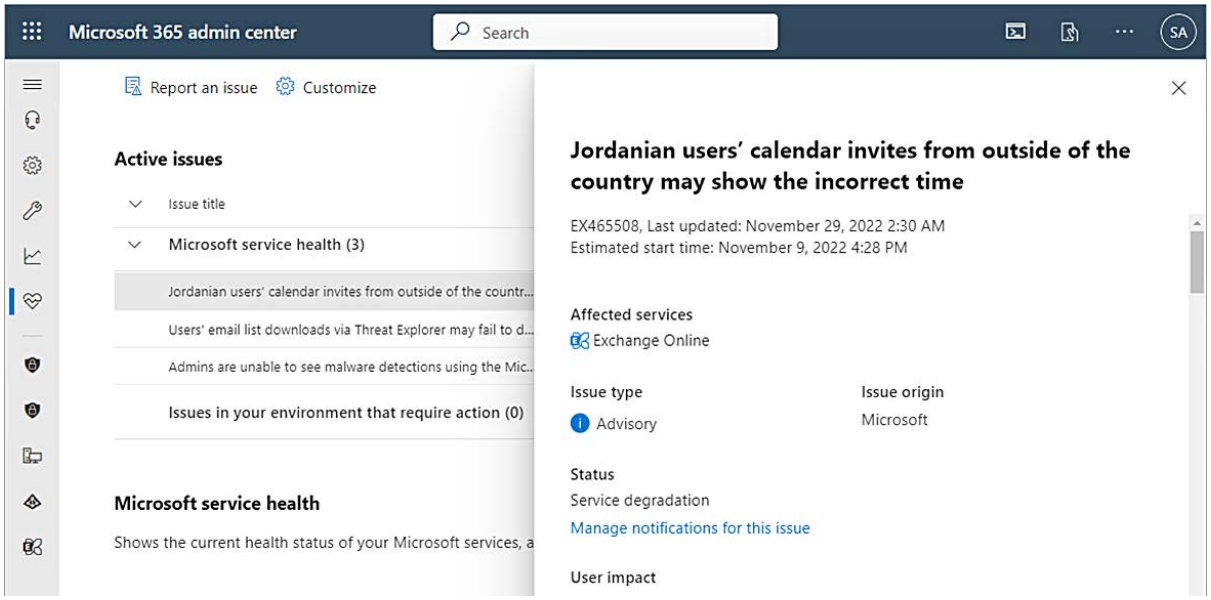

Figure 1.20 – Expanded active issue

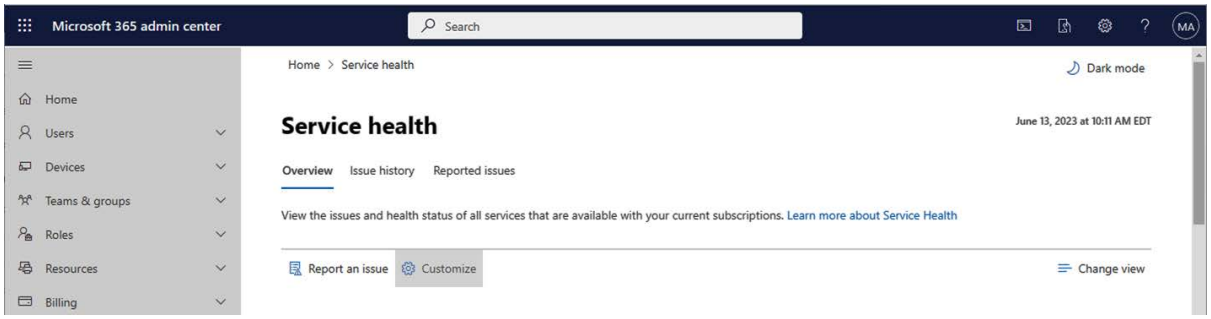

Figure 1.21 – Service health page with Customize highlighted

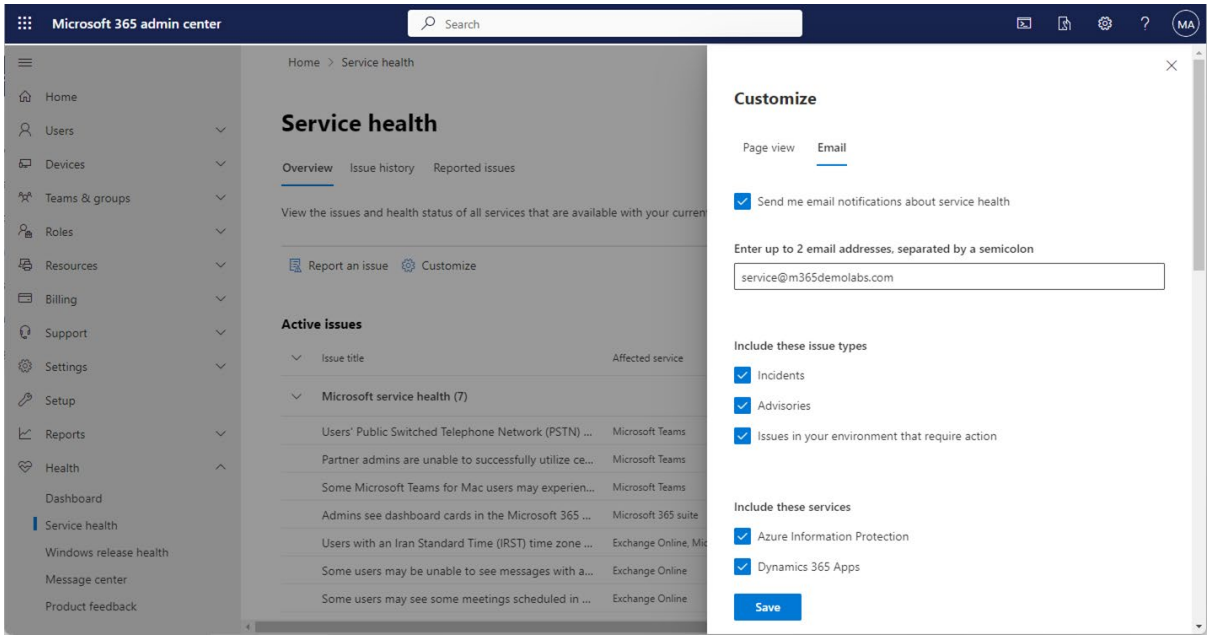

Figure 1.22 – Enabling notifications

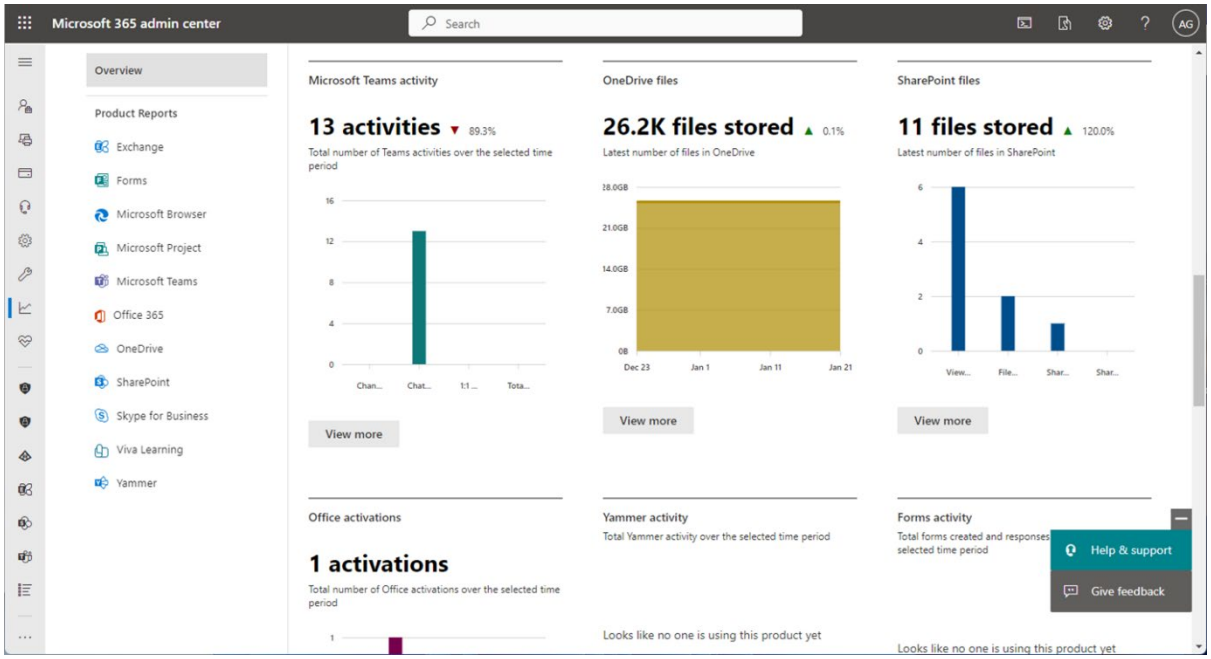

Figure 1.23 – Microsoft 365 usage reports

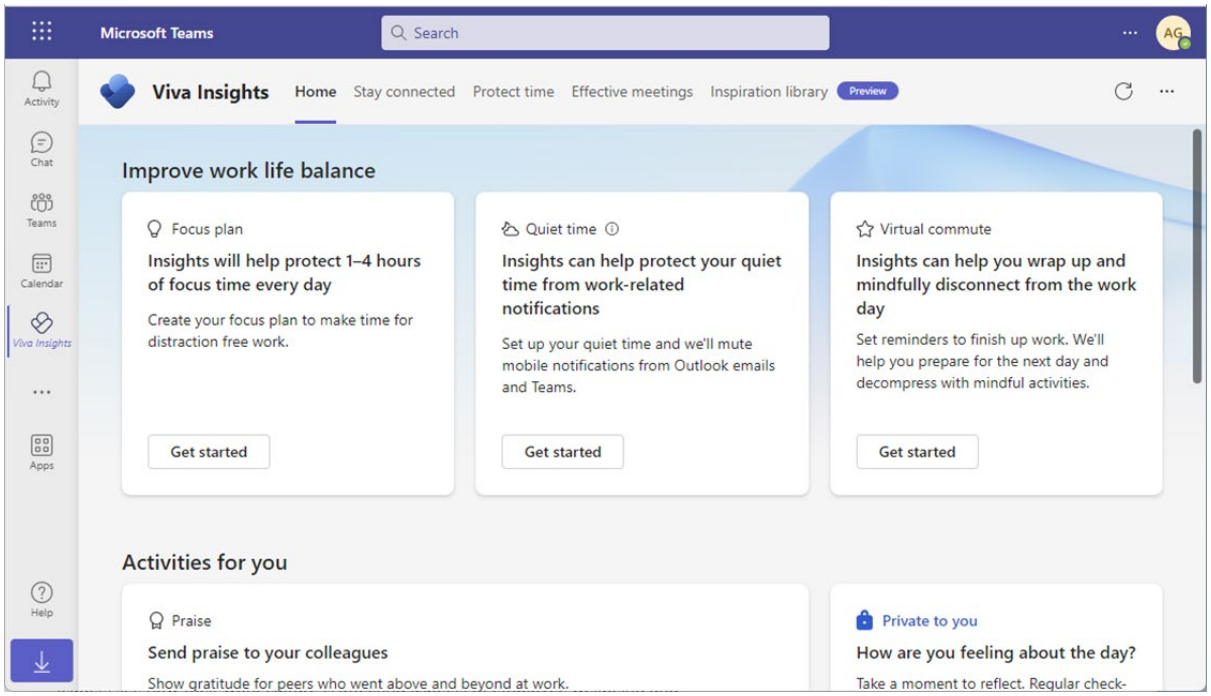

Figure 1.24 – Viva Insights app in Microsoft Teams

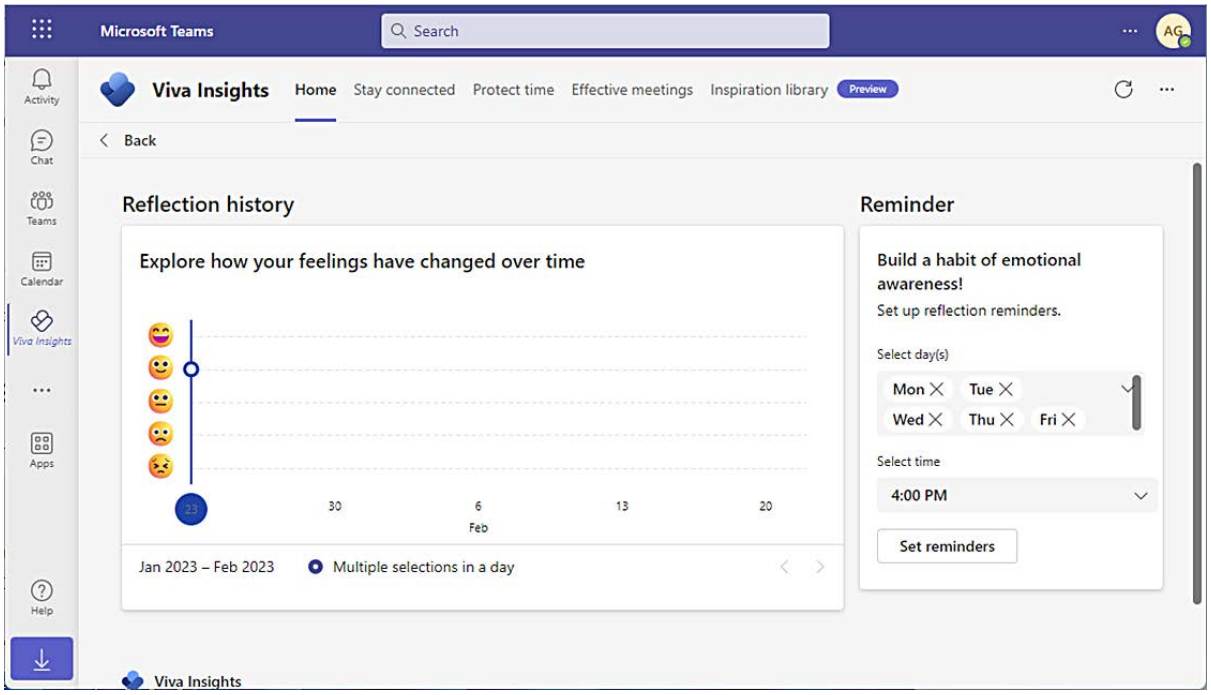

Figure 1.25 – Reflection activity card

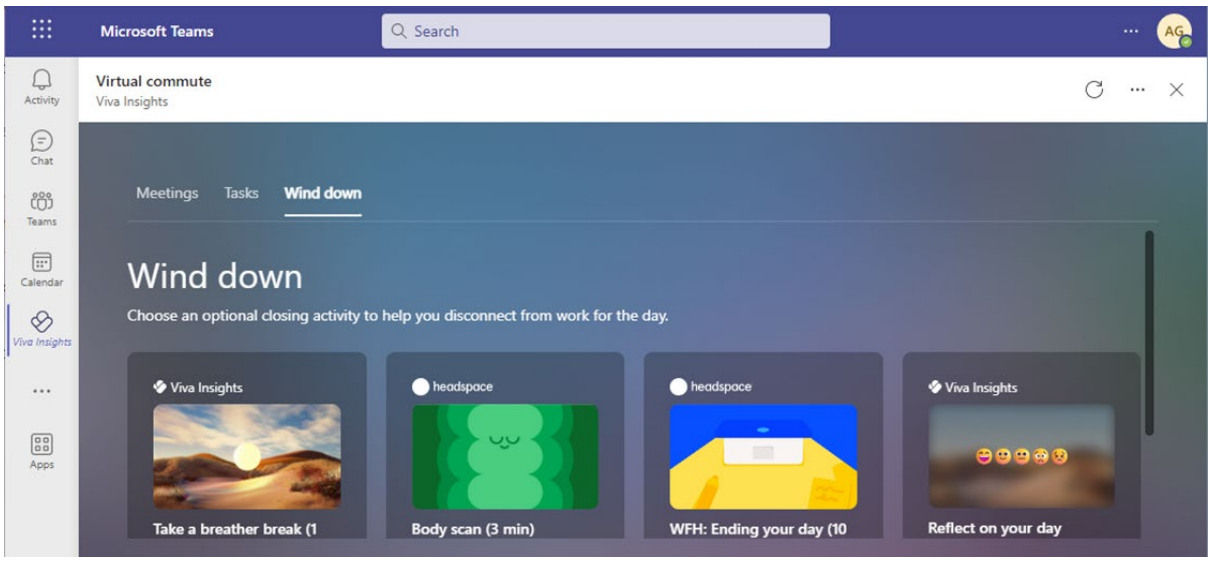

Figure 1.26 – Virtual commute activity card

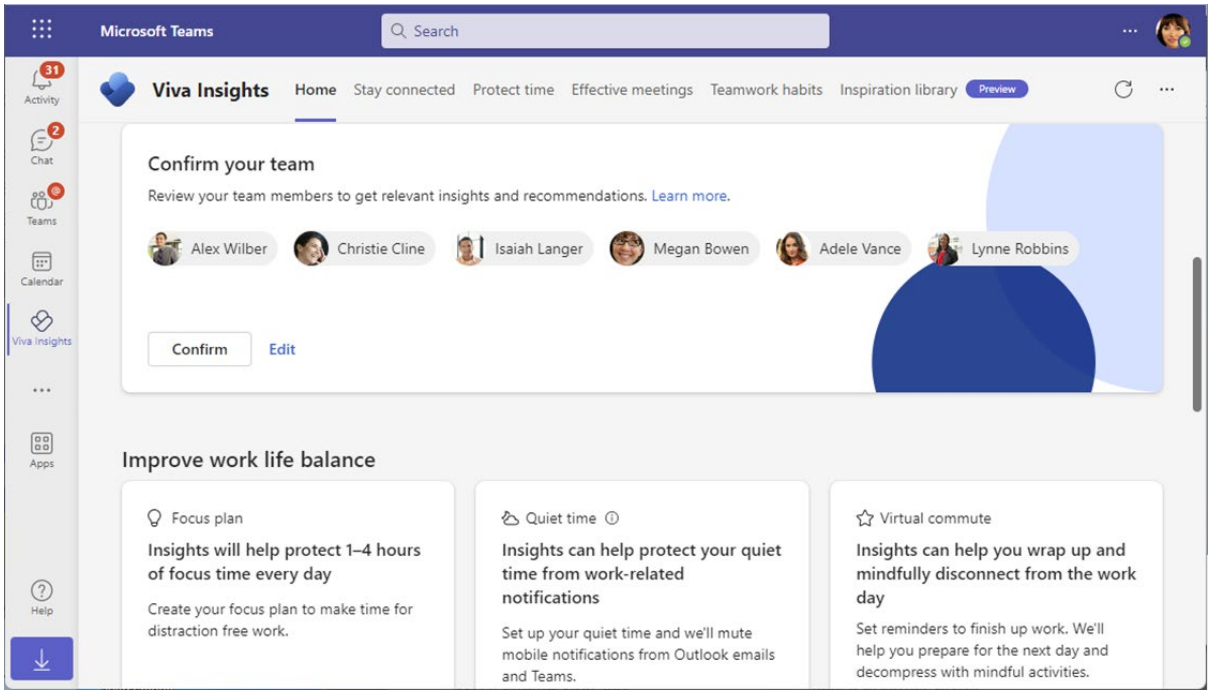

Figure 1.27 – Confirming team members

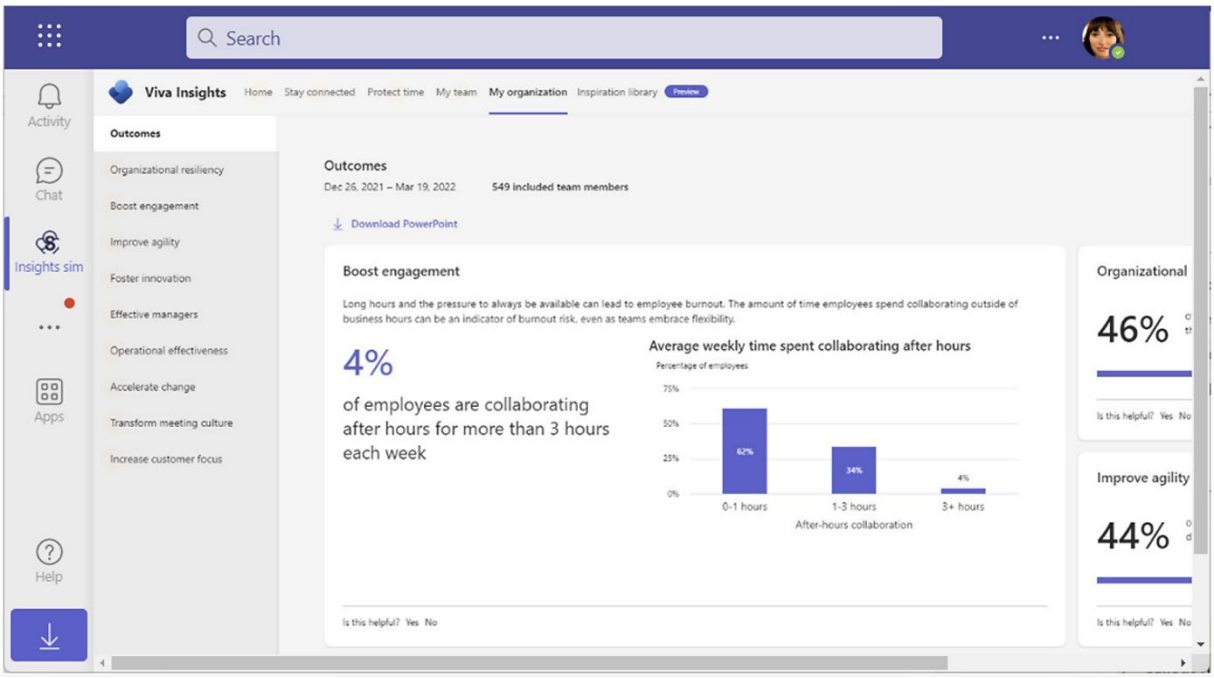

Figure 1.28 – Organization trends

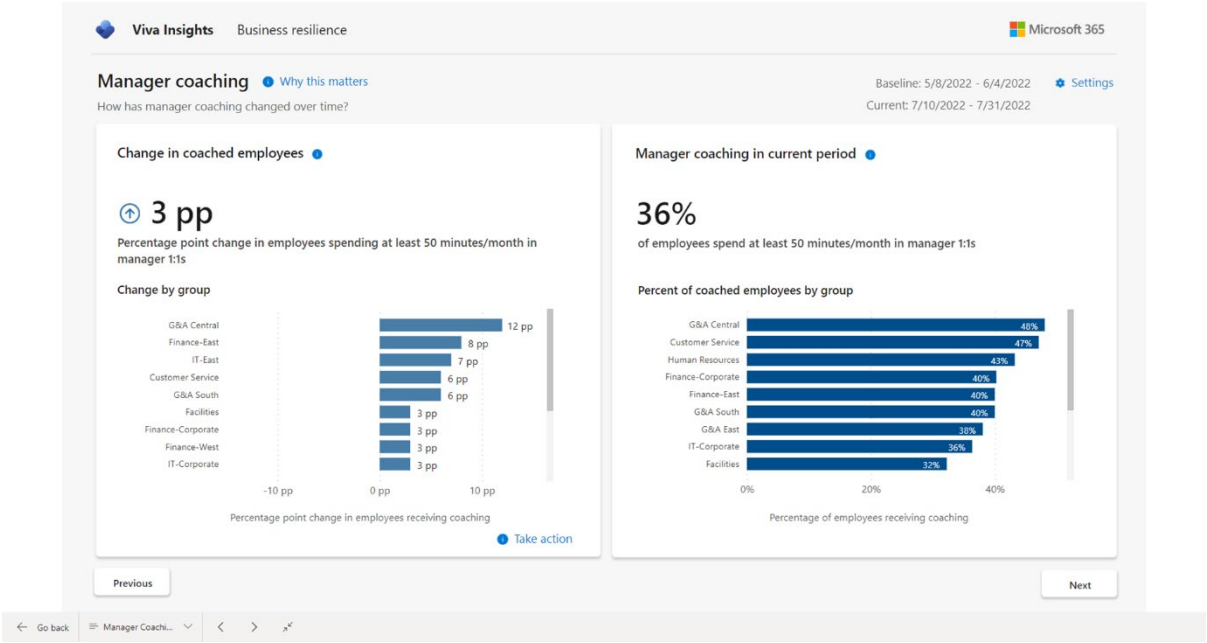

Figure 1.29 – Viva Insights Manager coaching report

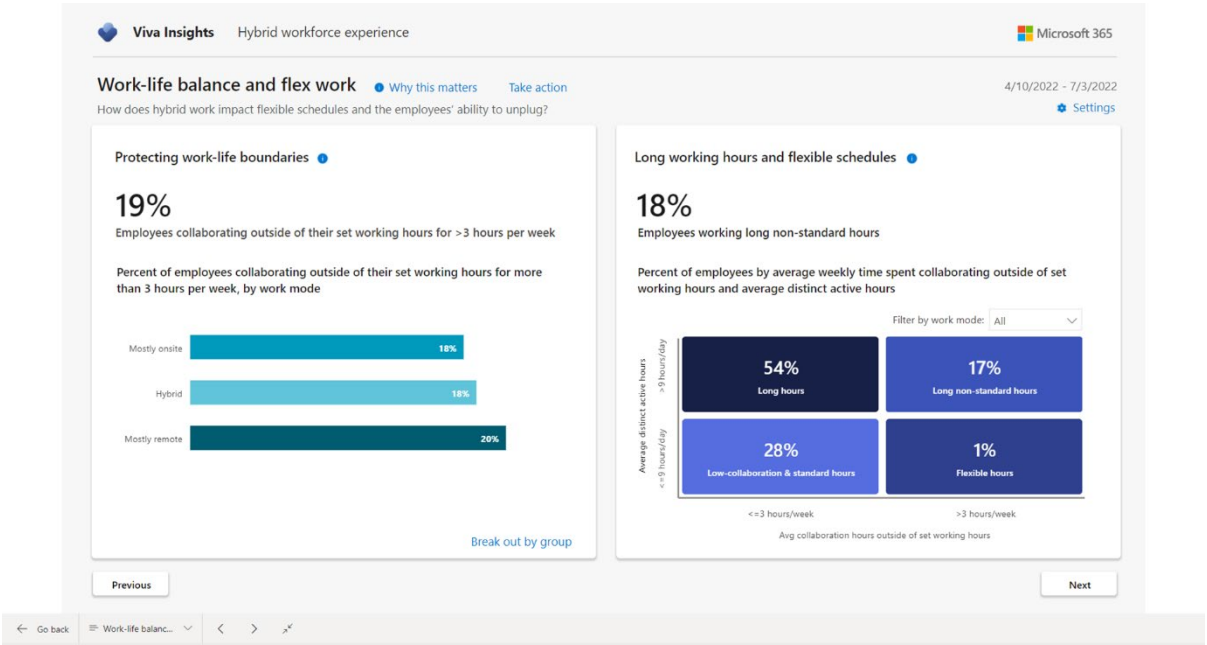

Figure 1.30 – Advanced insights working hour details

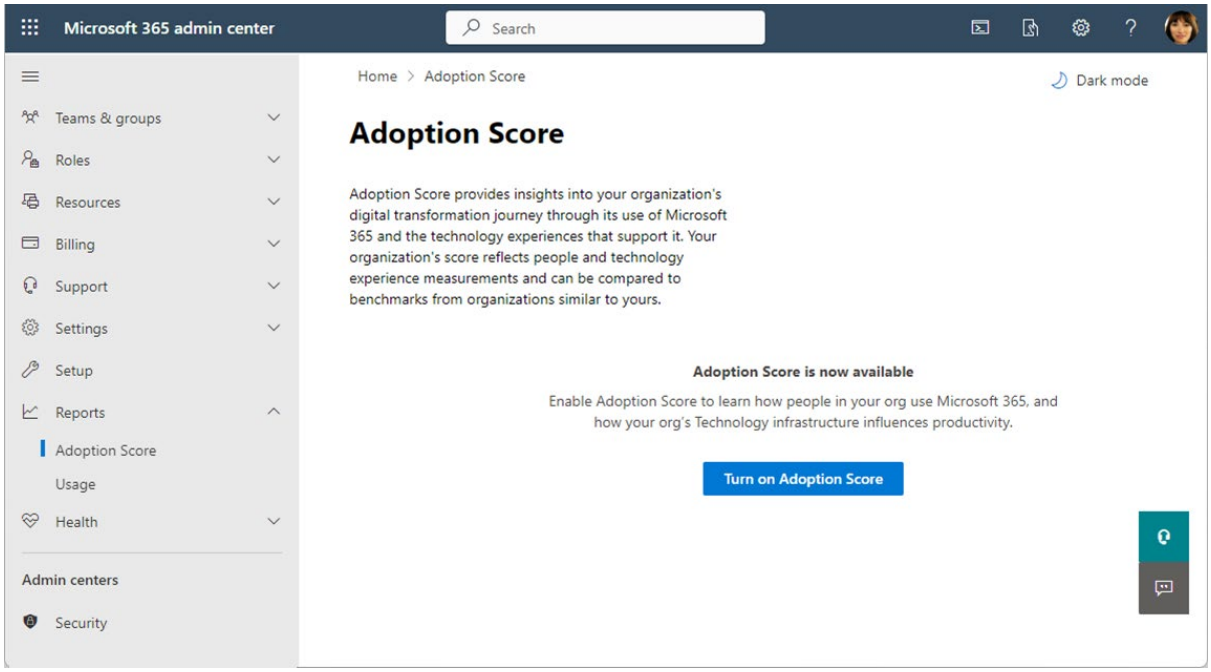

Figure 1.31 – Enabling Adoption Score

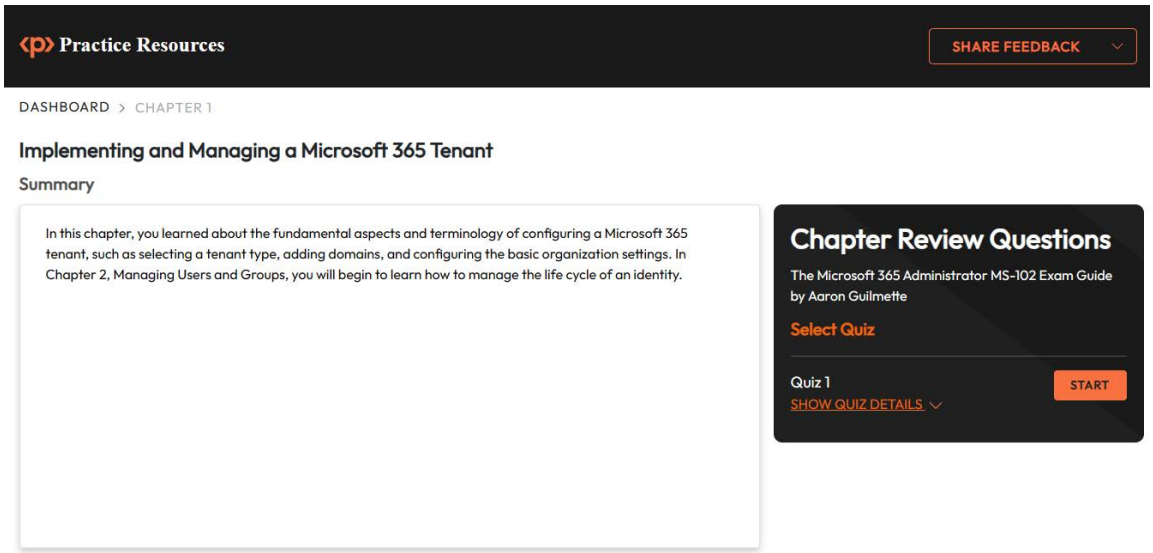

Figure 1.32 – Chapter Review Questions for Chapter 1

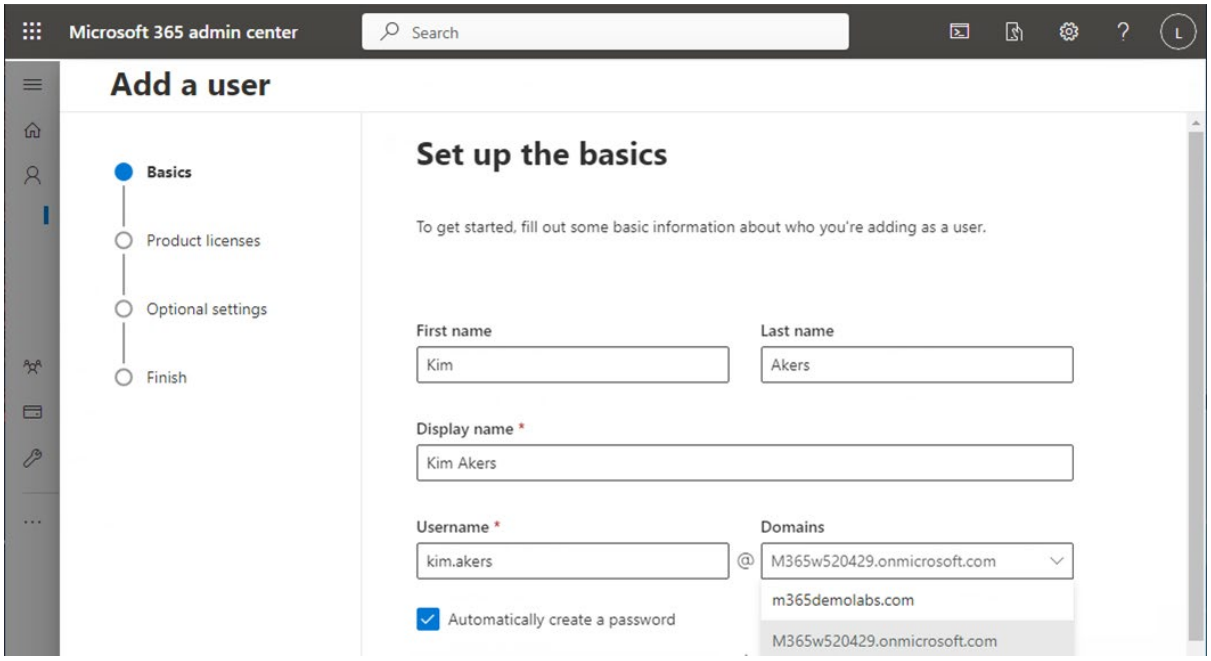

Figure 2.1 – Adding a new cloud user

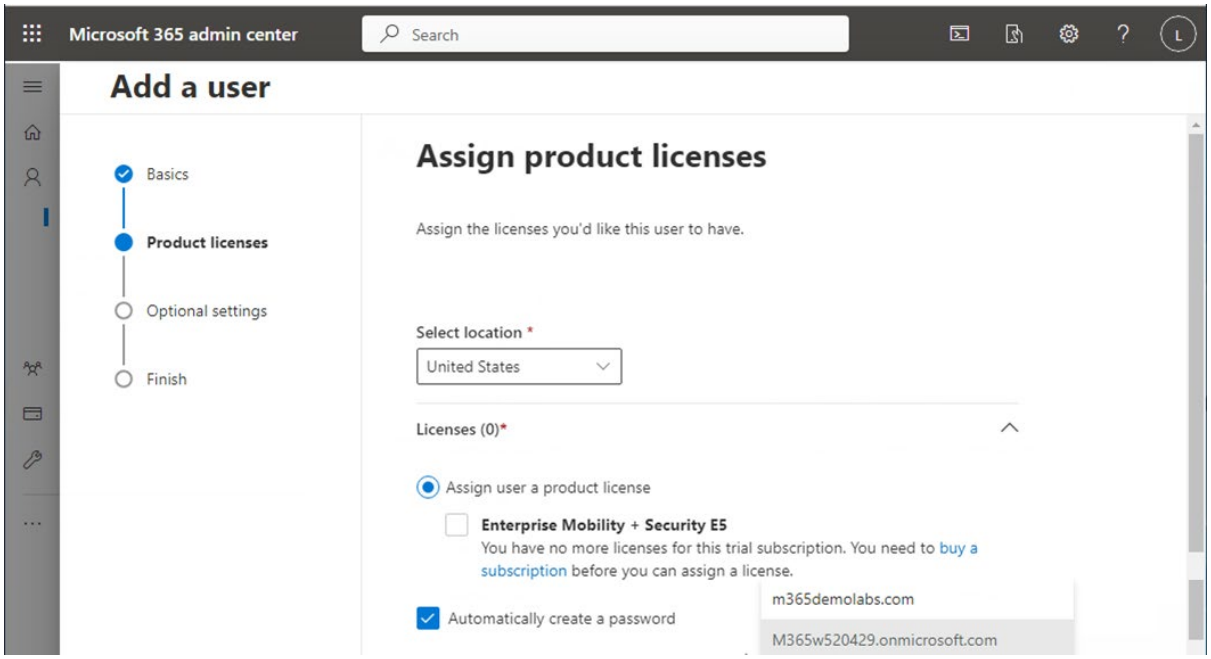

Figure 2.2 – Assign product licenses page

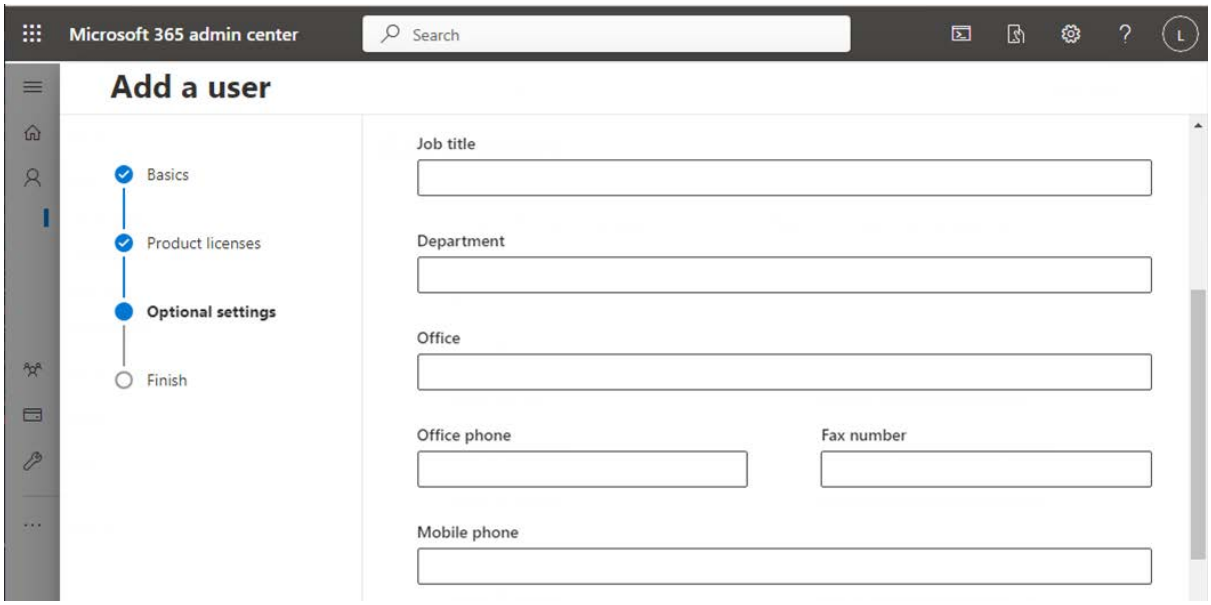

Figure 2.3 – Add a user profile information

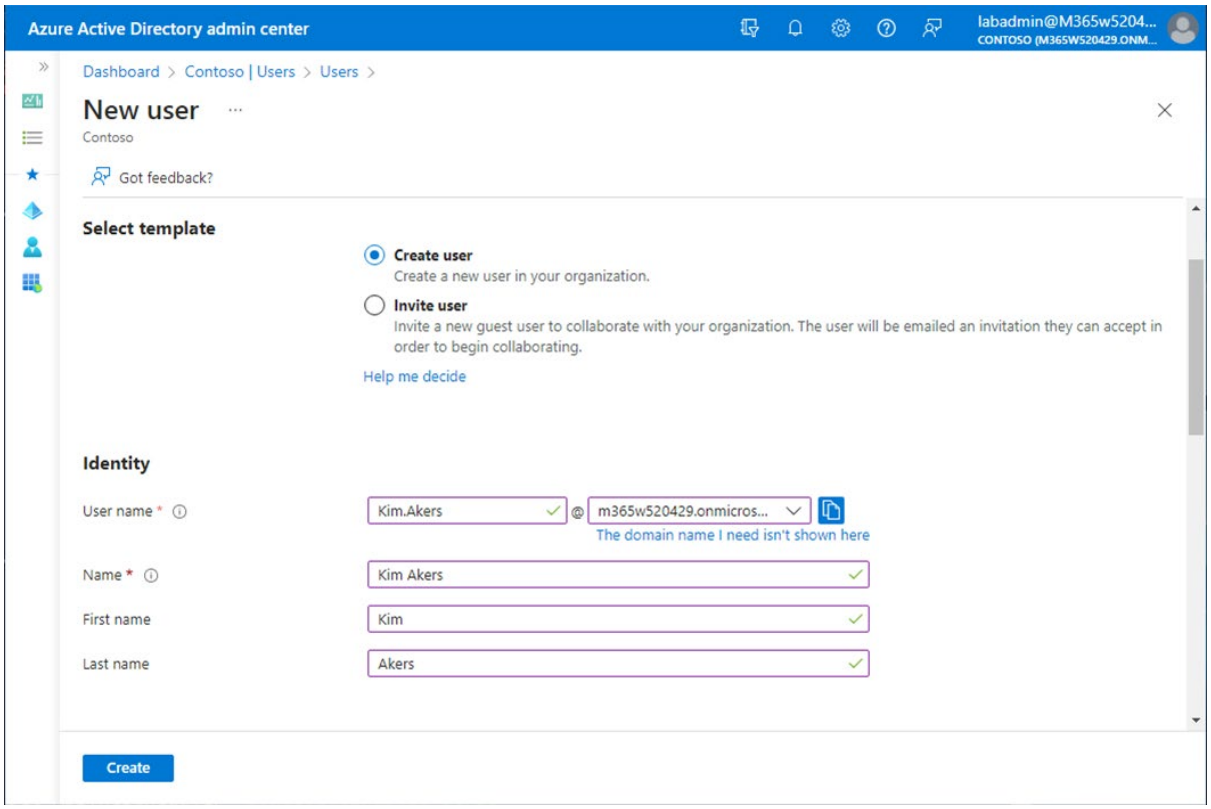

Figure 2.4 – Creating a user through the Azure AD portal

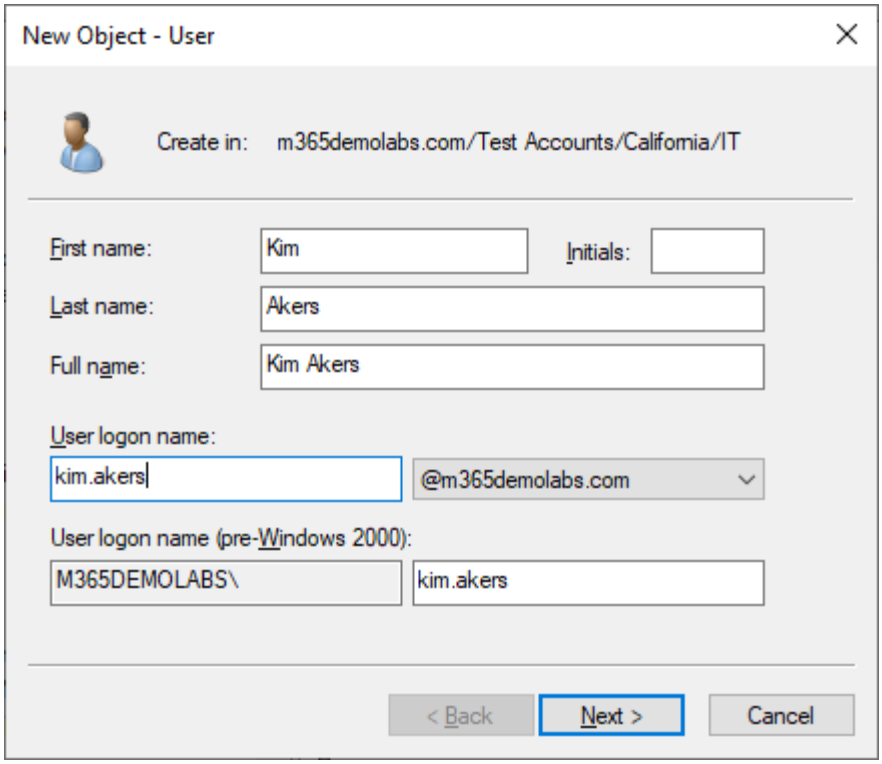

Figure 2.5 – Creating a new user through Active Directory Users and Computers

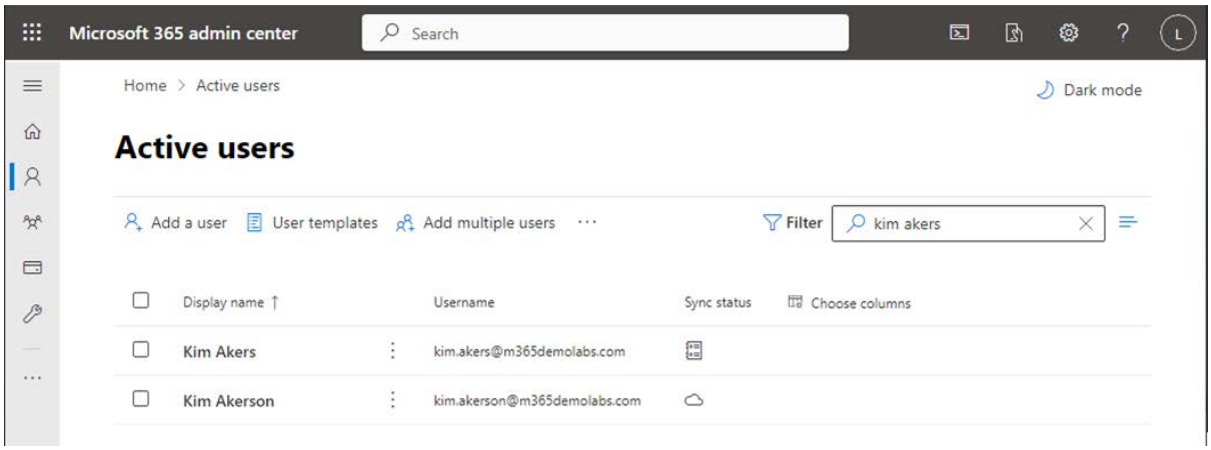

Figure 2.6 – Displaying cloud and synchronized users

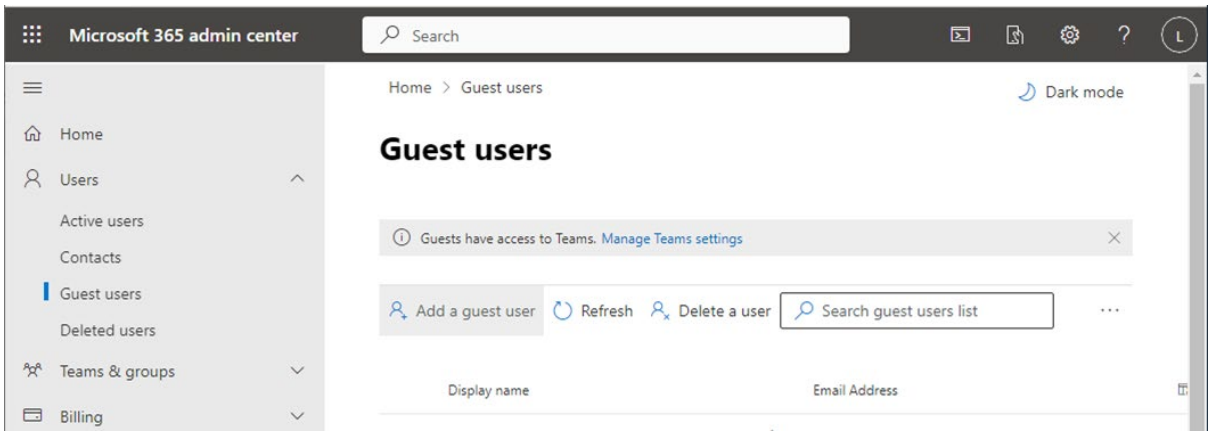

Figure 2.7 – Guest users administration in Microsoft 365 admin center

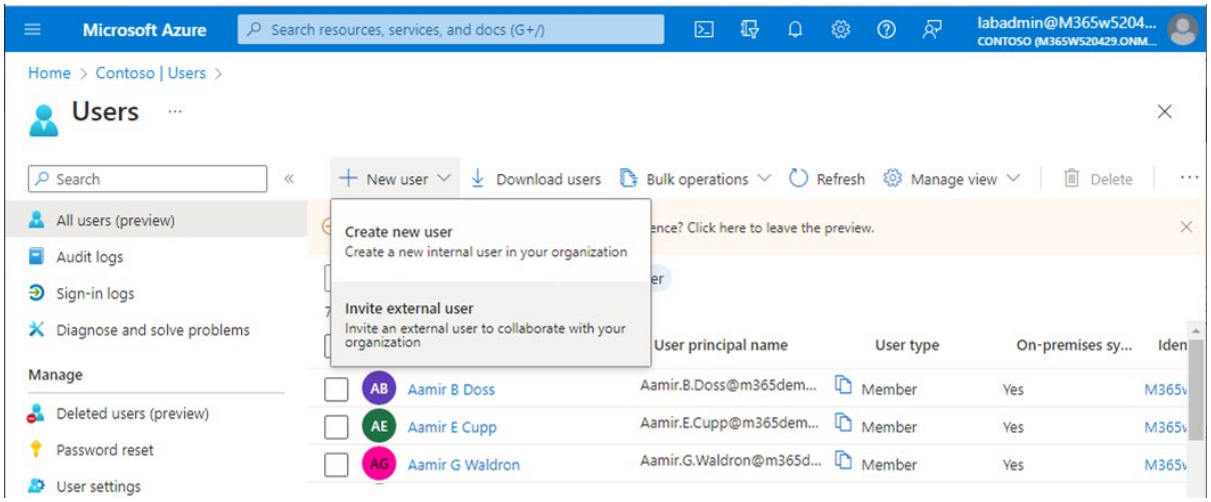

Figure 2.8 – Inviting a new guest user

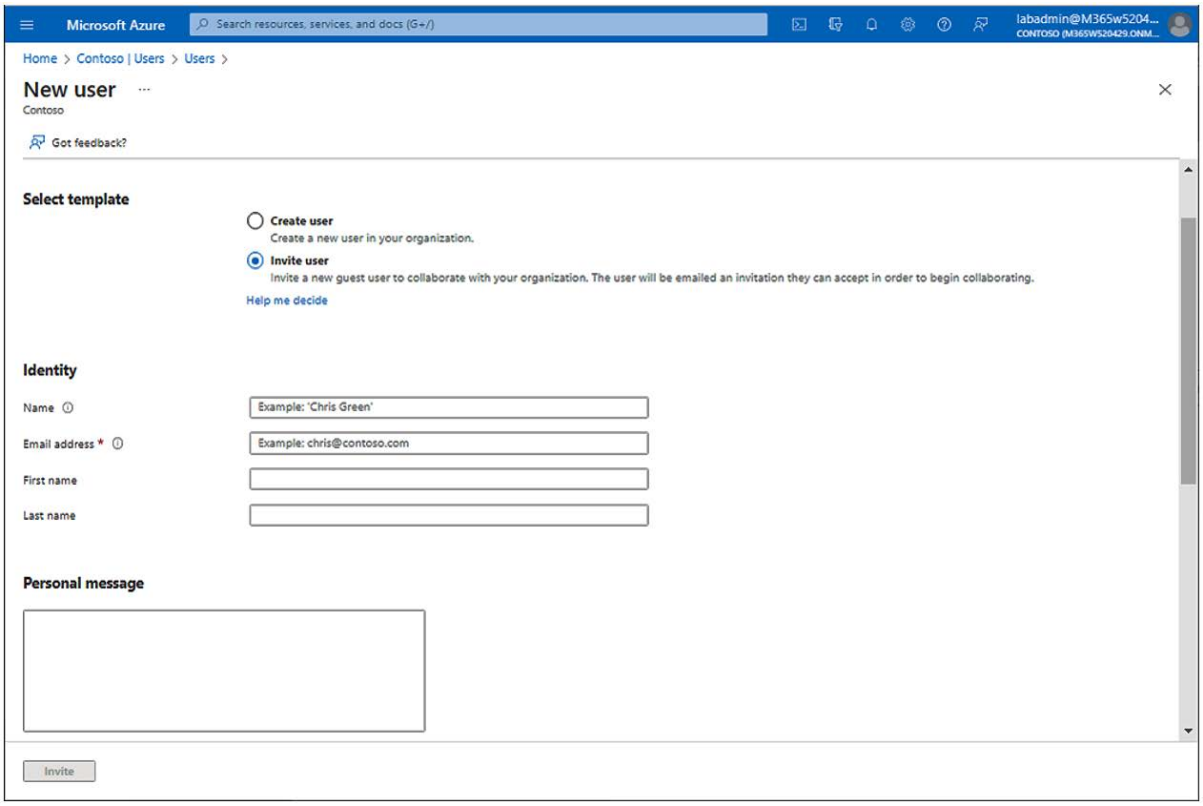

Figure 2.9 – Configuring the guest invitation

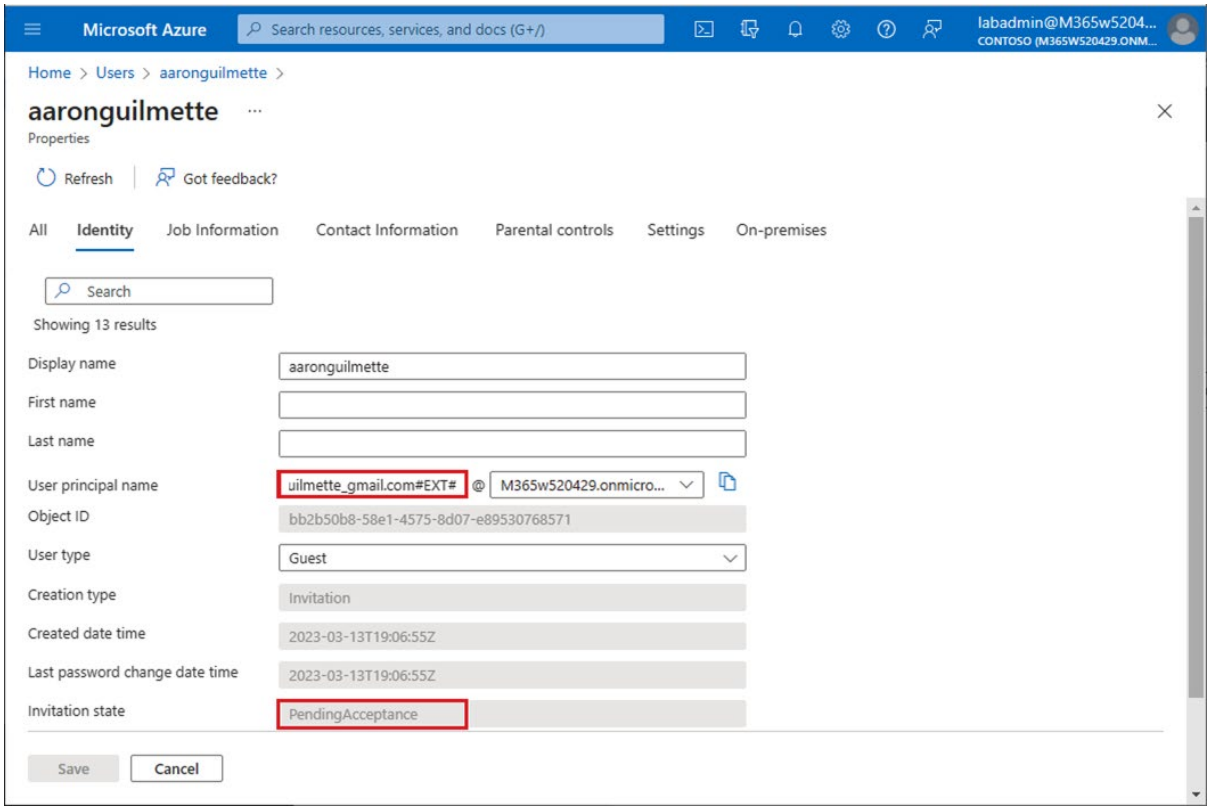

Figure 2.10 – Newly invited guest user

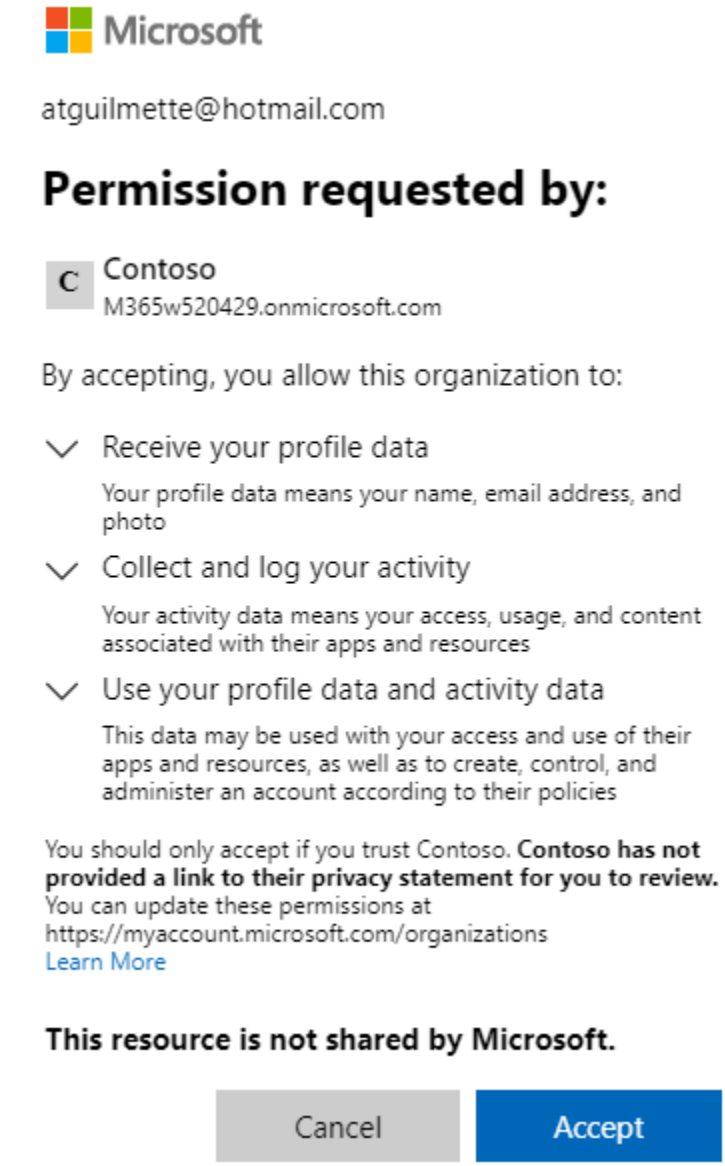

Figure 2.11 – Invitation redemption consent

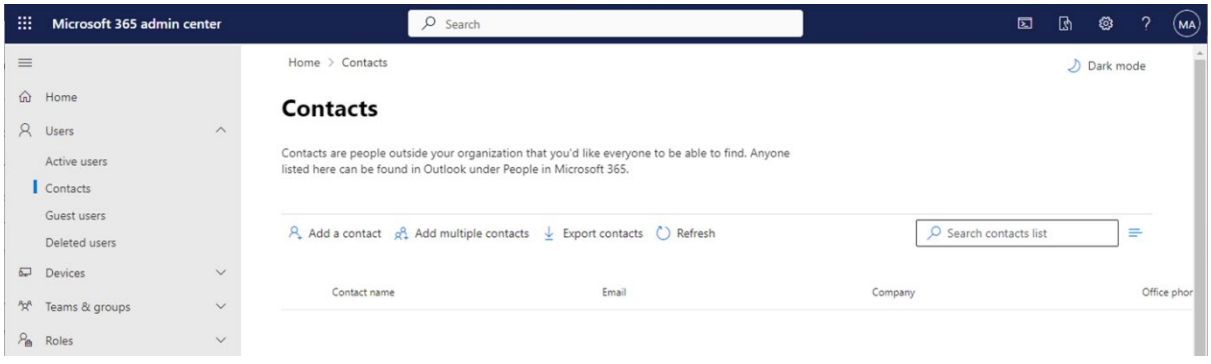

Figure 2.12 – Contacts page in Microsoft 365 admin center

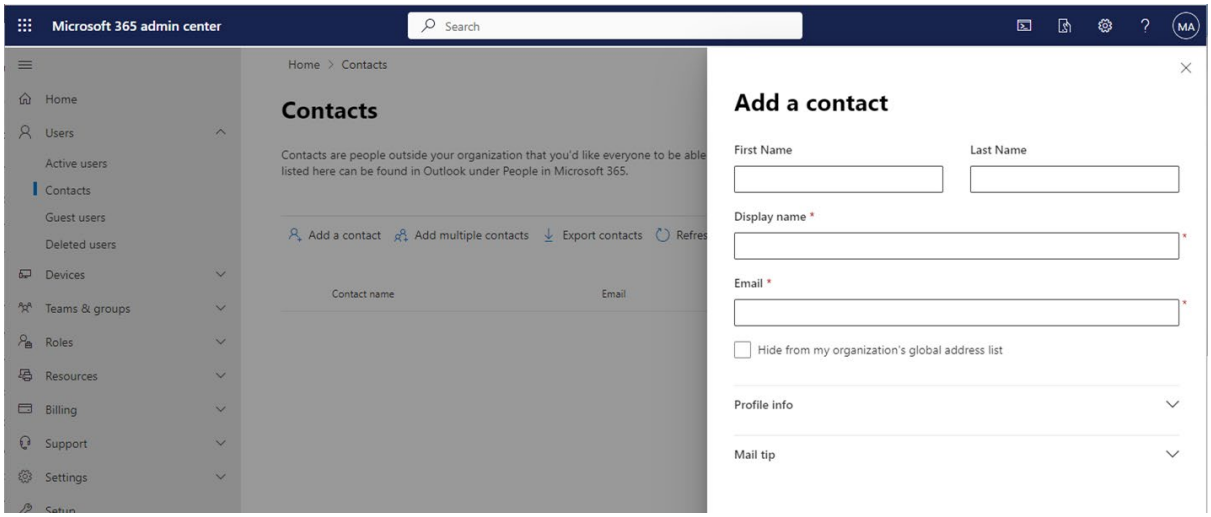

Figure 2.13 – Populating a contact

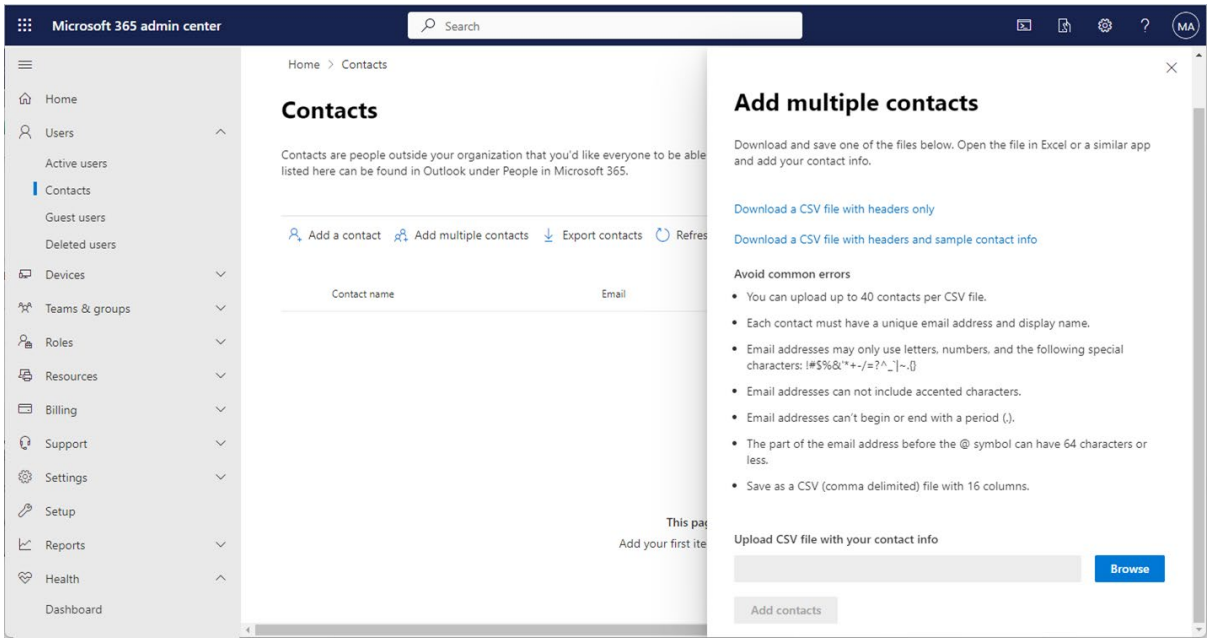

Figure 2.14 – Add multiple contacts flyout

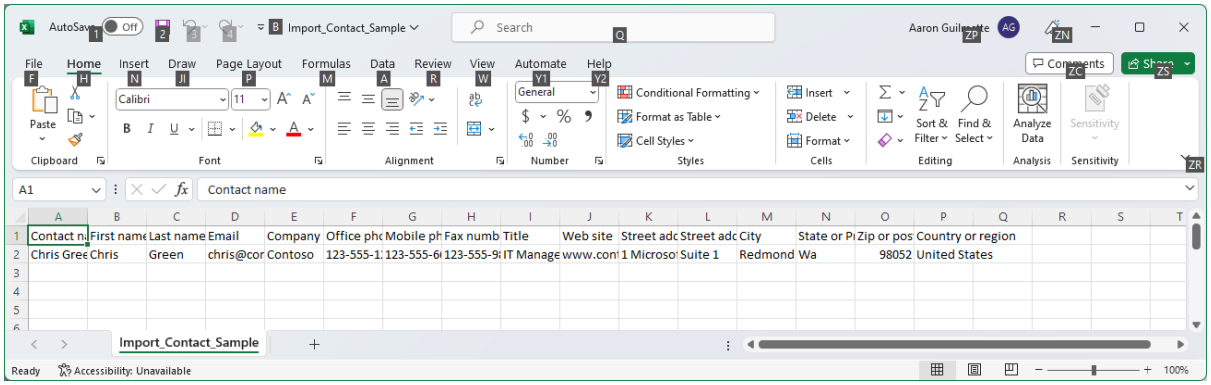

Figure 2.15 – Bulk contact import template

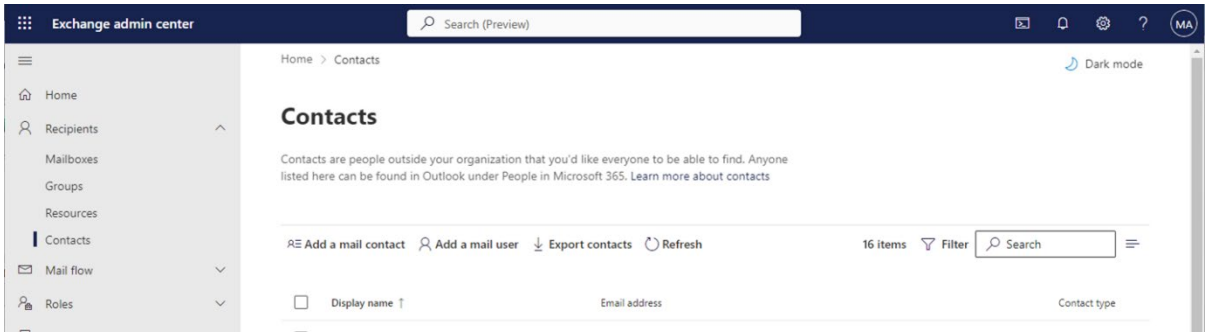

Figure 2.16 – Exchange admin center contact administration

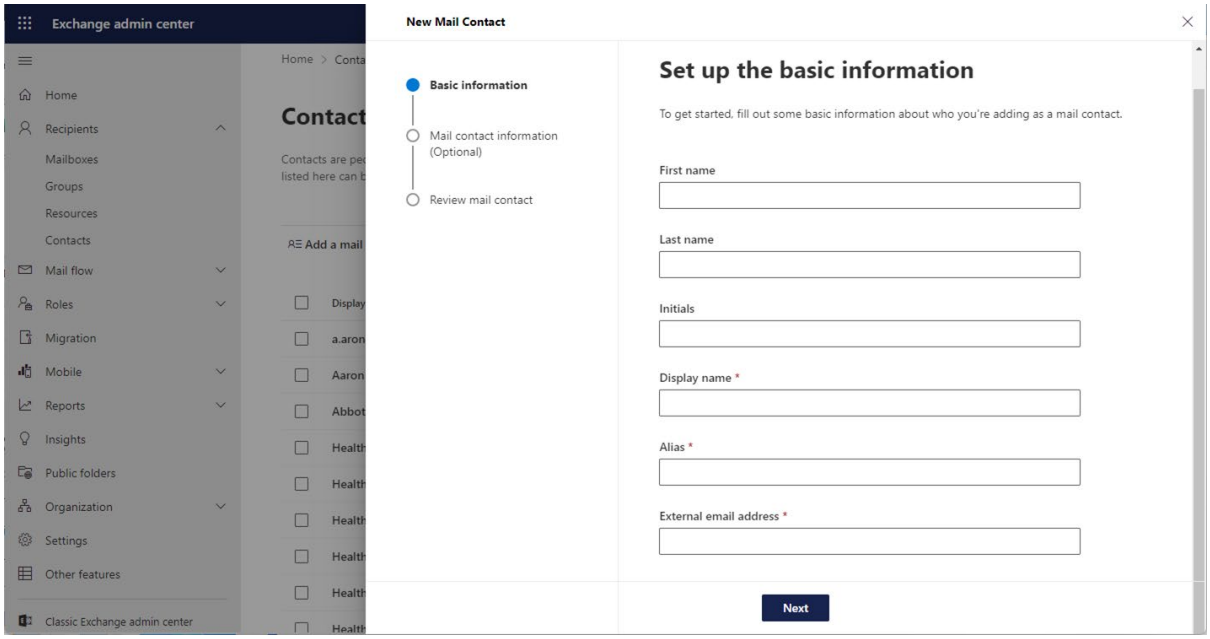

Figure 2.17 – New Mail Contact wizard in Exchange admin center

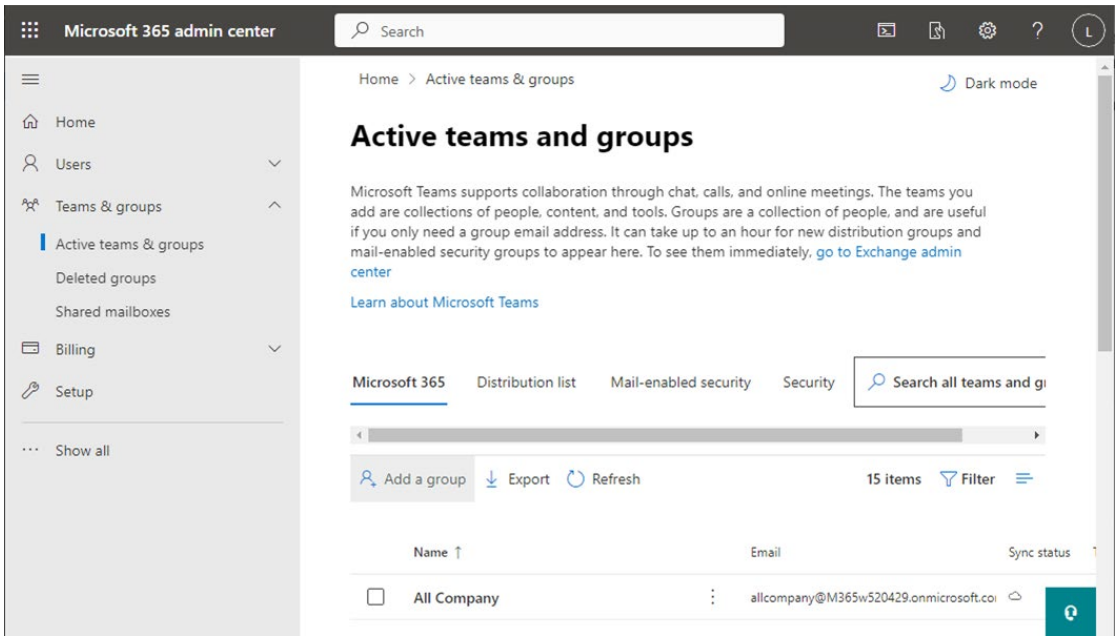

Figure 2.18 – Active teams and groups

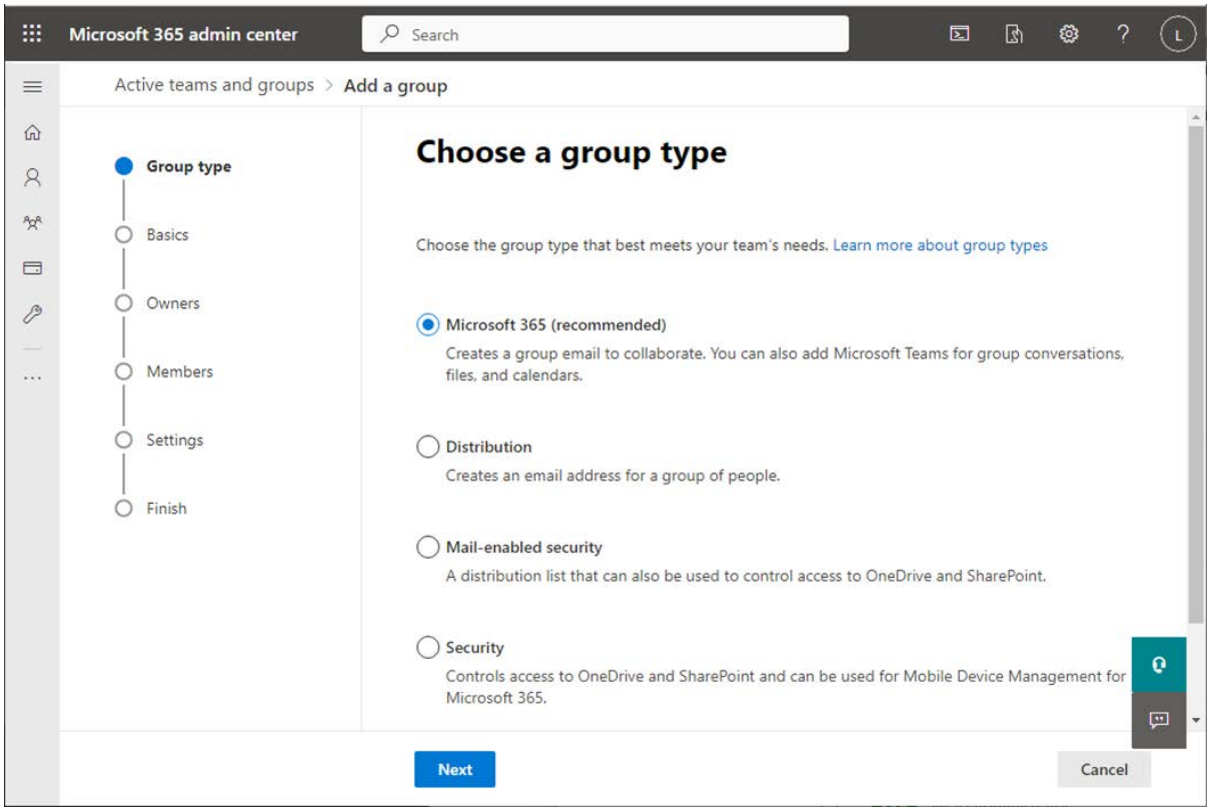

Figure 2.19 – Choose a group type

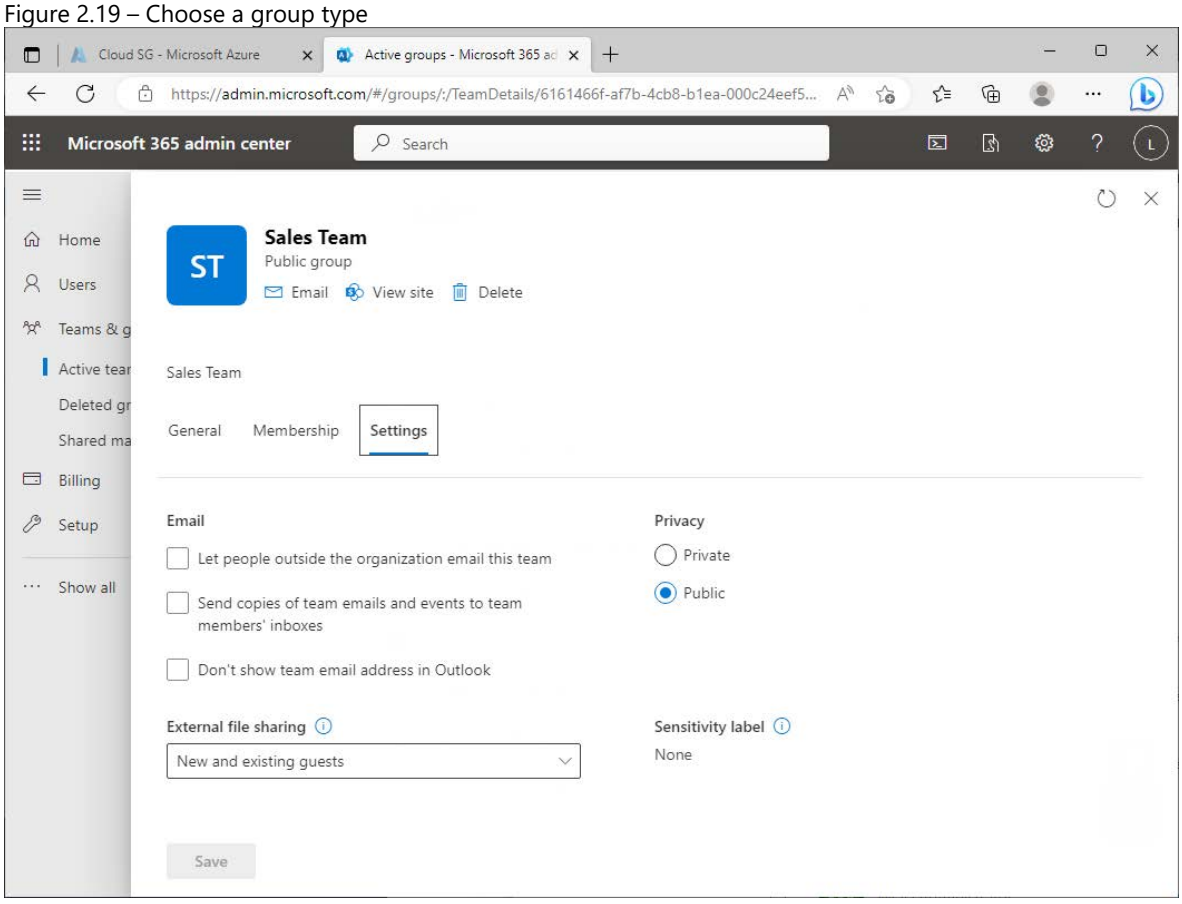

Figure 2.20 – Modifying settings of a Microsoft 365 group

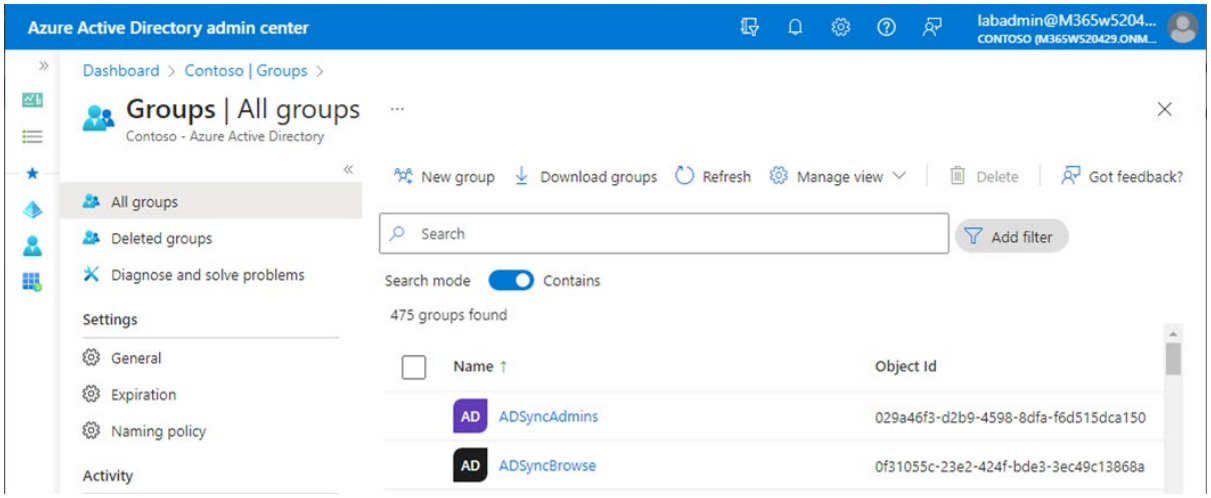

Figure 2.21 – Azure AD all groups

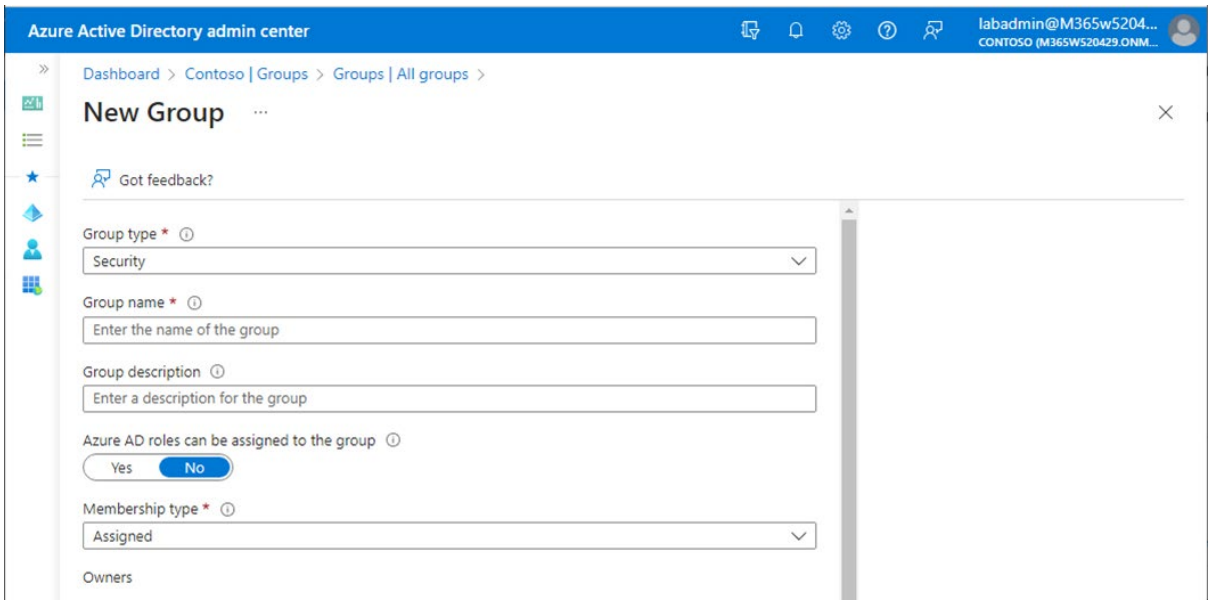

Figure 2.22 – New Group page

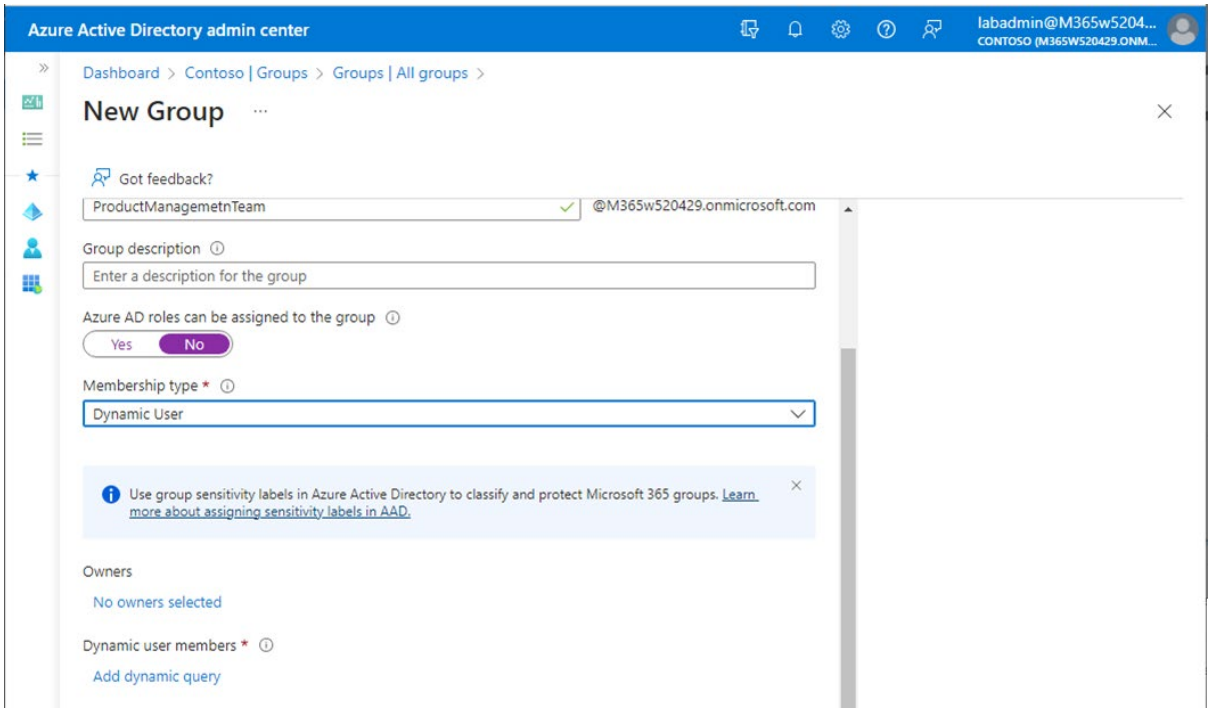

Figure 2.23 – Creating a new dynamic group

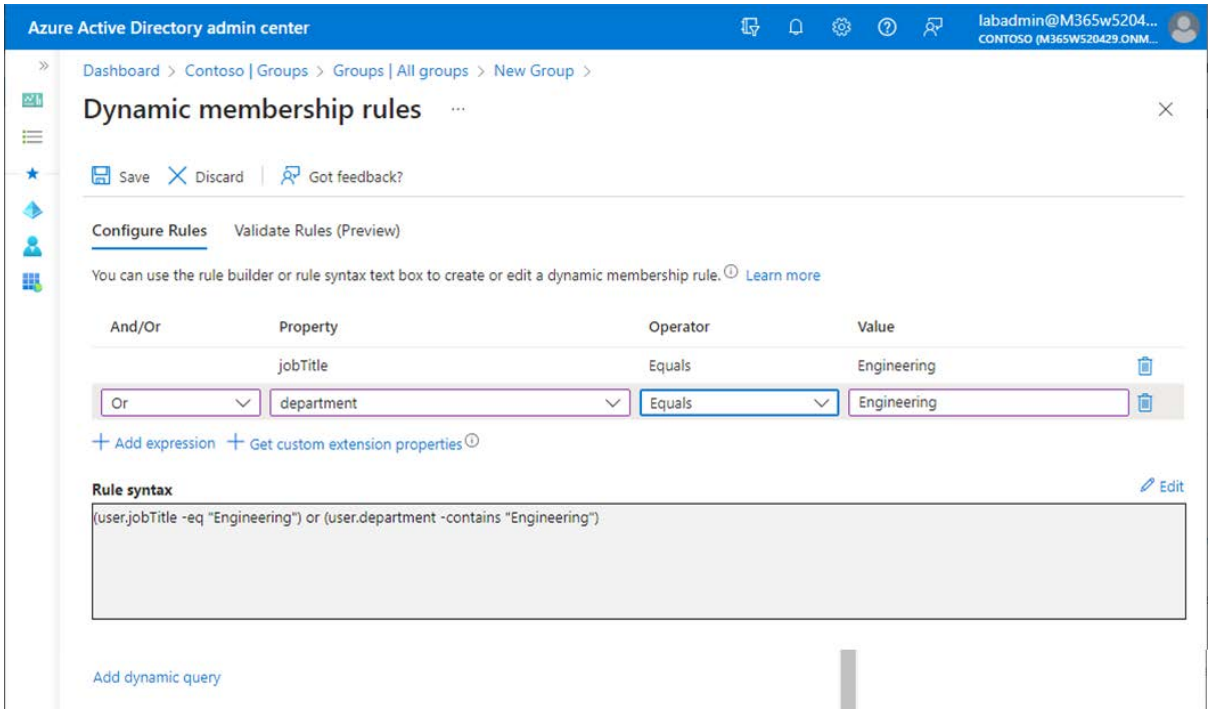

Figure 2.24 – Creating a dynamic membership rule

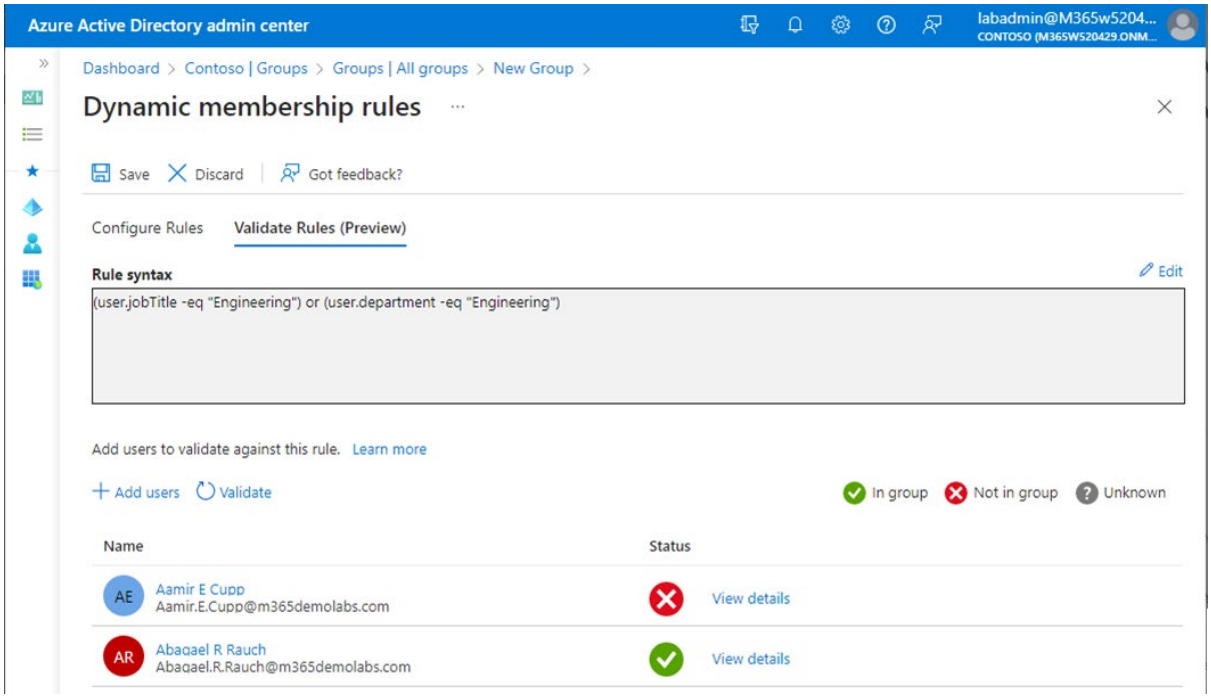

Figure 2.25 – Validating the dynamic membership rule

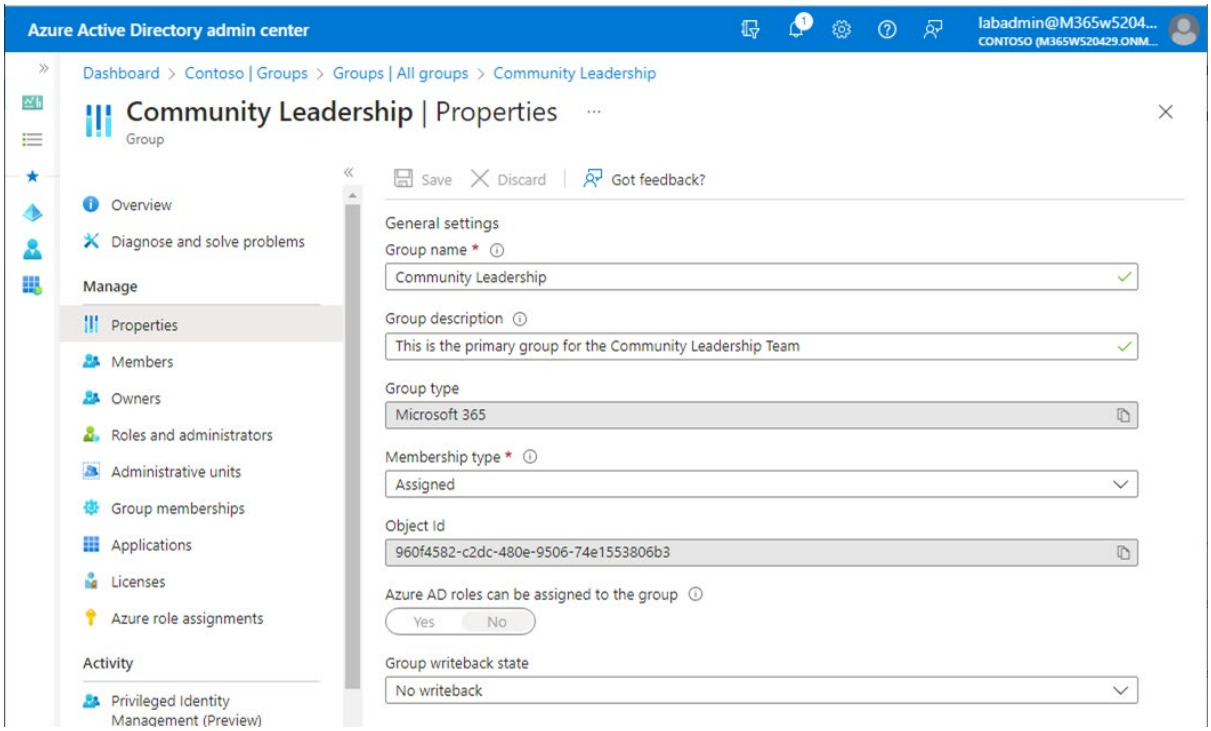

Figure 2.26 – Editing a group

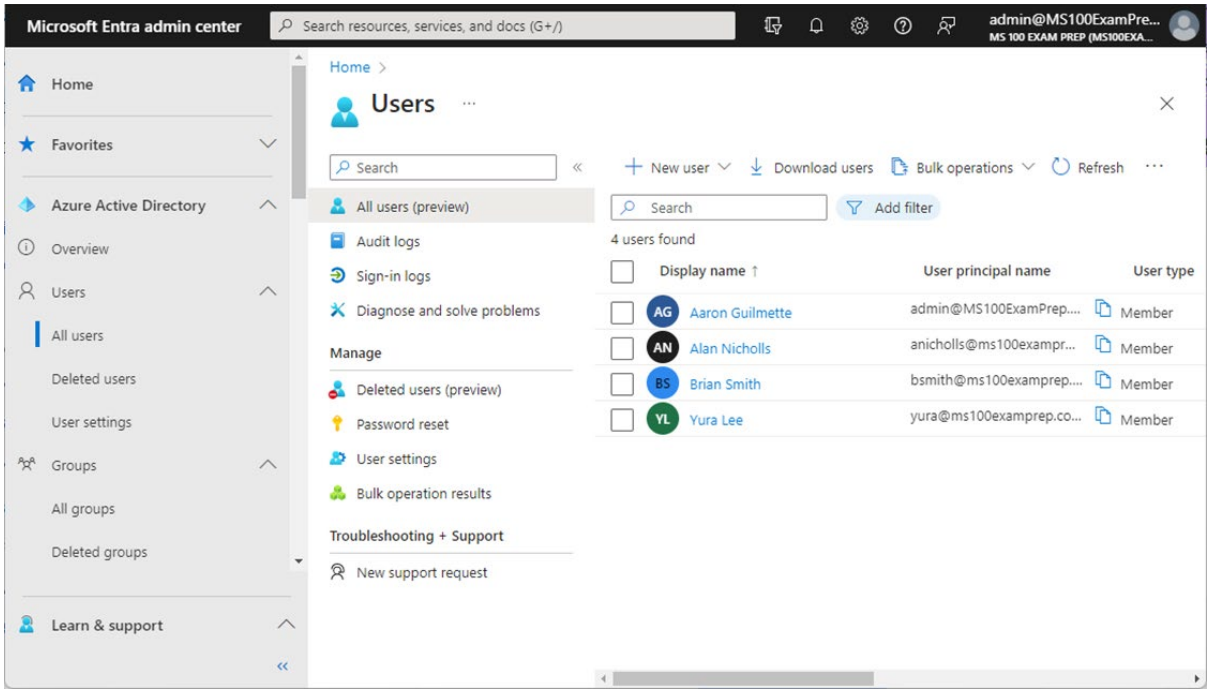

Figure 2.27 – Entra admin center

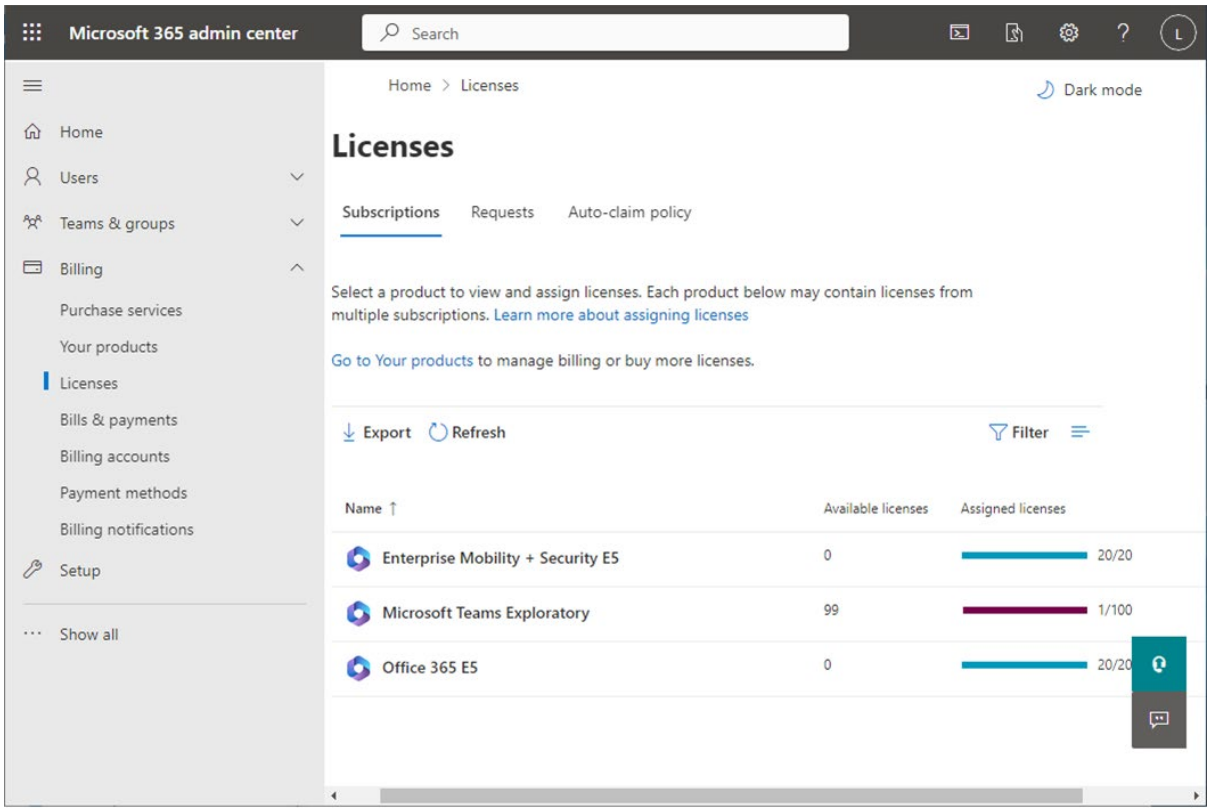

Figure 2.28 – License details in the Microsoft 365 admin center

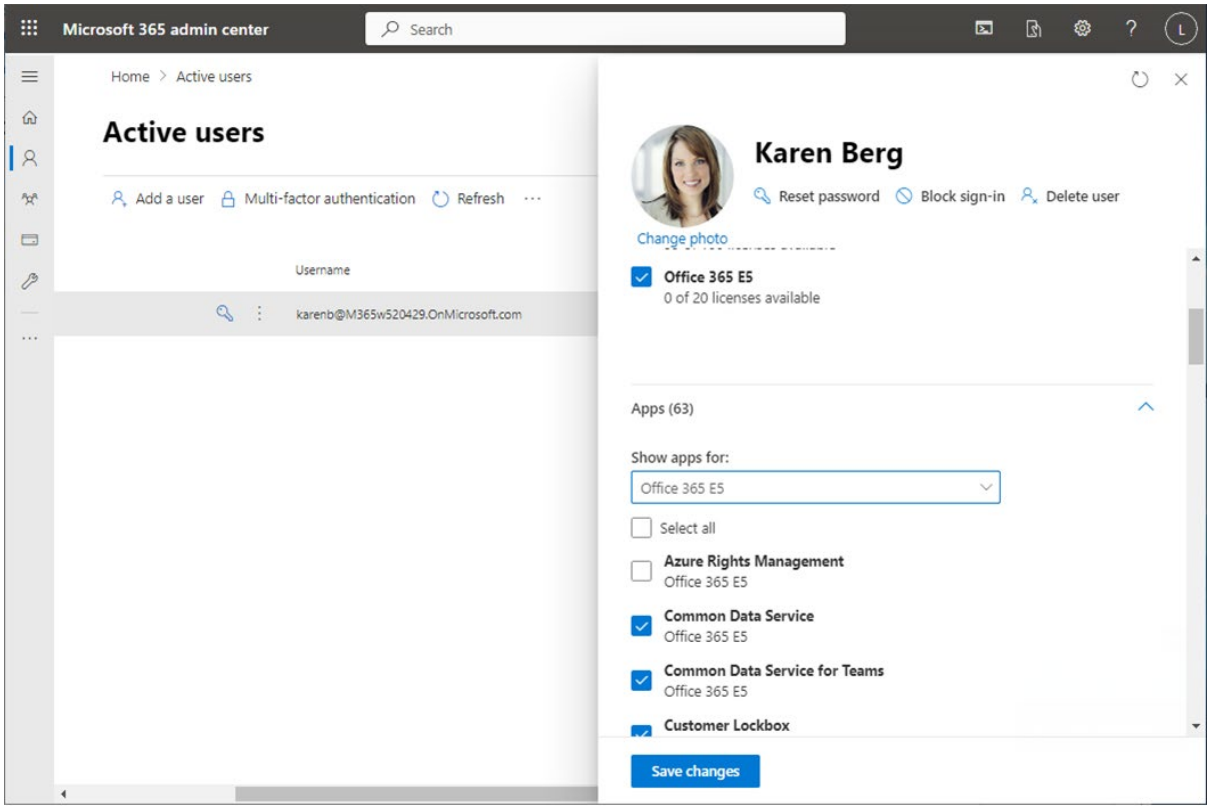

Figure 2.29 – User license management

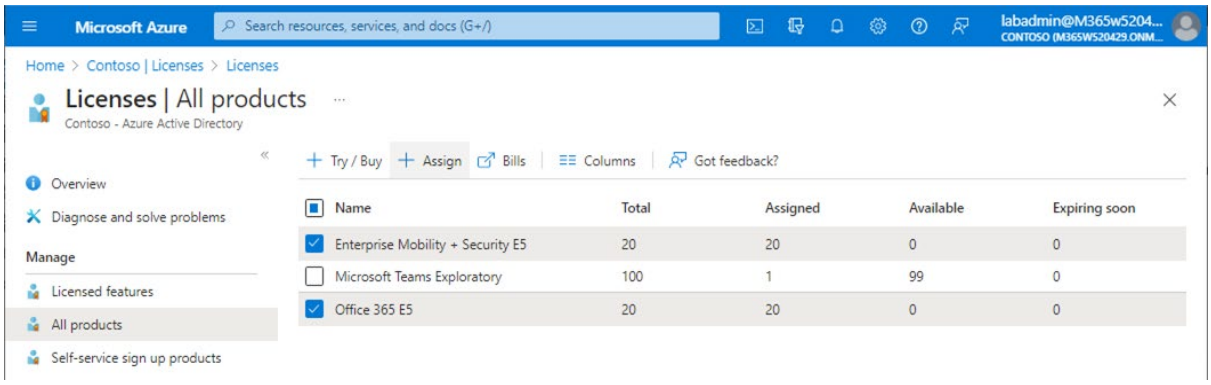

Figure 2.30 – Assign selected licenses to a group

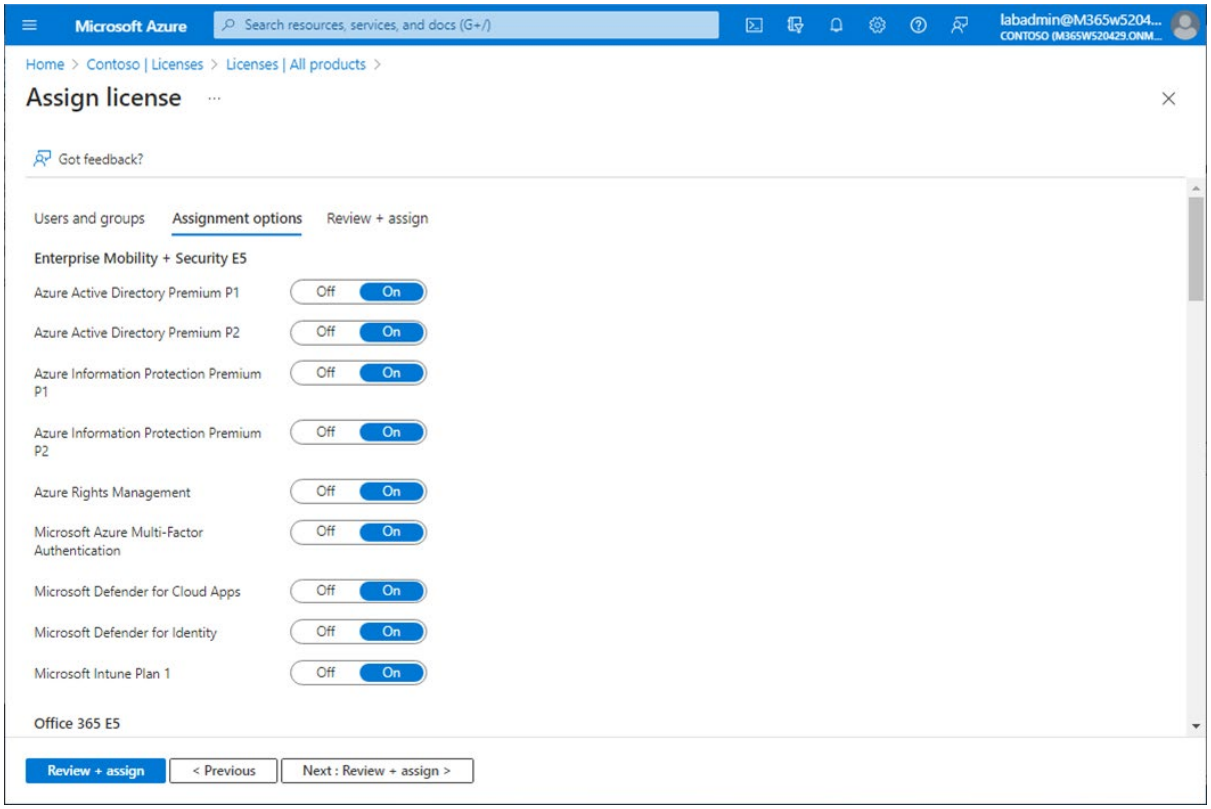

Figure 2.31 – Configuring assignment options

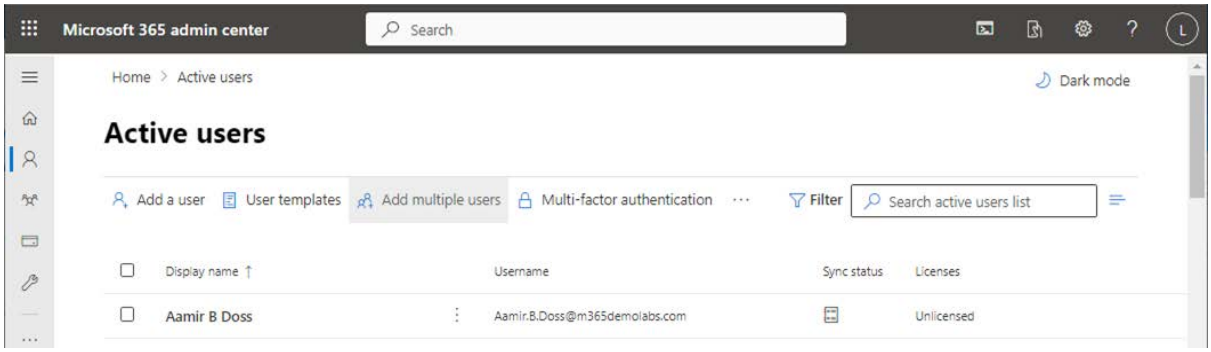

Figure 2.32 – Active users page

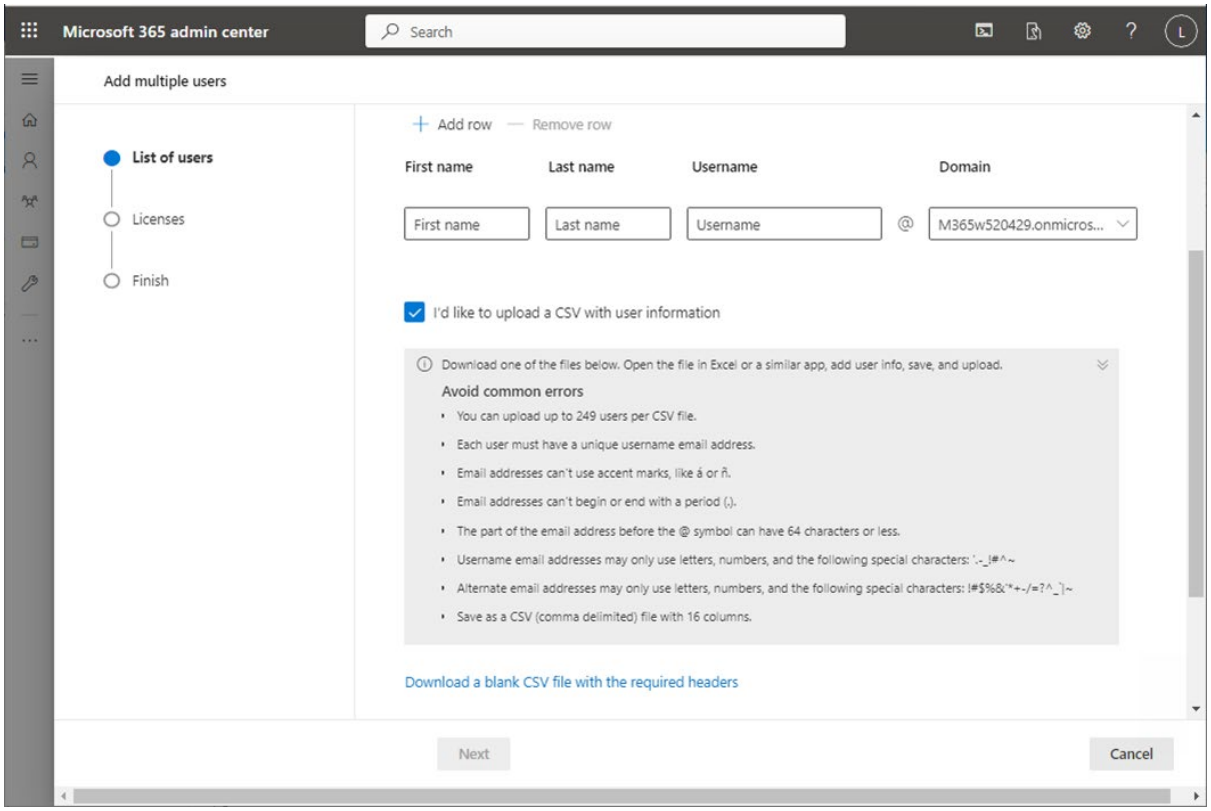

Figure 2.33 – Configuring the bulk user upload

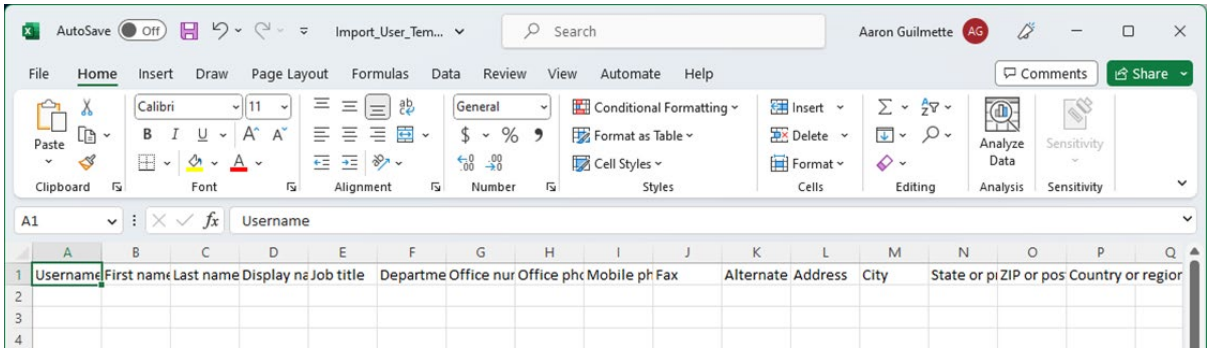

Figure 2.34 – Microsoft 365 admin center bulk user template

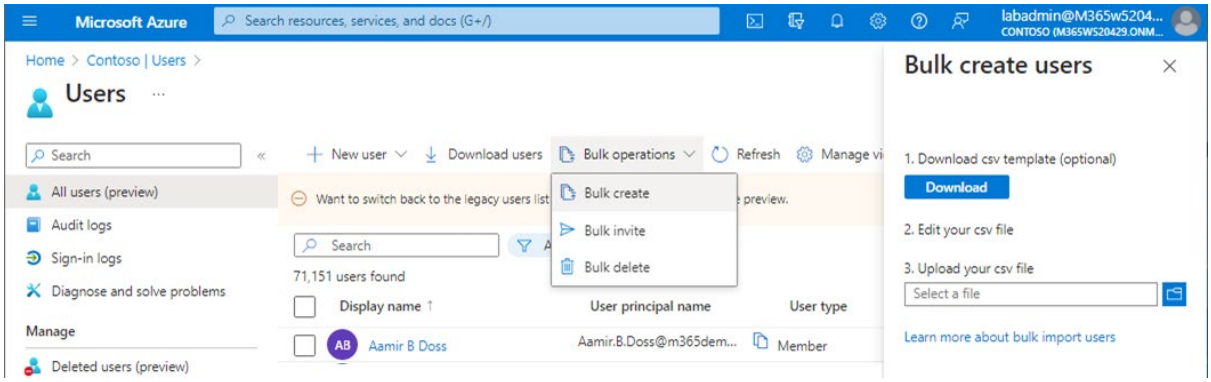

Figure 2.35 – Bulk operations menu in the Azure AD portal

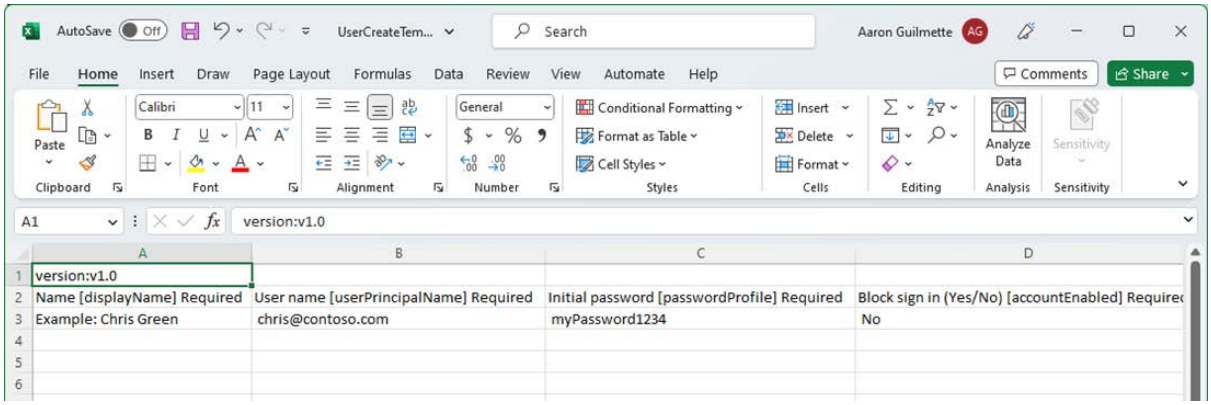

Figure 2.36 – Azure AD bulk user create template

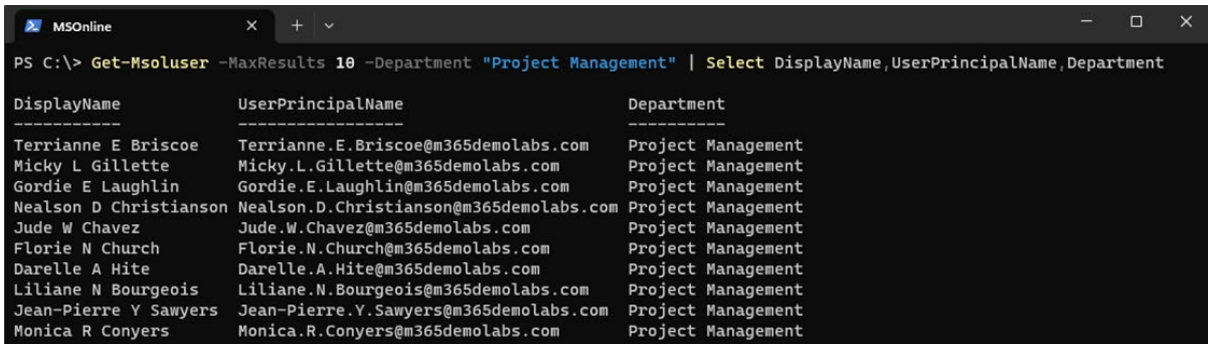

Figure 2.37 – Get-MsolUser cmdlet

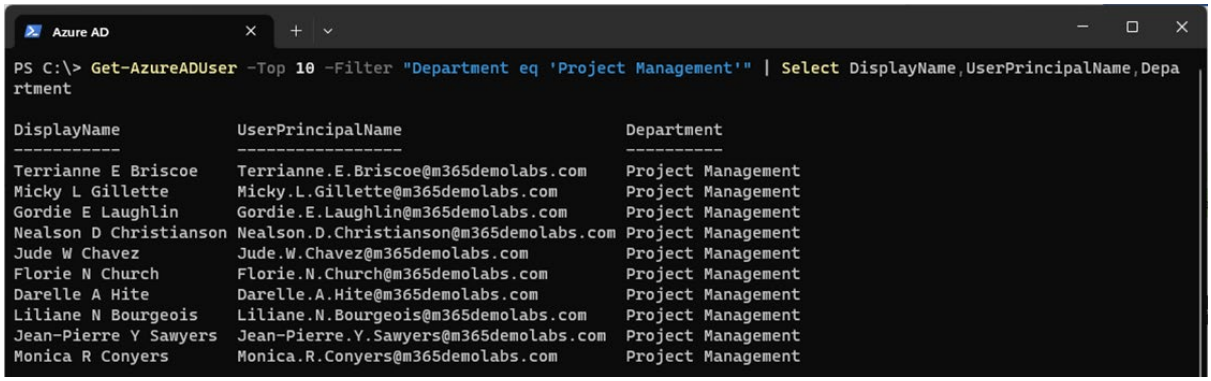

Figure 2.38 – Get-AzureADUser cmdlet

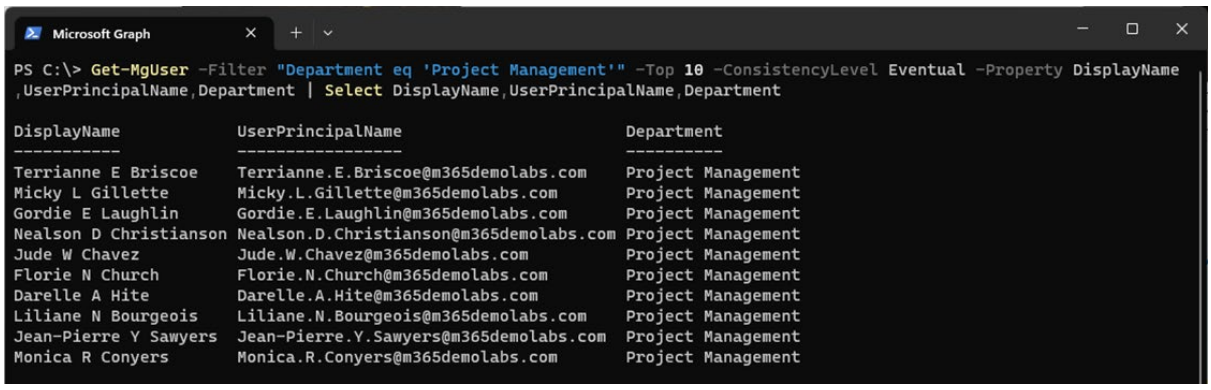

Figure 2.39 – Get-MgUser cmdlet

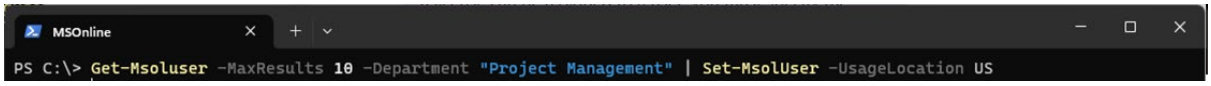

Figure 2.40 – Updating the UsageLocation with Set-MsolUser

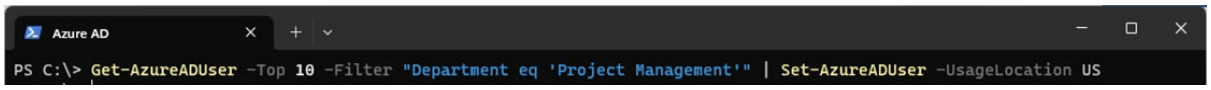

Figure 2.41 – Updating the UsageLocation with Set-AzureADUser

Figure 2.42 – Updating the UsageLocation with Update-MgUser

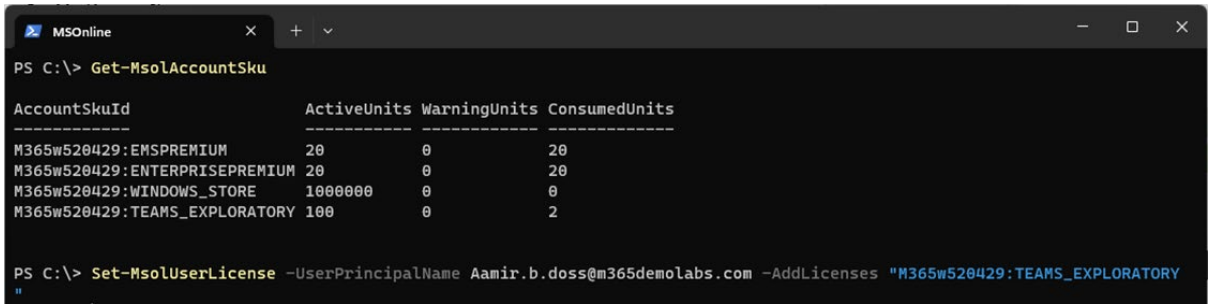

Figure 2.43 – Adding a license to a user with the MSOnline module

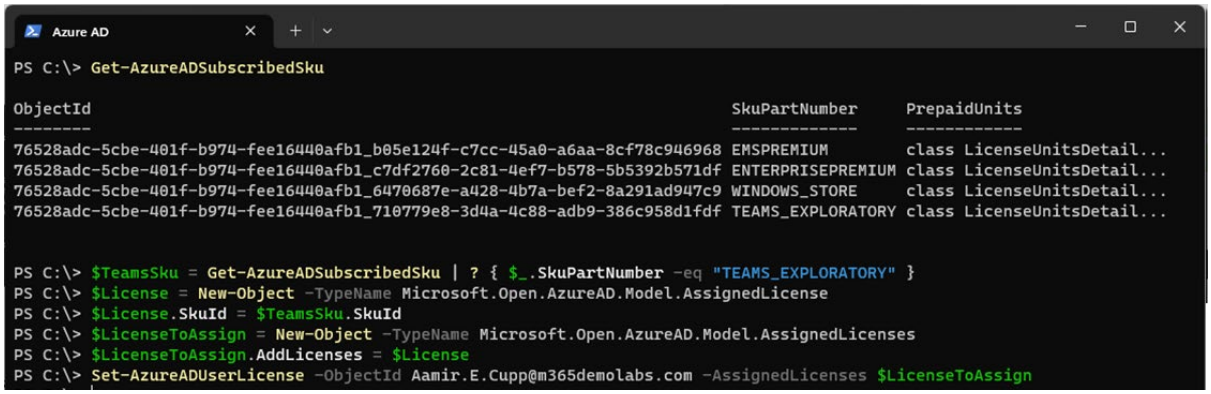

Figure 2.44 – Adding a license with the Set-AzureADUserLicense cmdlet

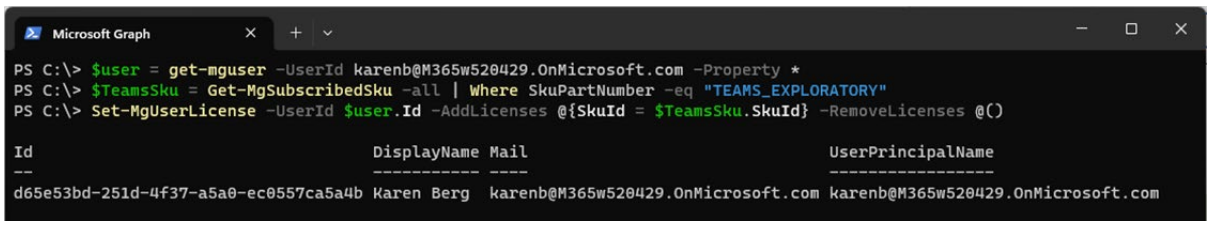

Figure 2.45 – Adding a license with the Set-MgUserLicense cmdlet

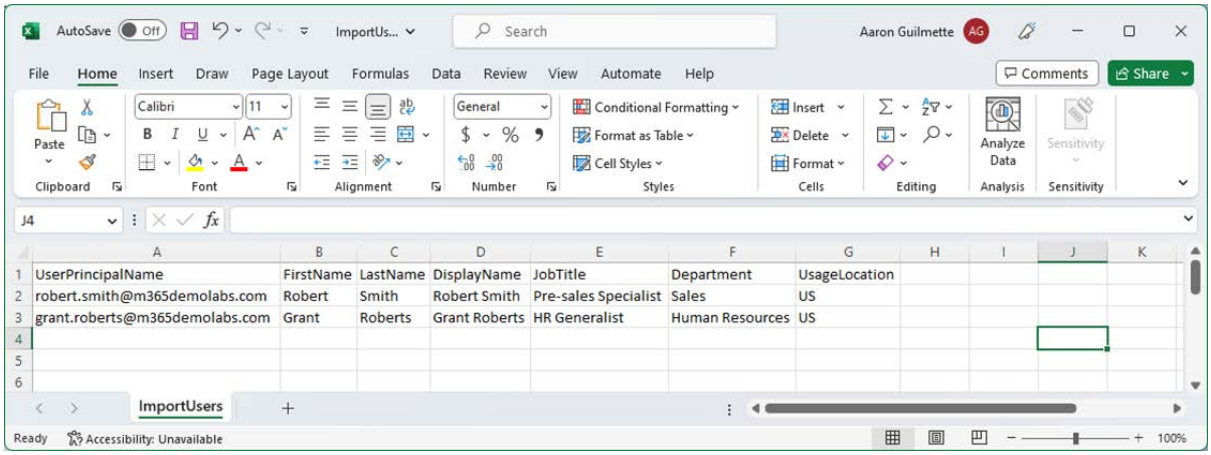

Figure 2.46 – Bulk user template

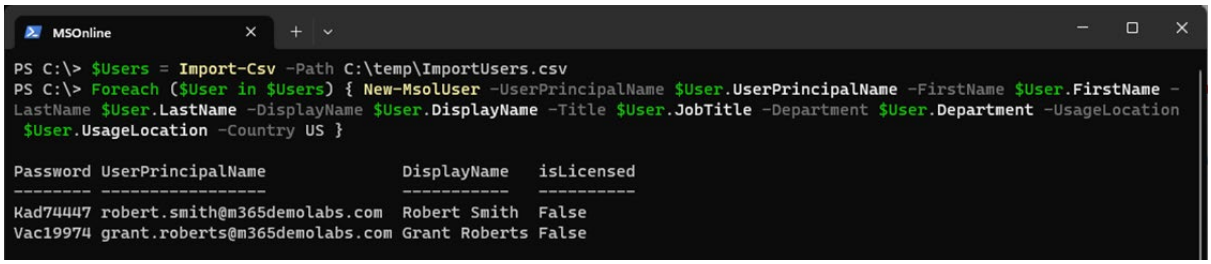

Figure 2.47 – Bulk creating users with New-MsolUser

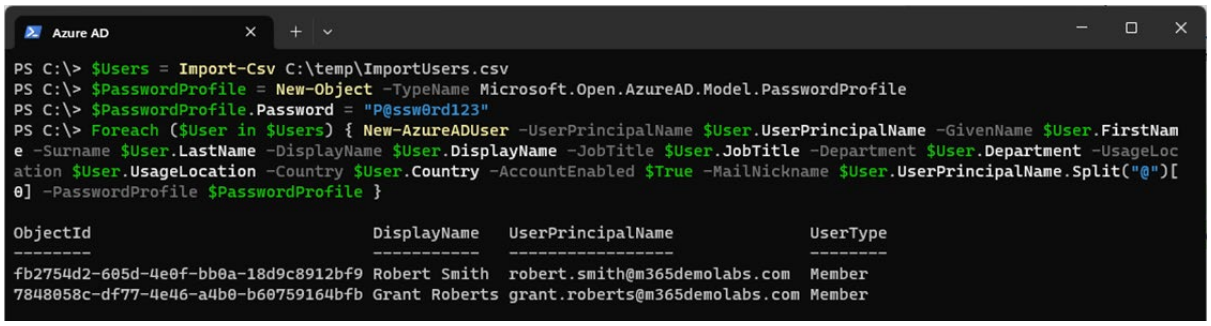

Figure 2.48 – Creating new users with New-AzureADUser

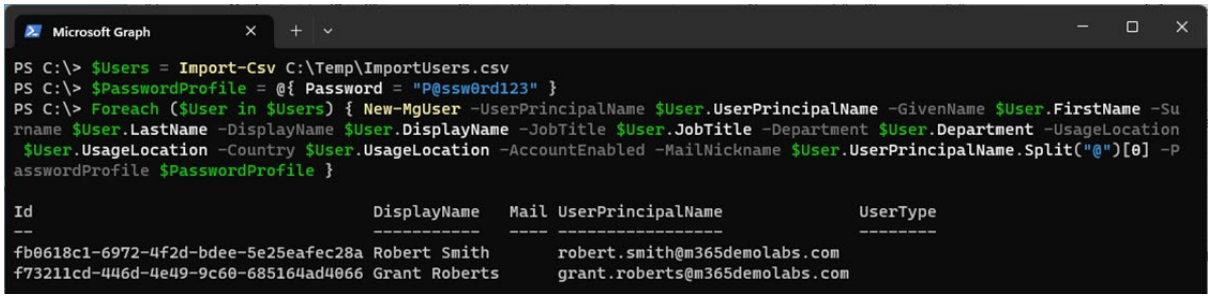

Figure 2.49 – Creating new users with the New-MgUser cmdlet

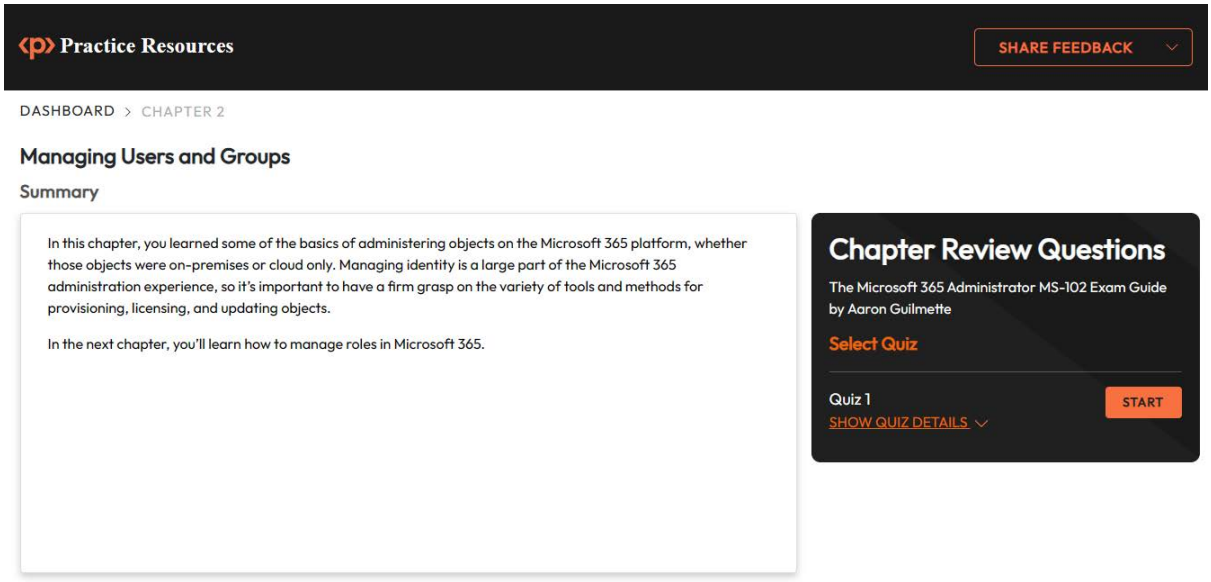

Figure 2.50 – Chapter Review Questions for Chapter 2

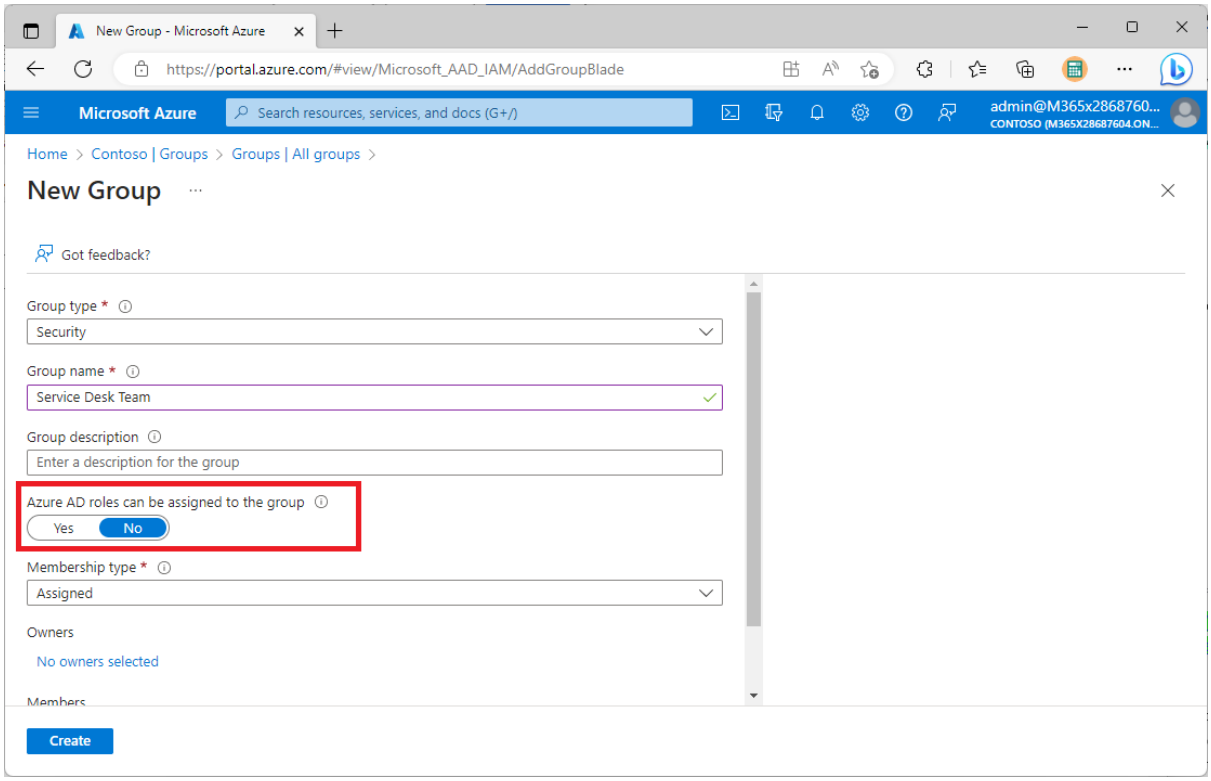

Figure 3.1 – Configuring the isAssignableToRole property on a new group

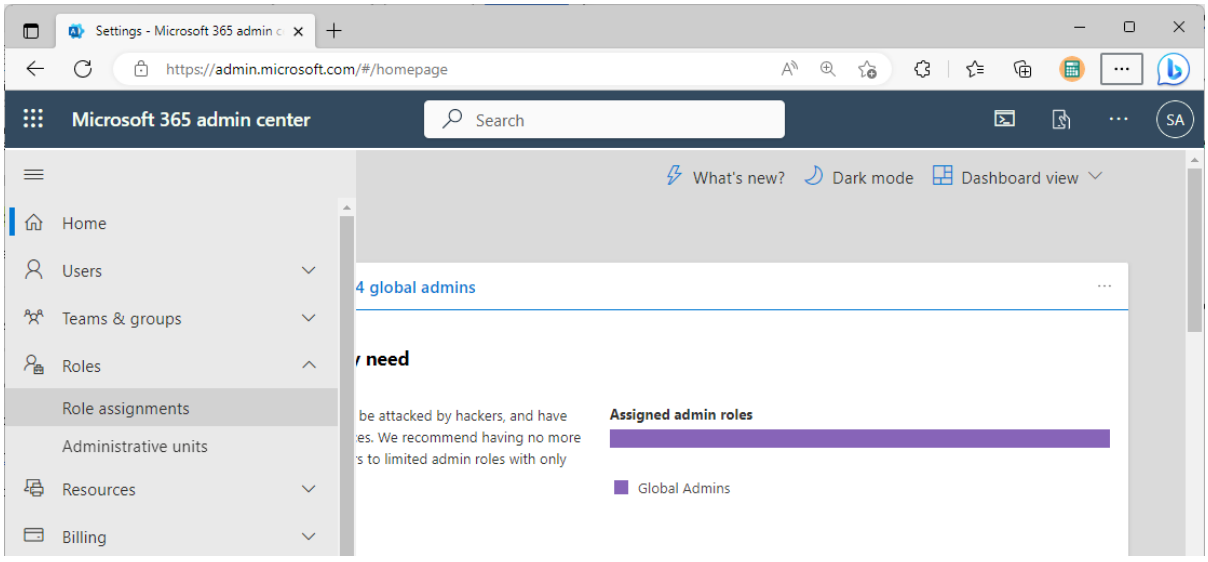

Figure 3.2 – Role assignments

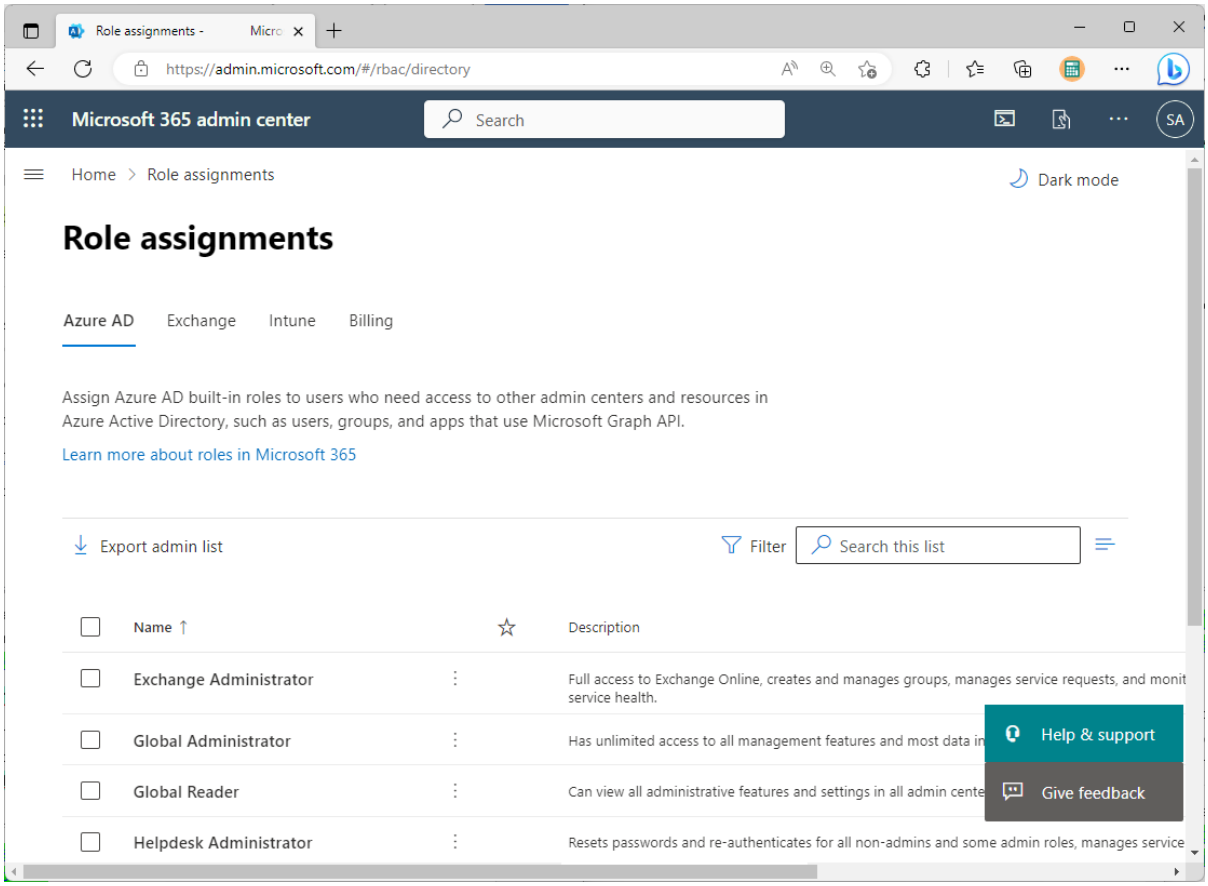

Figure 3.3 – Role assignments page

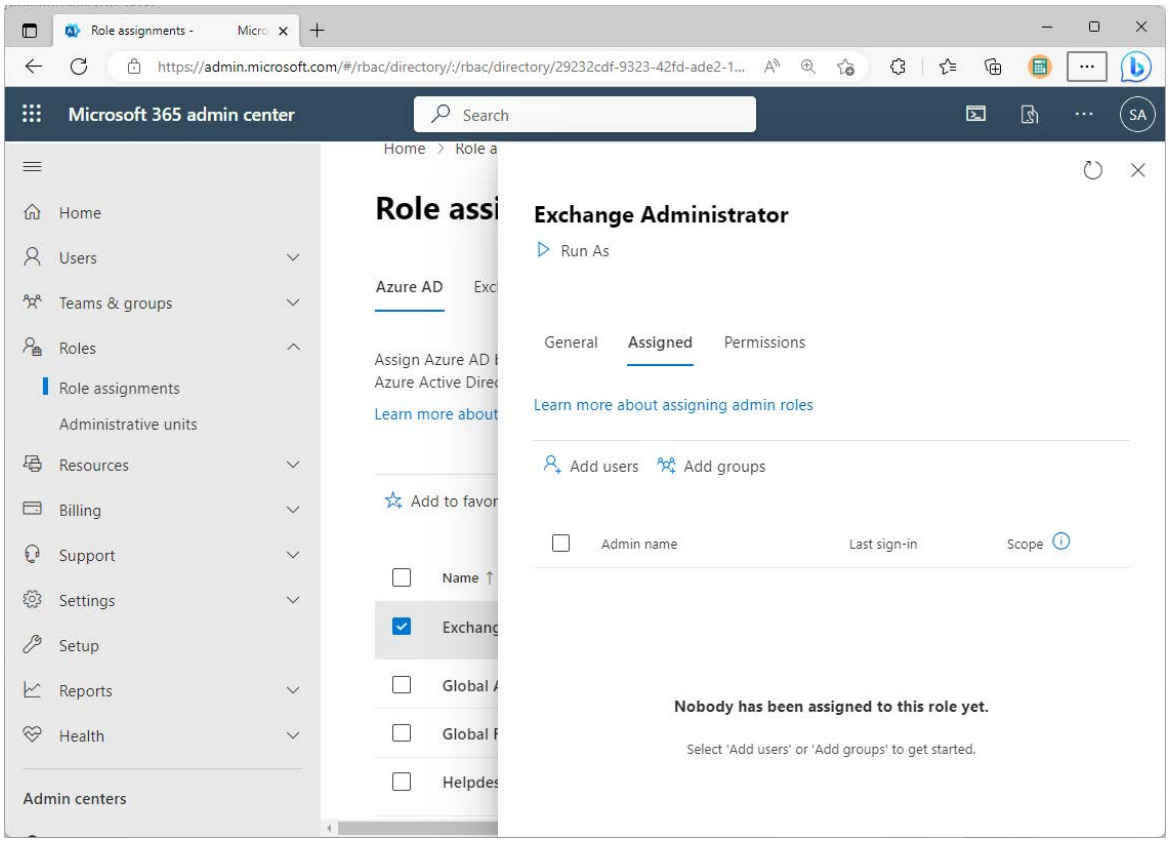

Figure 3.4 – Making role assignments

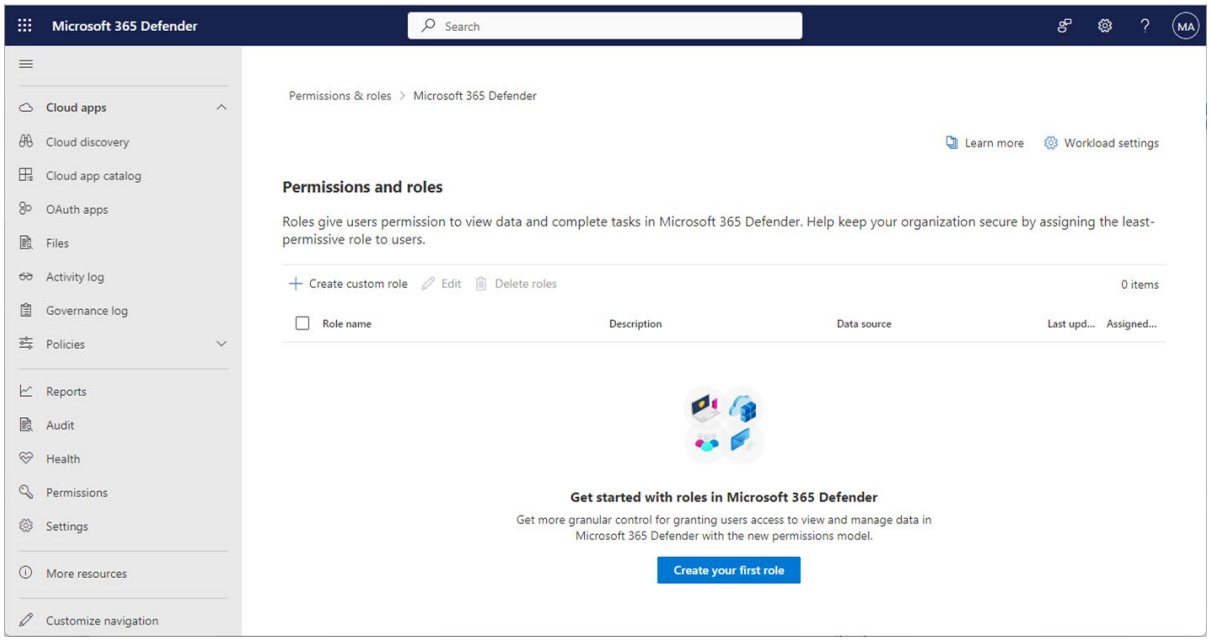

Figure 3.5 – Microsoft 365 Defender permissions

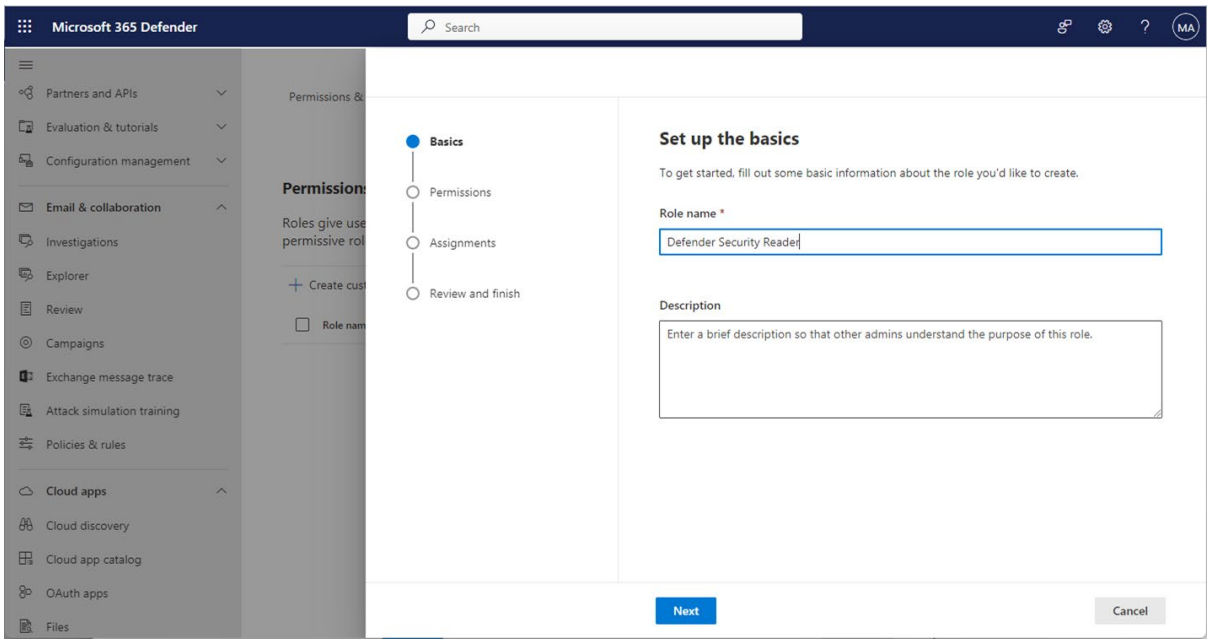

Figure 3.6 – Creating a new custom role

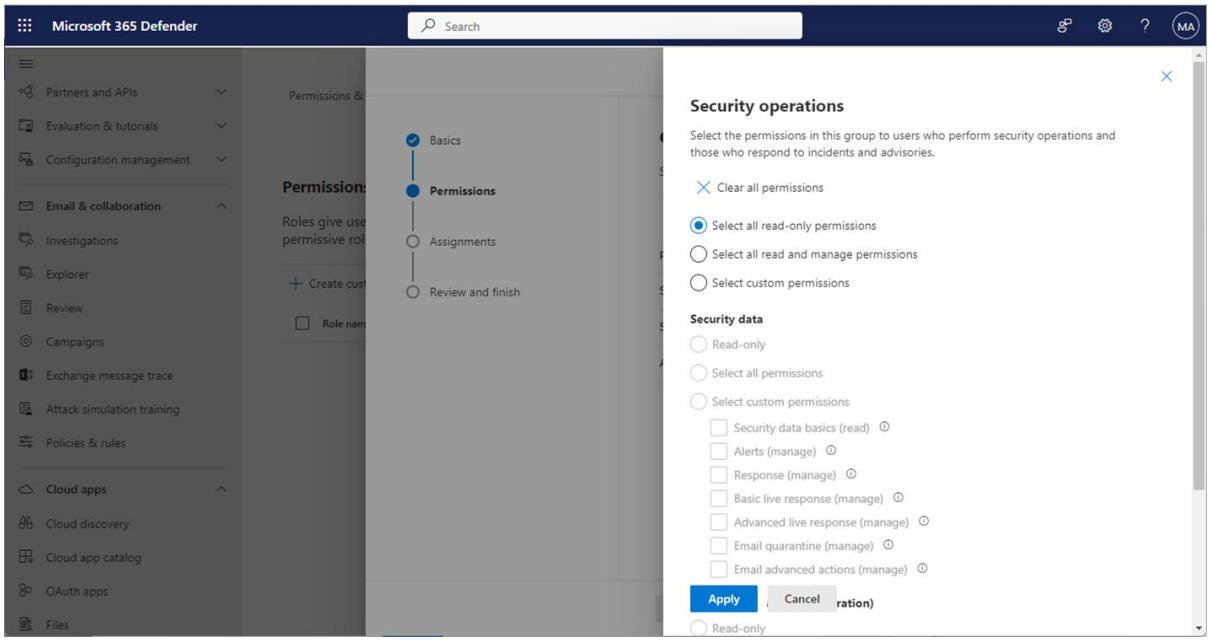

Figure 3.7 – Selecting permissions

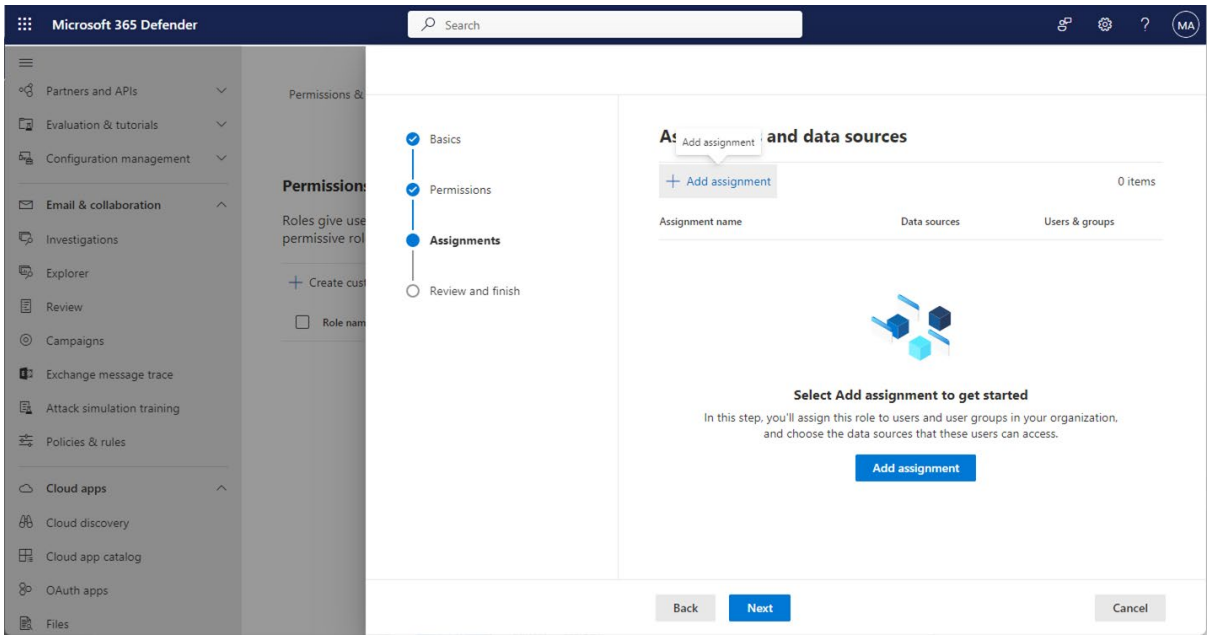

Figure 3.8 – Adding user and data assignments

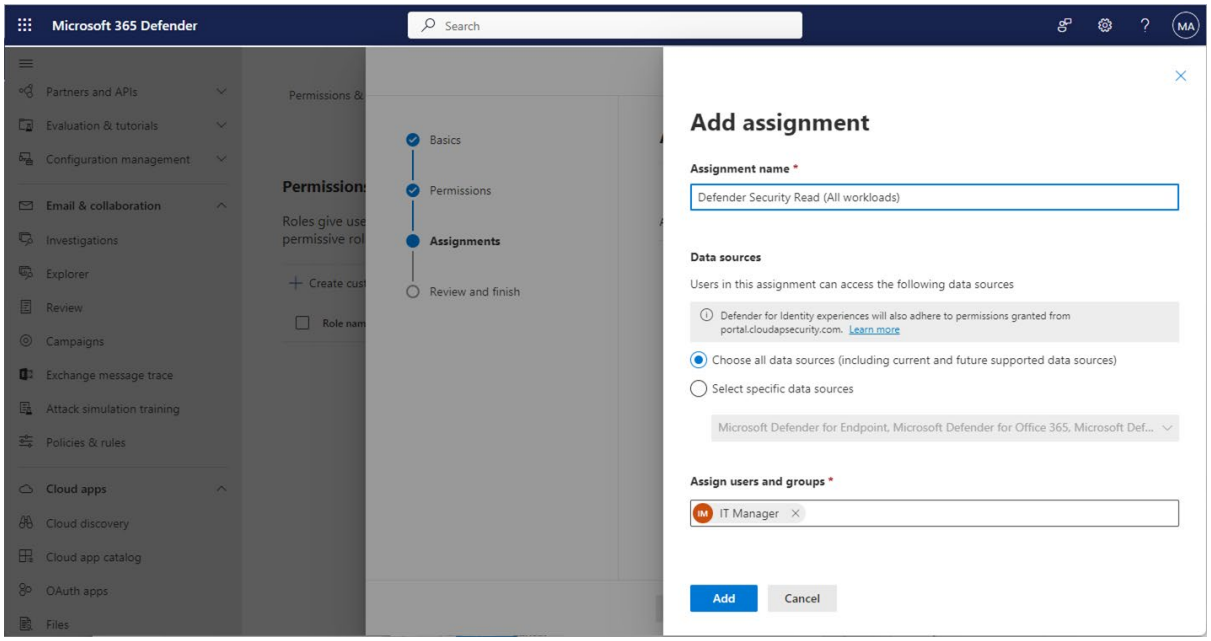

Figure 3.9 – Selecting assignment options

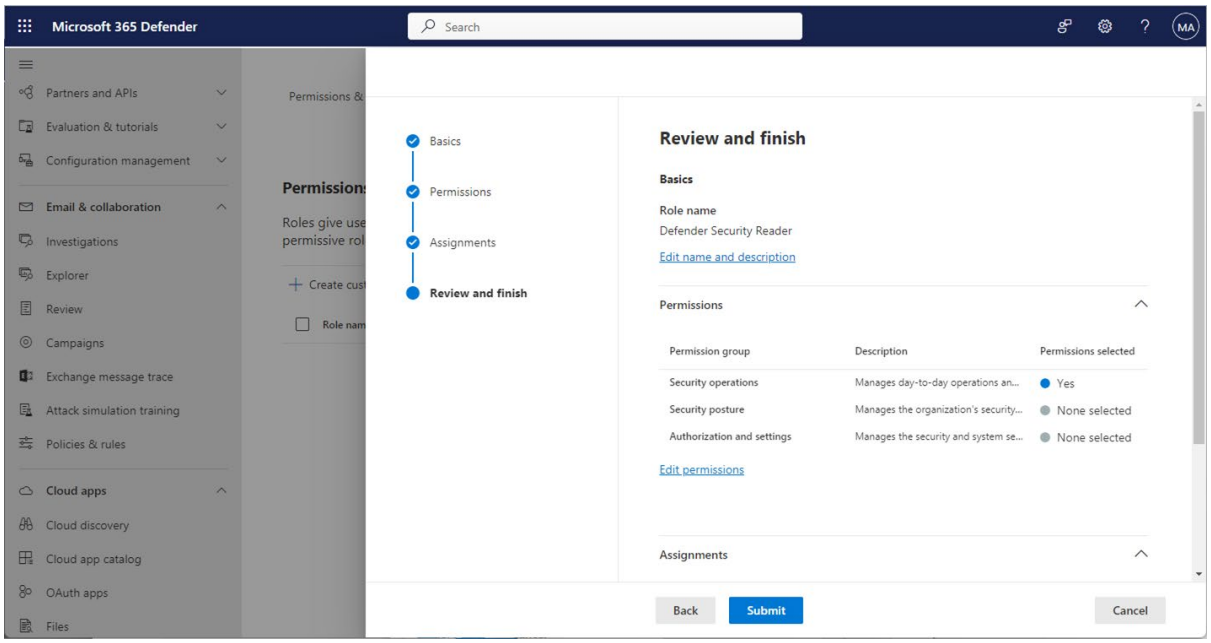

Figure 3.10 – Confirming configuration

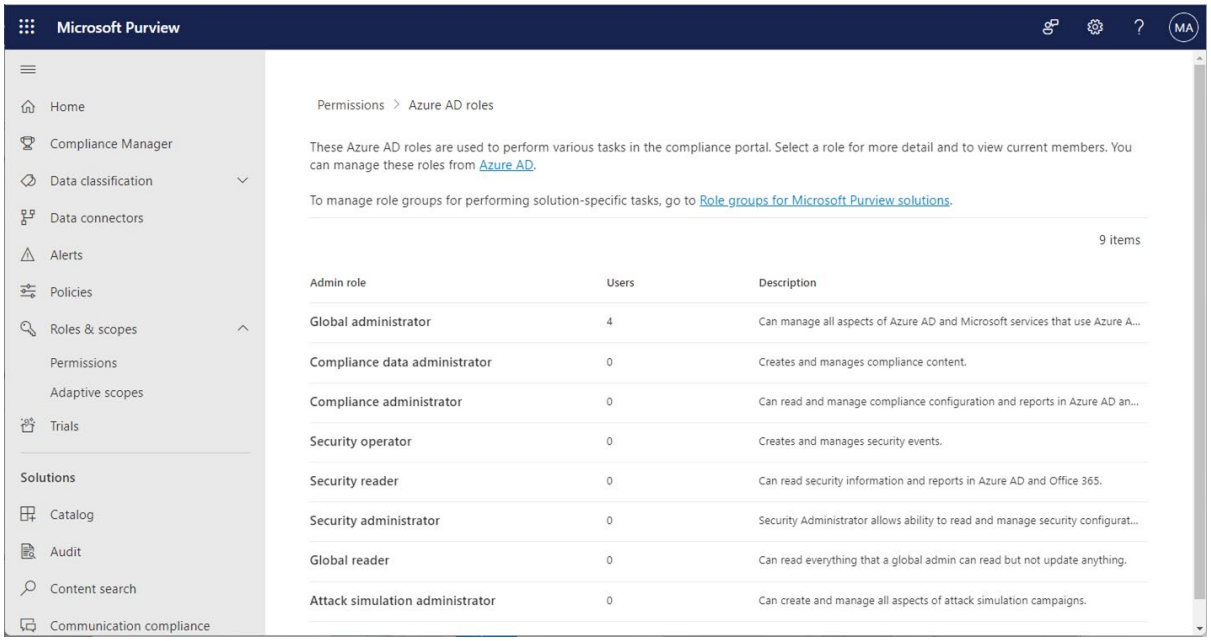

Figure 3.11 – Viewing the Azure AD roles in the Microsoft 365 admin center

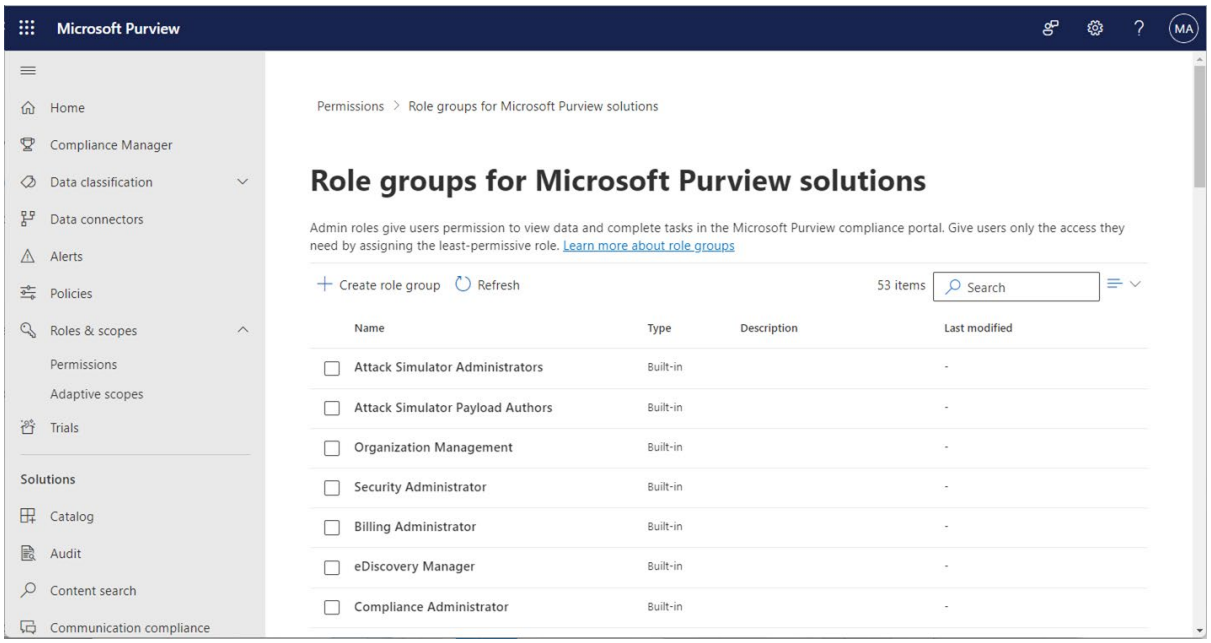

Figure 3.12 – Microsoft Purview solutions roles

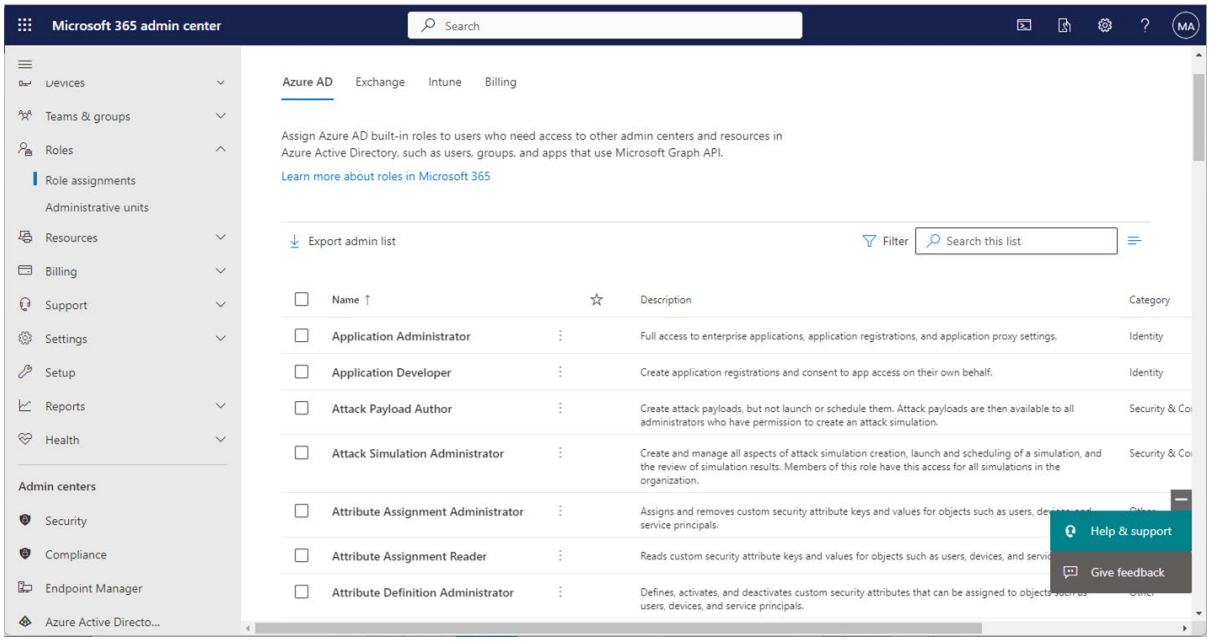

Figure 3.13 – Microsoft 365 workload roles

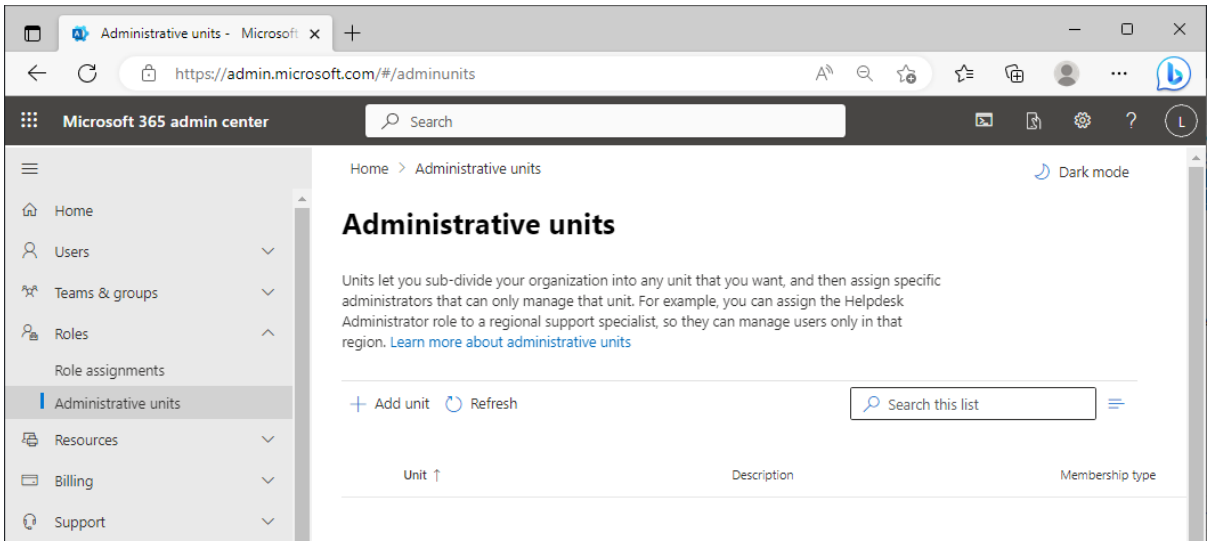

Figure 3.14 – Administrative units page

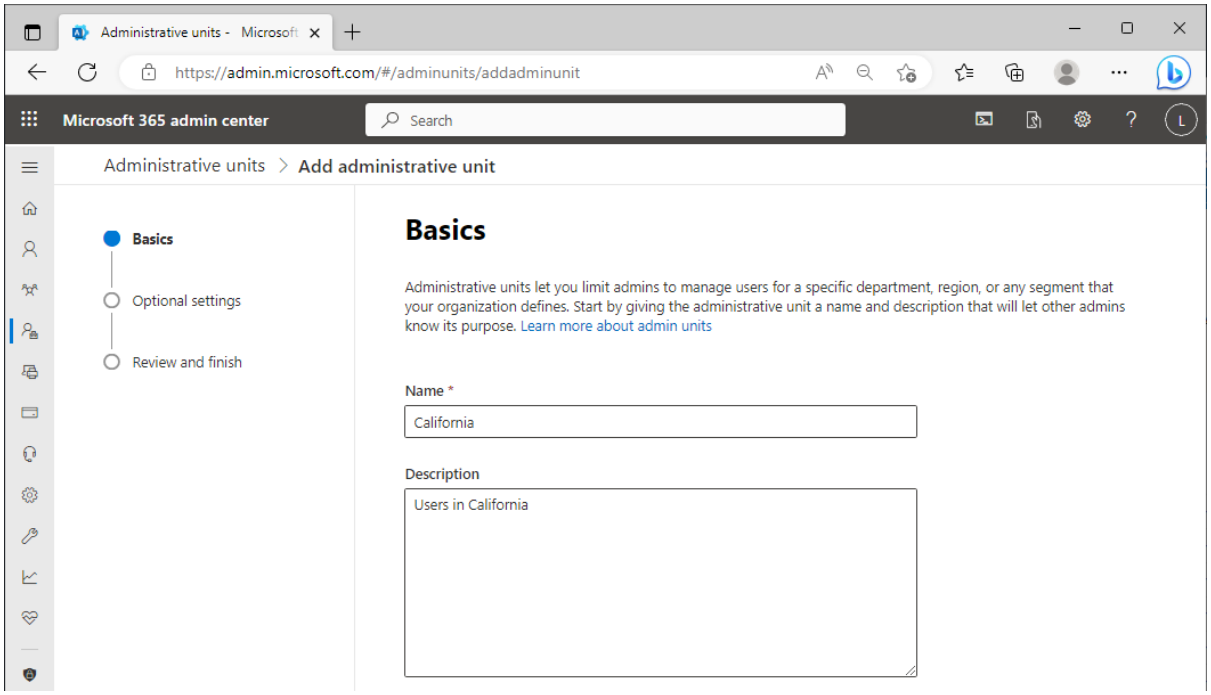

Figure 3.15 – Basics page

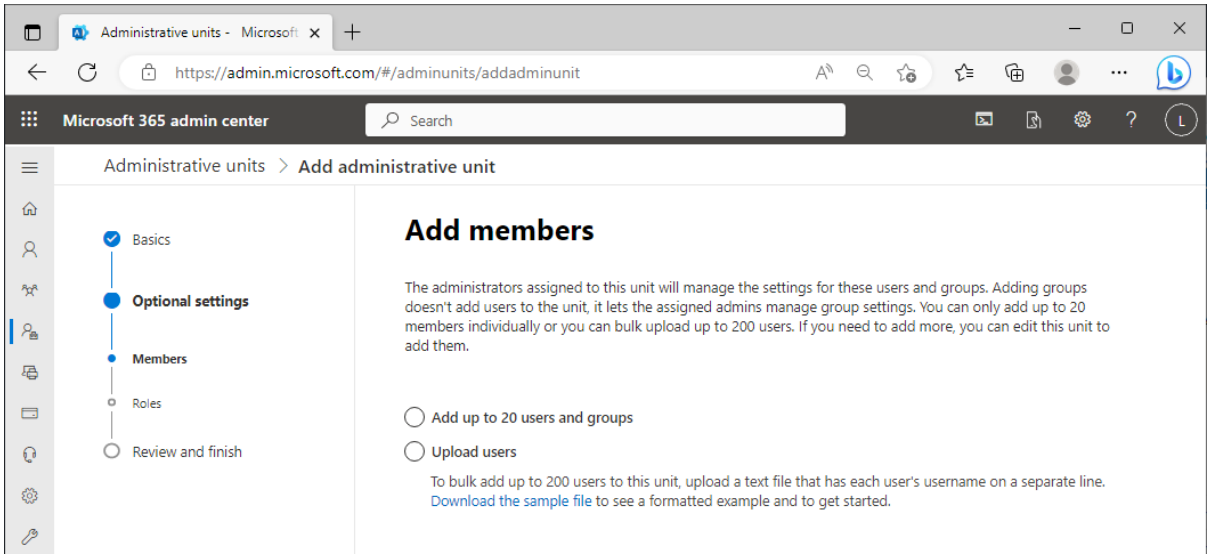

Figure 3.16 – Add members page

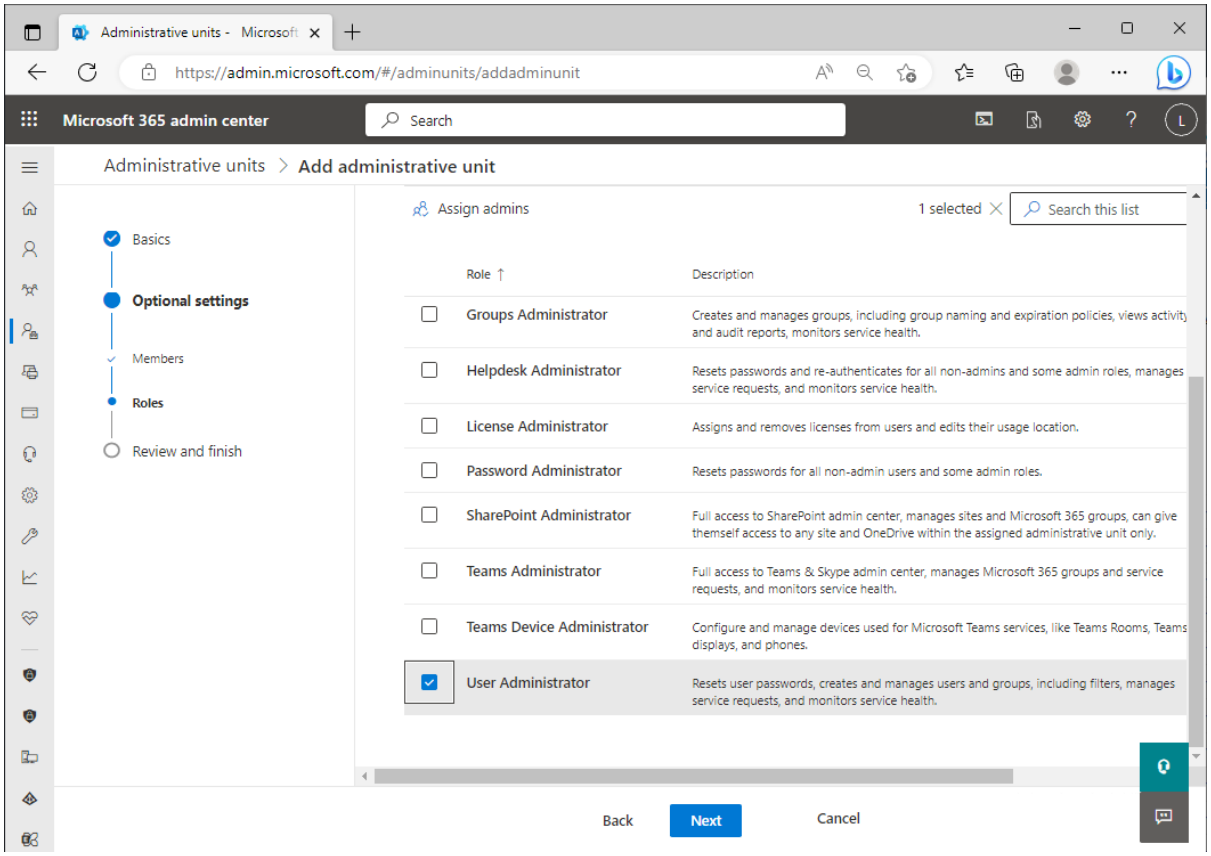

Figure 3.17 – Adding roles

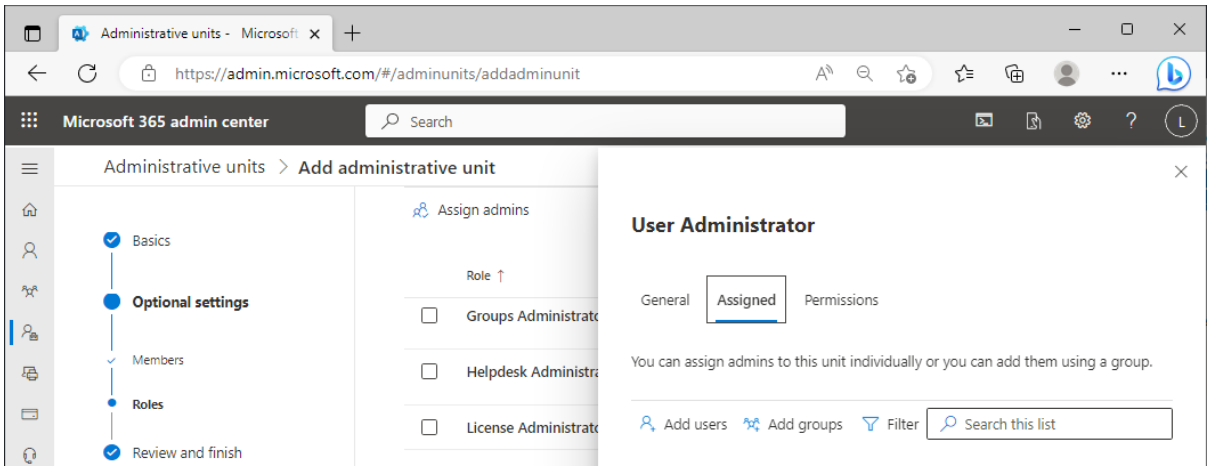

Figure 3.18 – User Administrator flyout

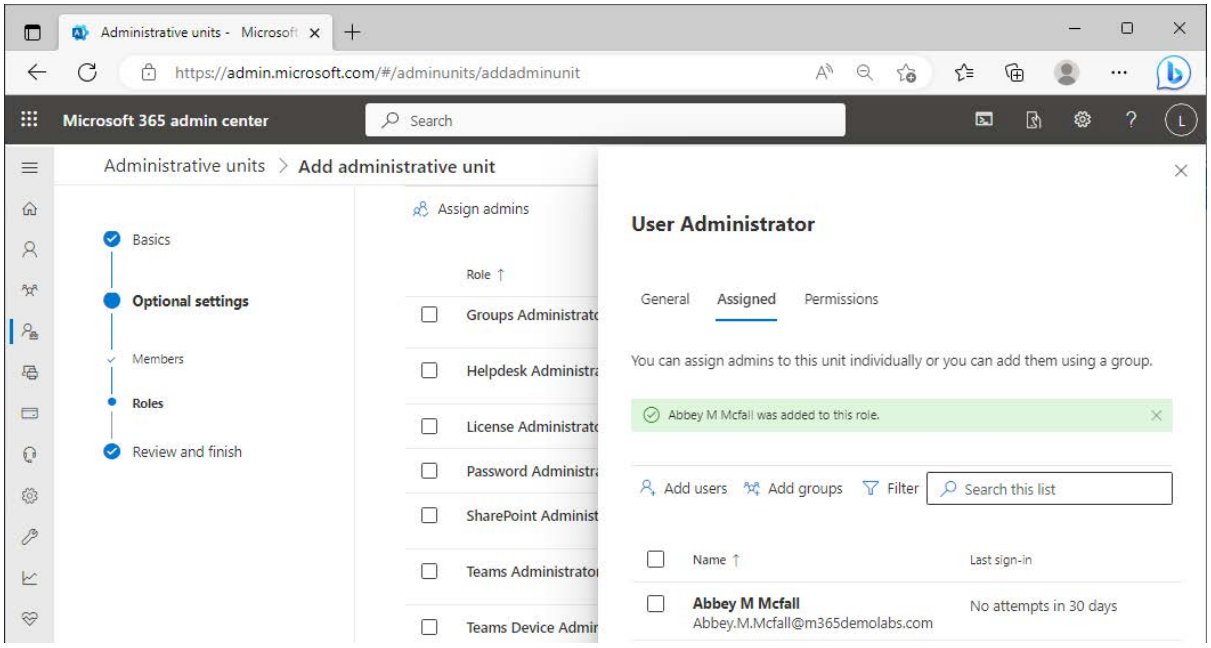

Figure 3.19 – Adding users to role

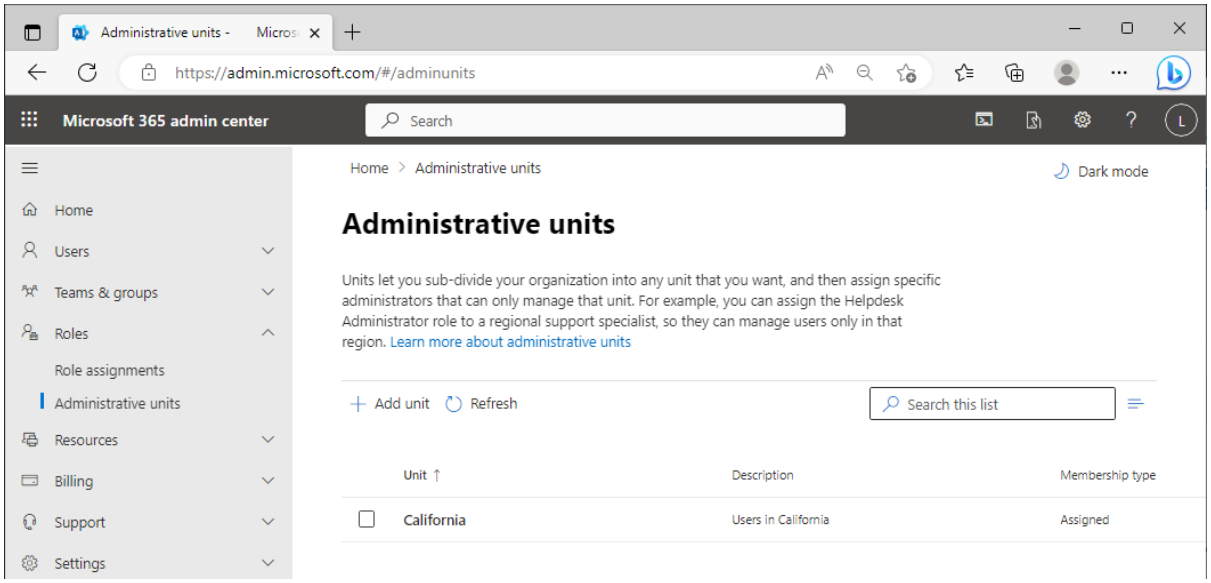

Figure 3.20 – Viewing administrative units

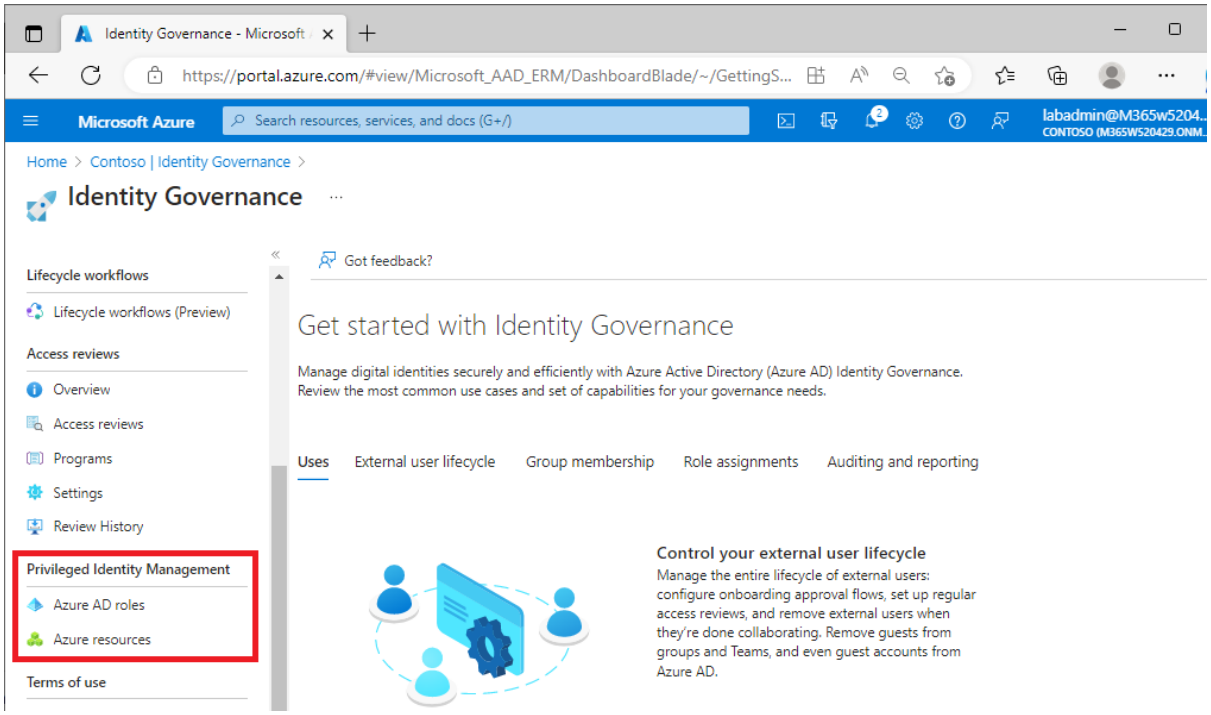

Figure 3.21 – Privileged Identity Management

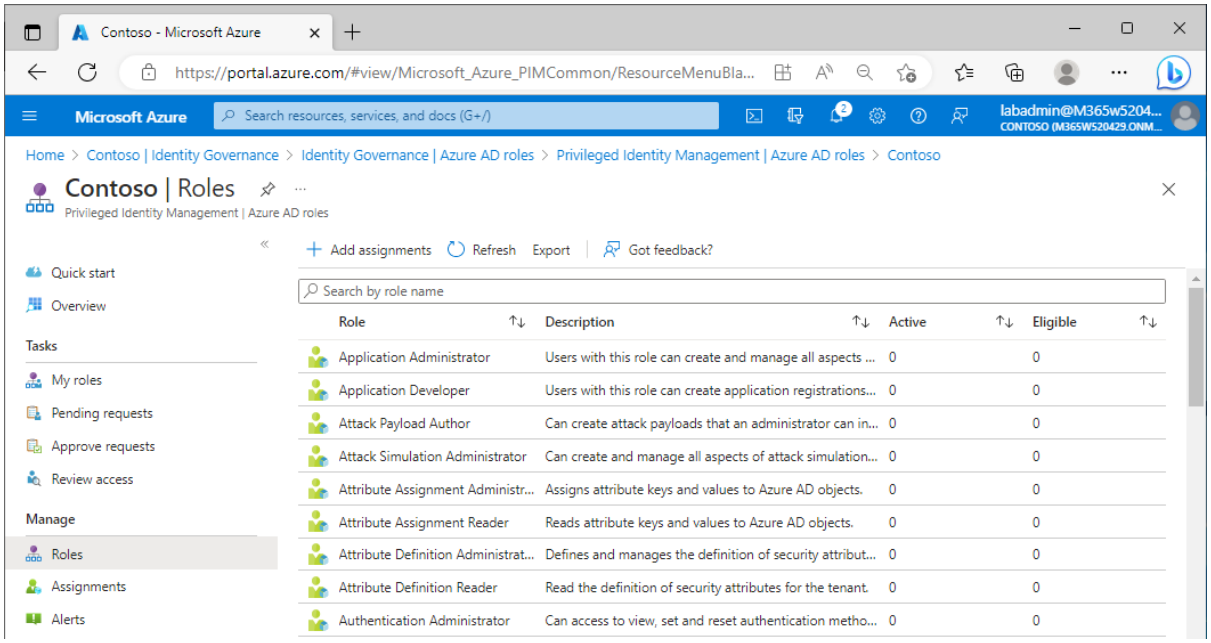

Figure 3.22 – Role assignments

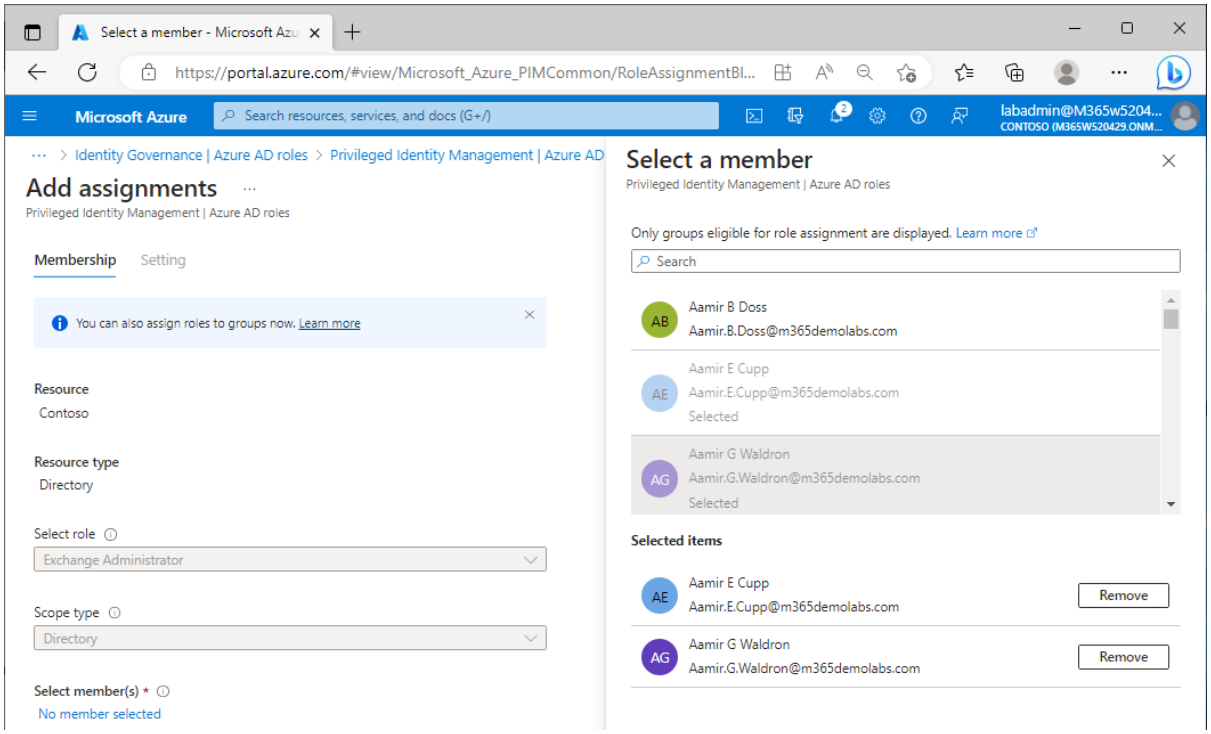

Figure 3.23 – Selecting members

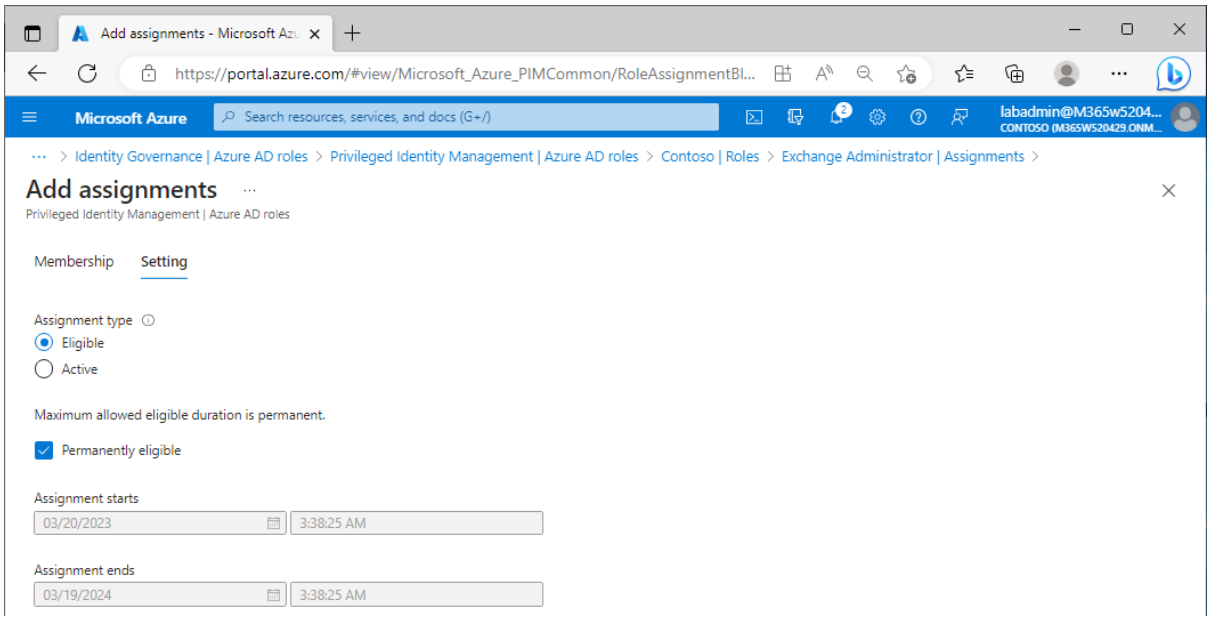

Figure 3.24 – Configuring assignment type and eligibility duration

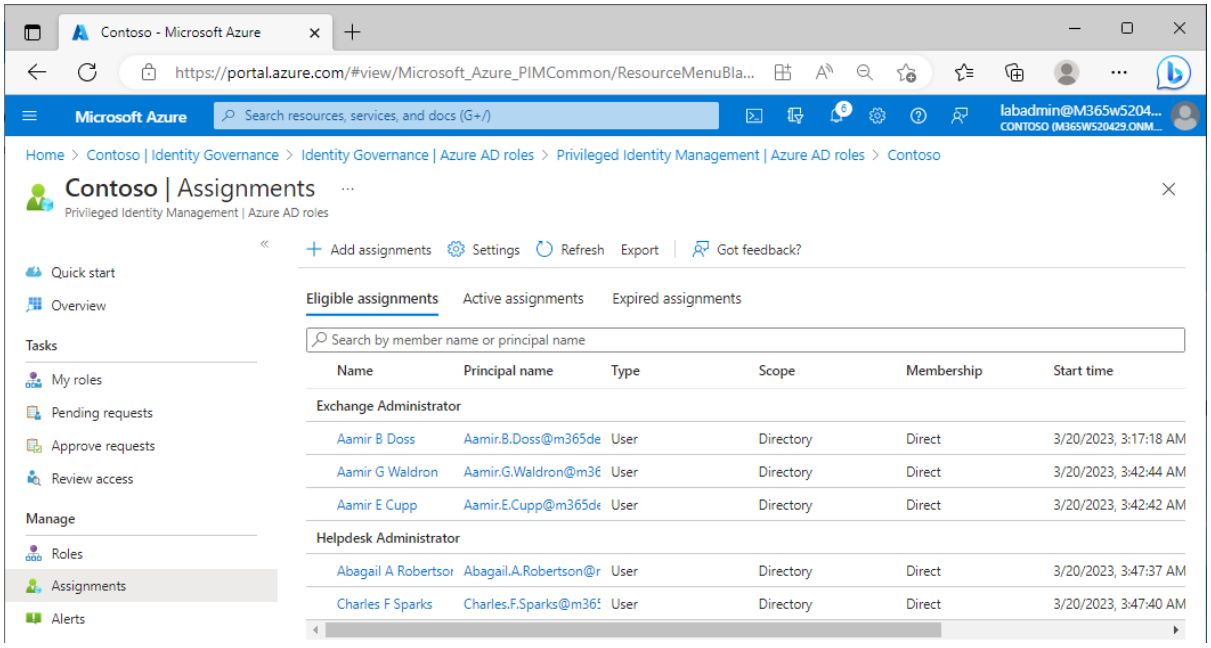

Figure 3.25 – Viewing role assignments

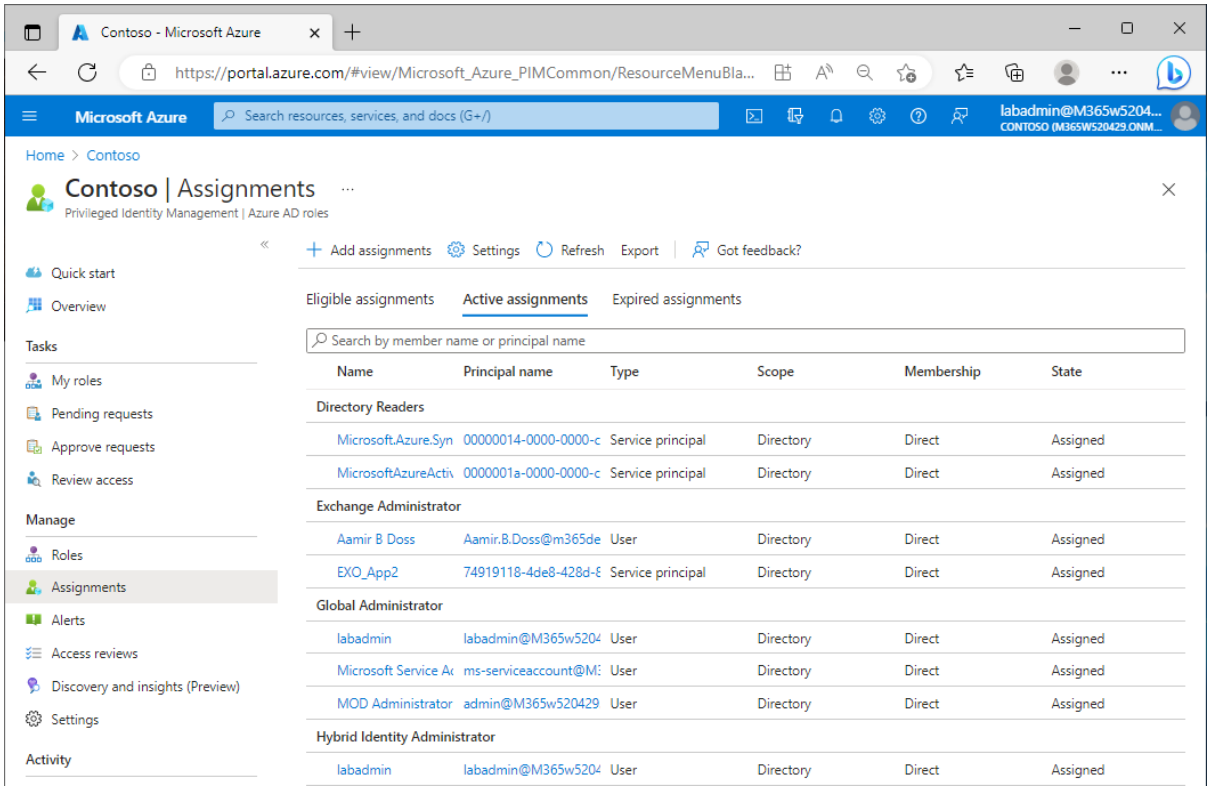

Figure 3.26 – Viewing active assignments

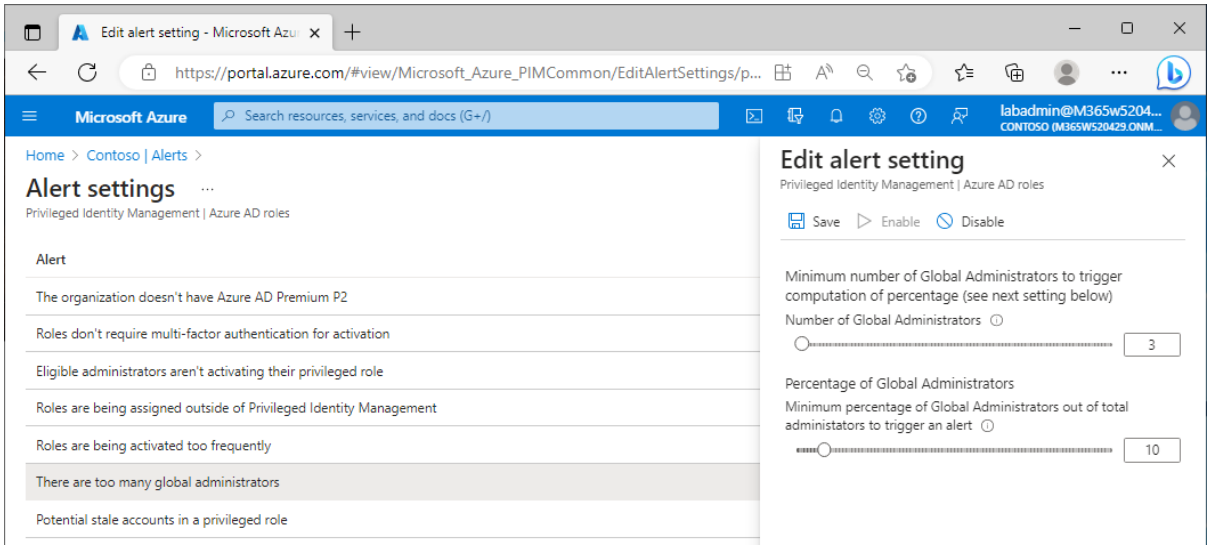

Figure 3.27 – Viewing PIM Alert settings

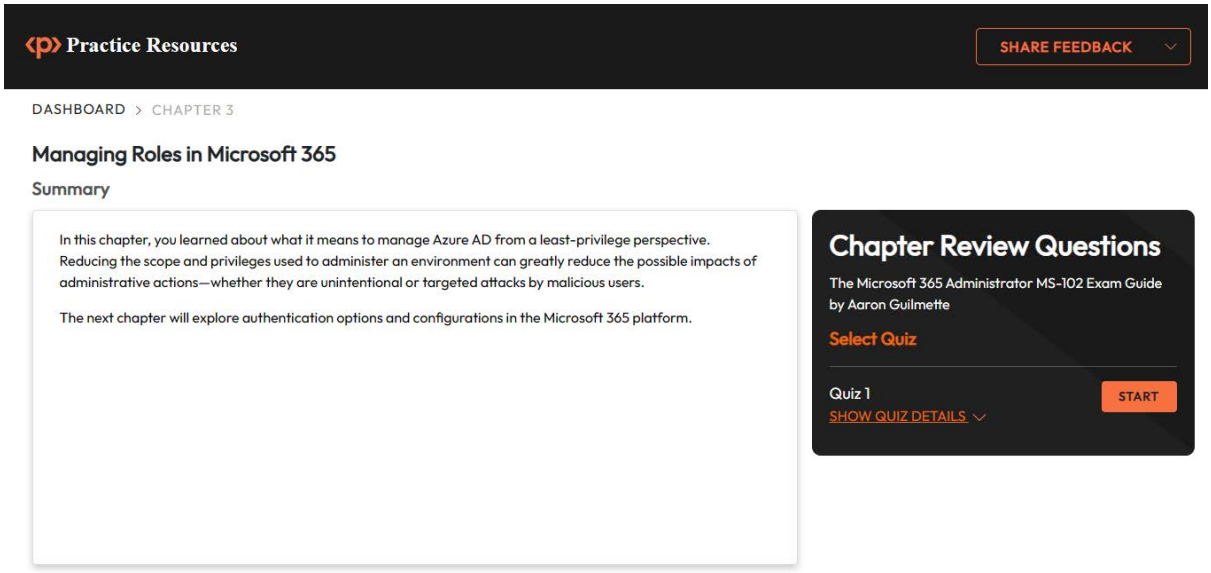

Figure 3.28 – Chapter Review Questions for Chapter 3

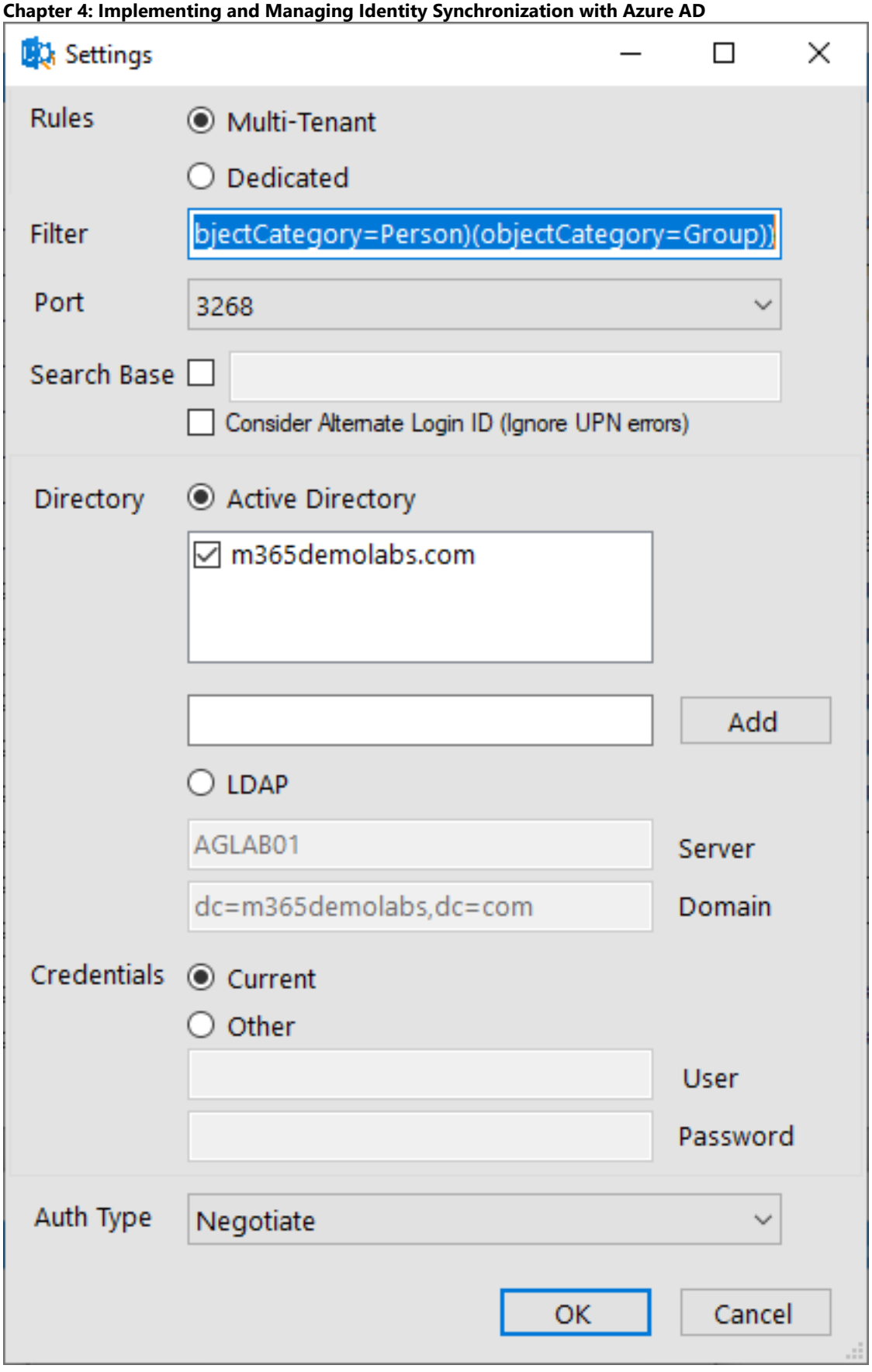

Figure 4.1 – IdFix Settings

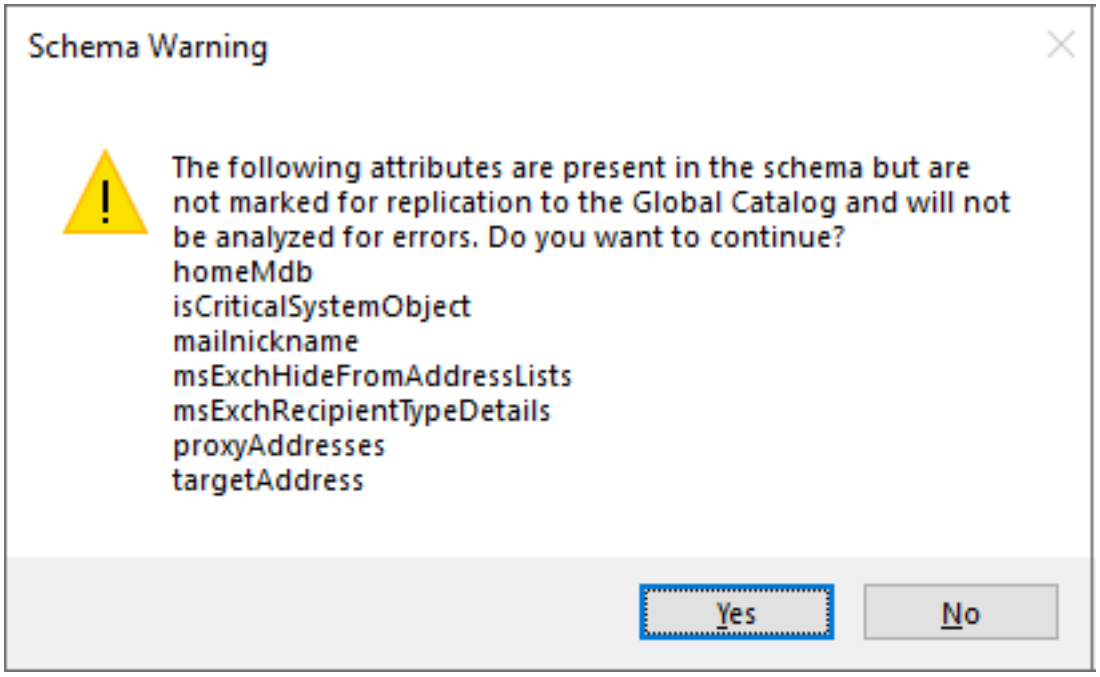

Figure 4.2 – IdFix schema warning

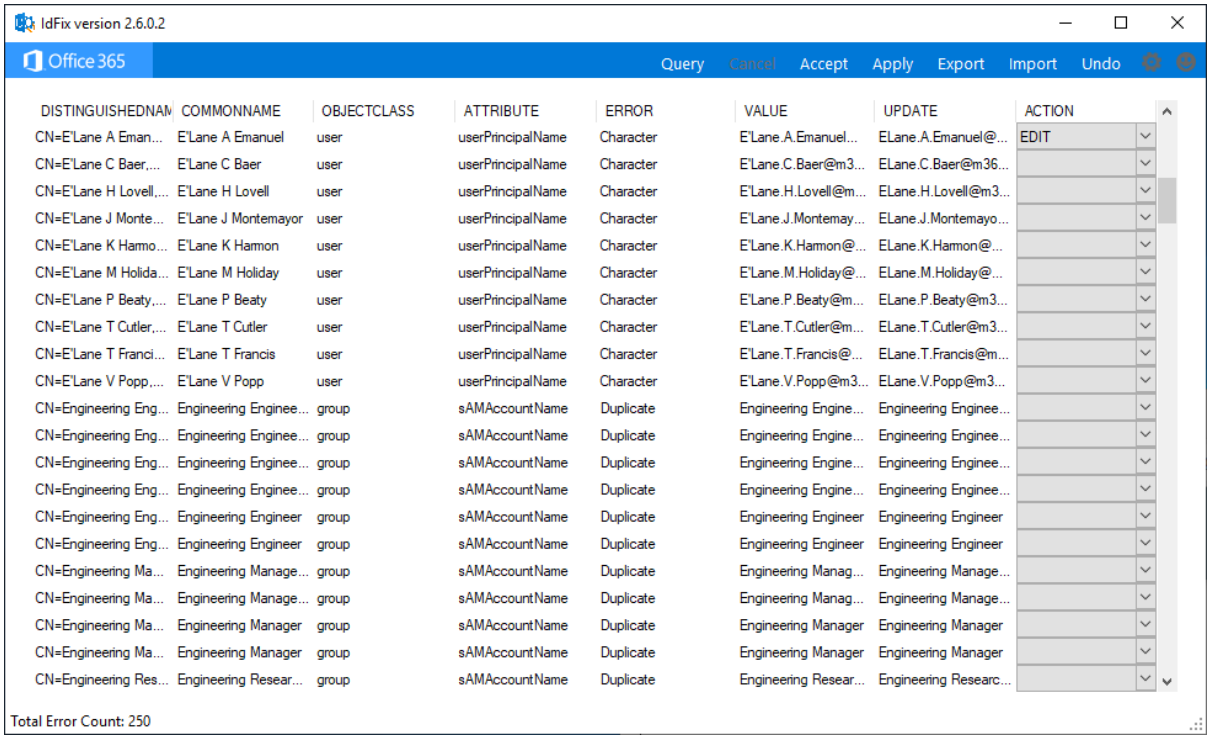

Figure 4.3 – IdFix data grid

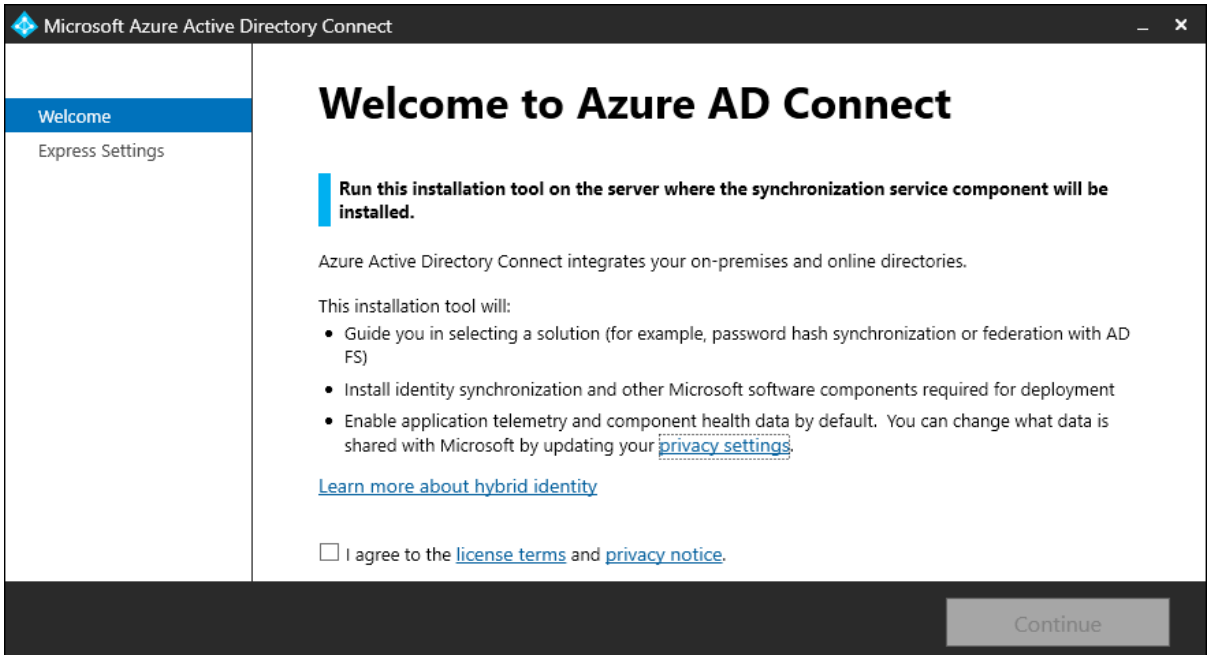

Figure 4.4 – Azure AD Connect welcome page

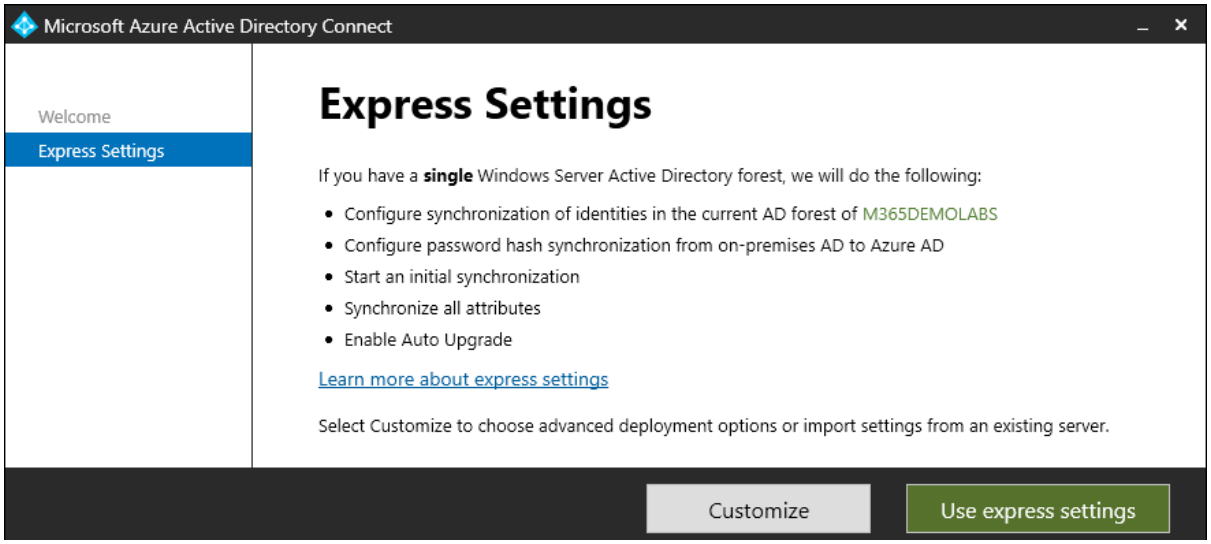

Figure 4.5 – Azure AD Connect Express Settings page

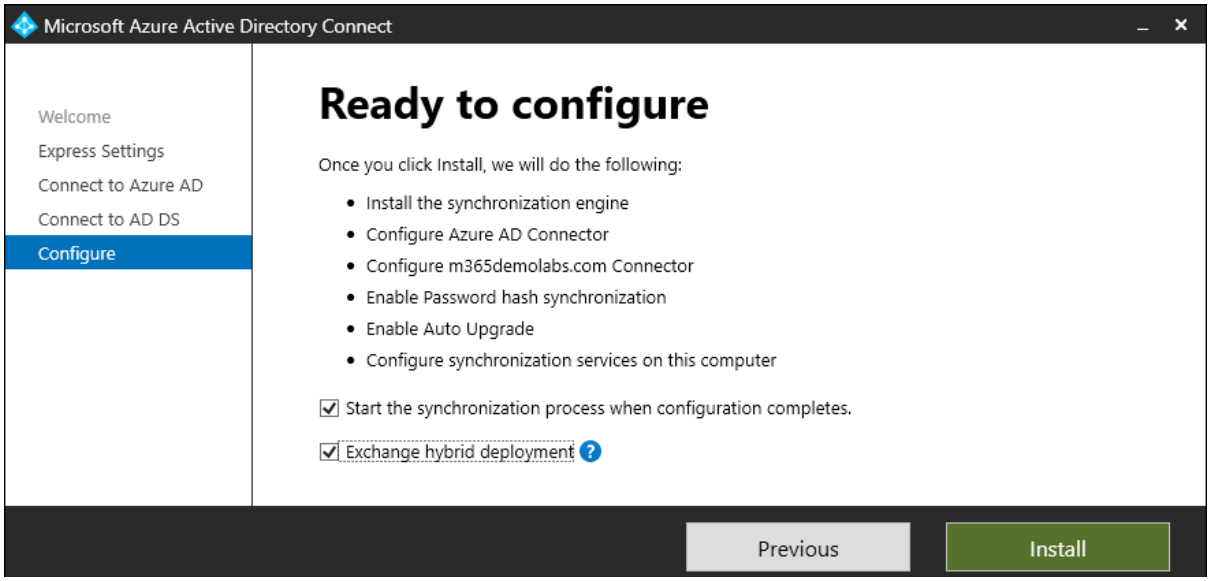

Figure 4.6 – Azure AD Connect Ready to configure page

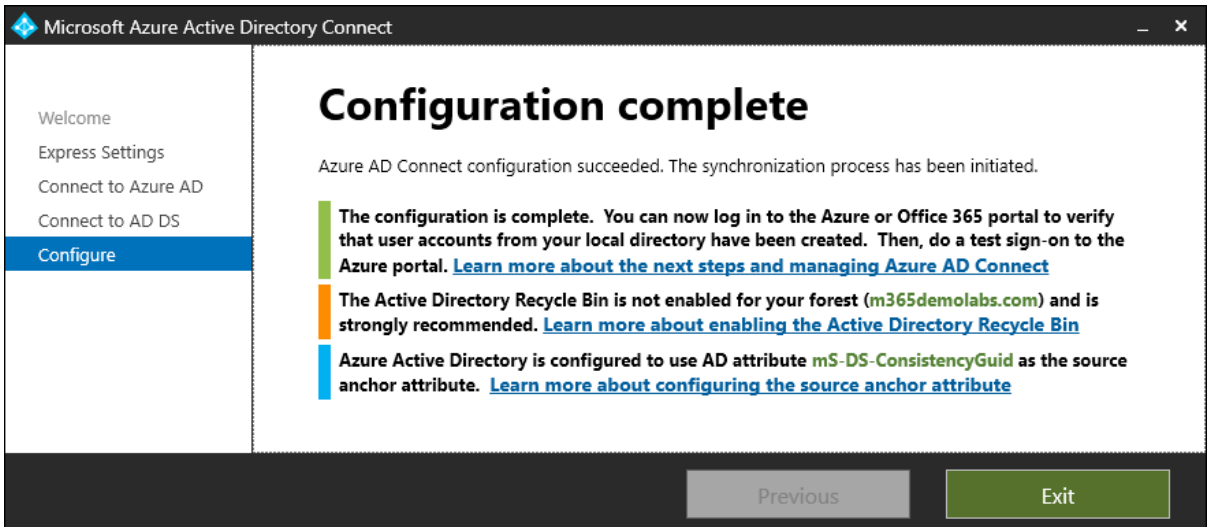

Figure 4.7 – Azure AD Connect Configuration complete page

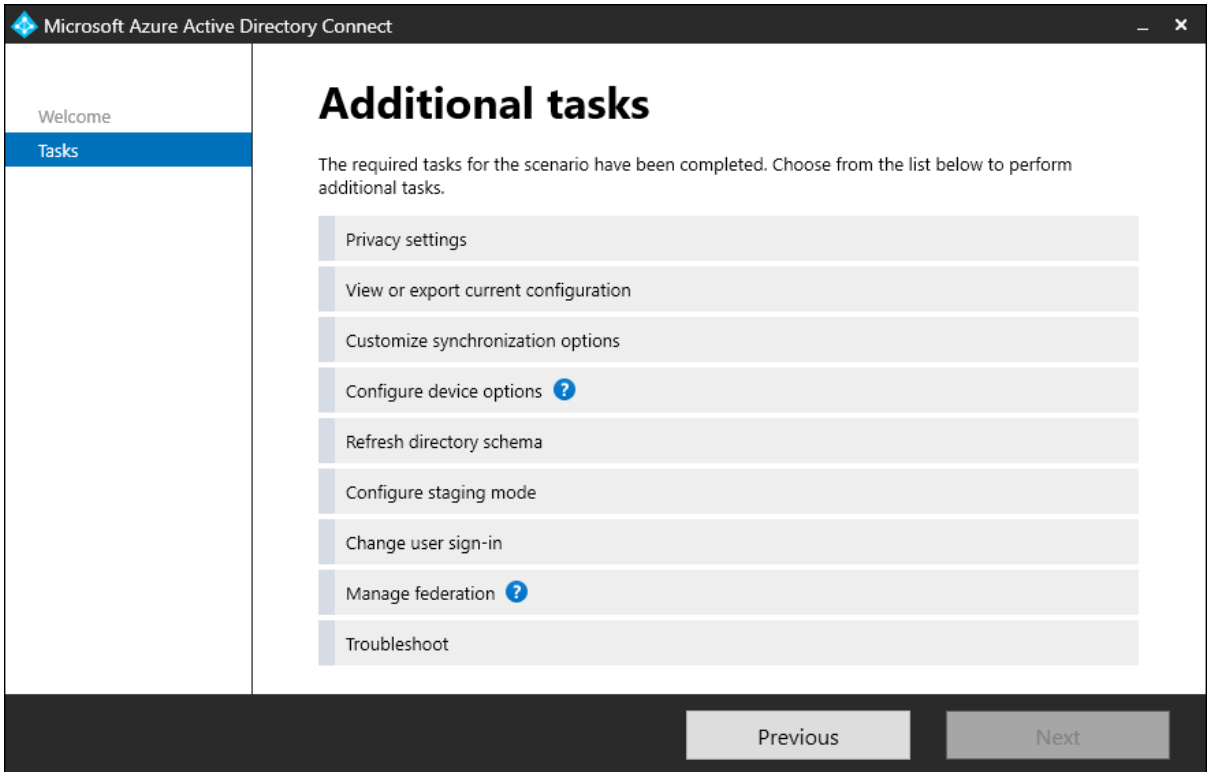

Figure 4.8 – Additional tasks page

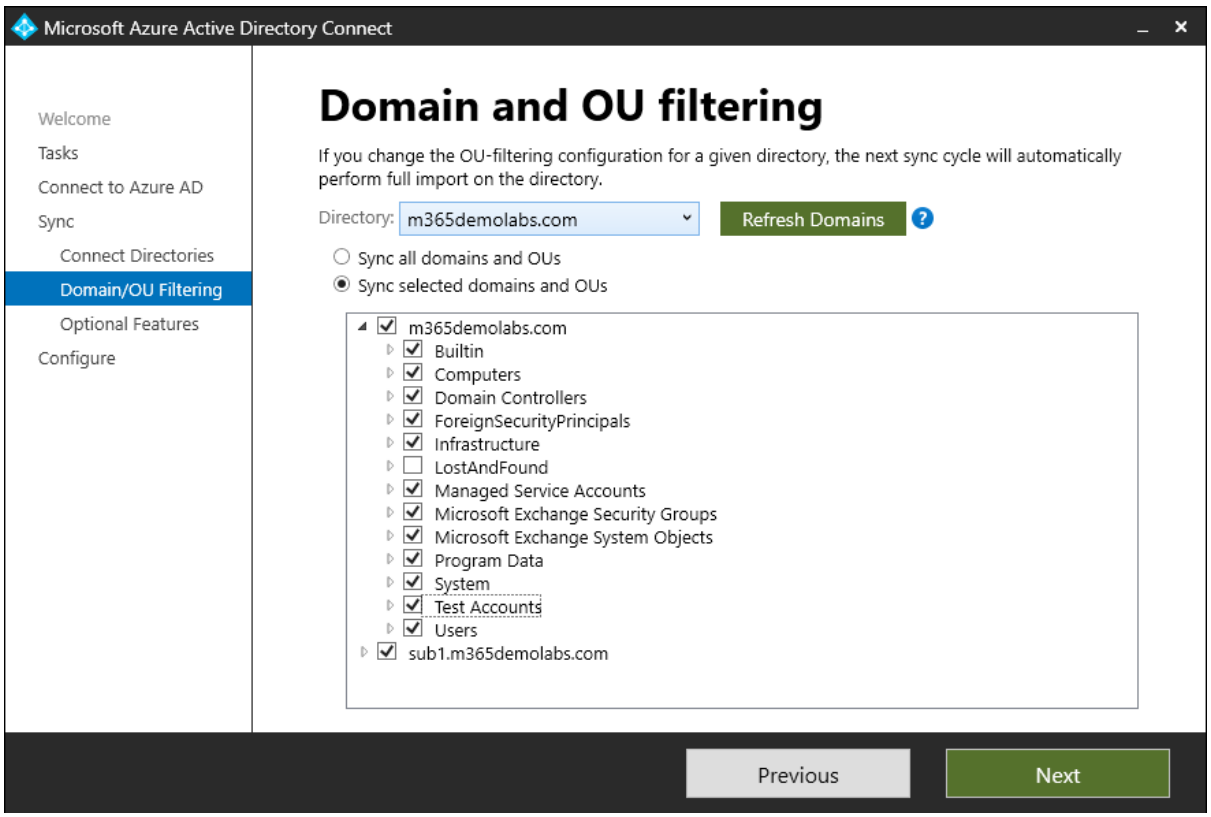

Figure 4.9 – Azure AD Connect Domain and OU filtering page

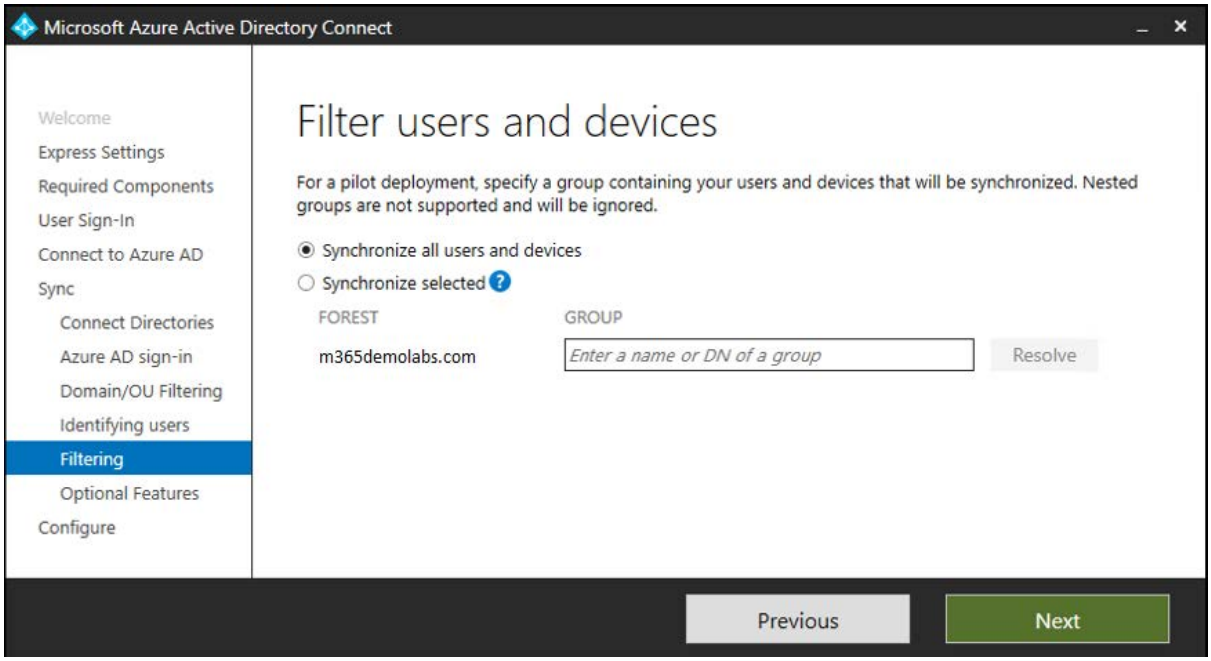

Figure 4.10 – Filter users and devices page

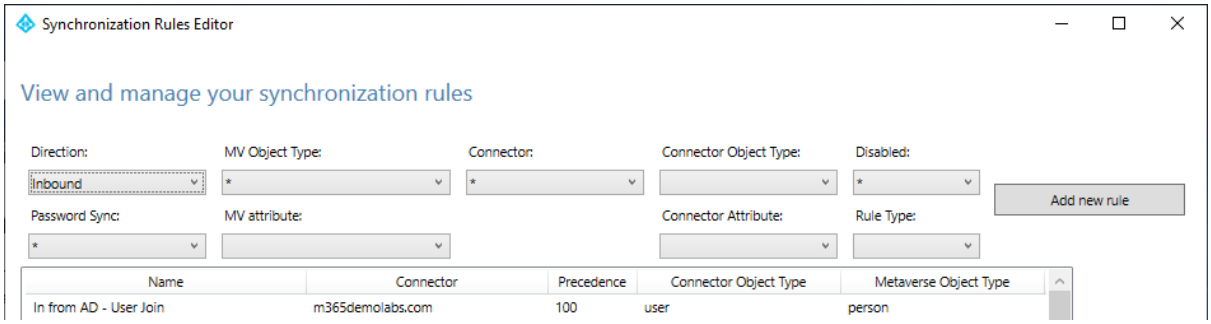

Figure 4.11 – Synchronization rules editor

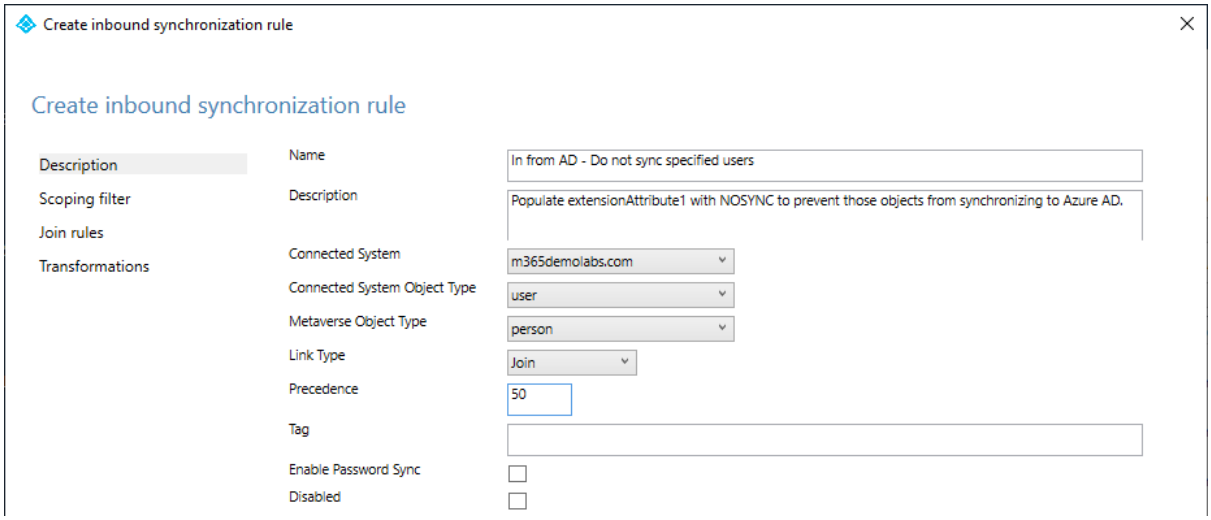

Figure 4.12 – Creating a new inbound synchronization rule

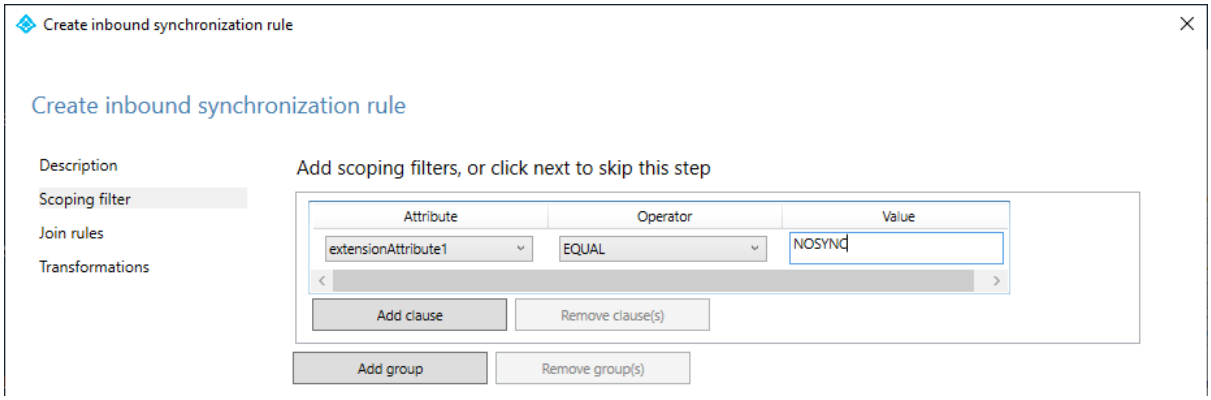

Figure 4.13 – Configuring a scoping filter for extensionAttribute1

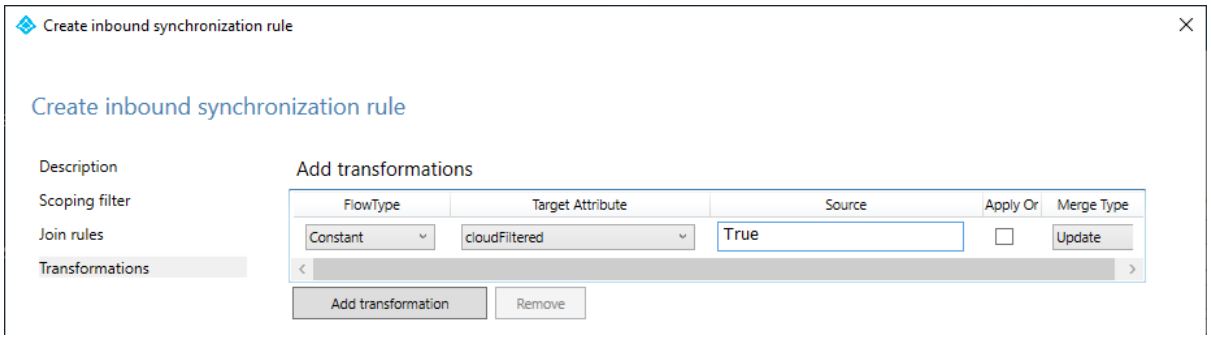

Figure 4.14 – Adding a transformation for the cloudFiltered attribute

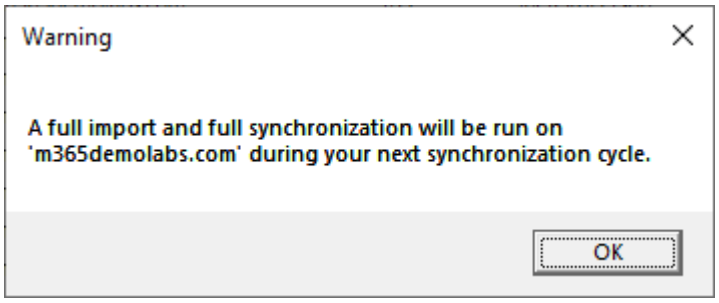

Figure 4.15 – Warning for full import and synchronization

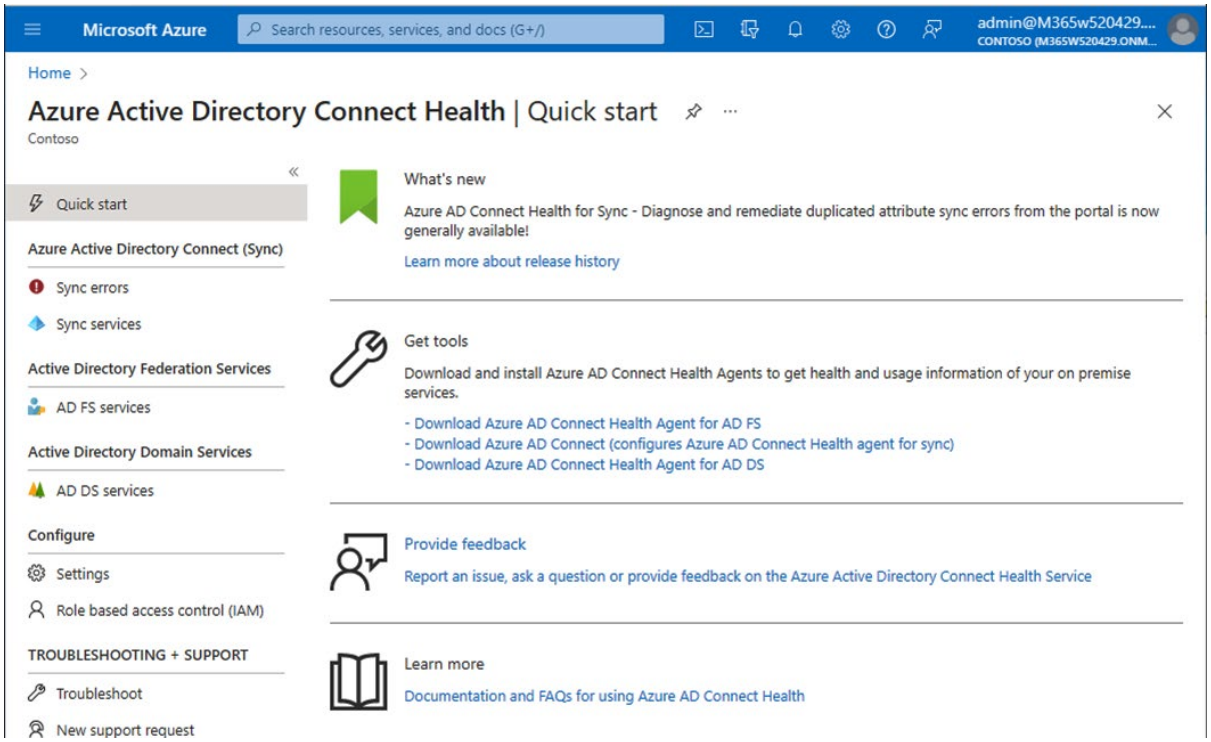

Figure 4.16 – Azure Active Directory Connect Health

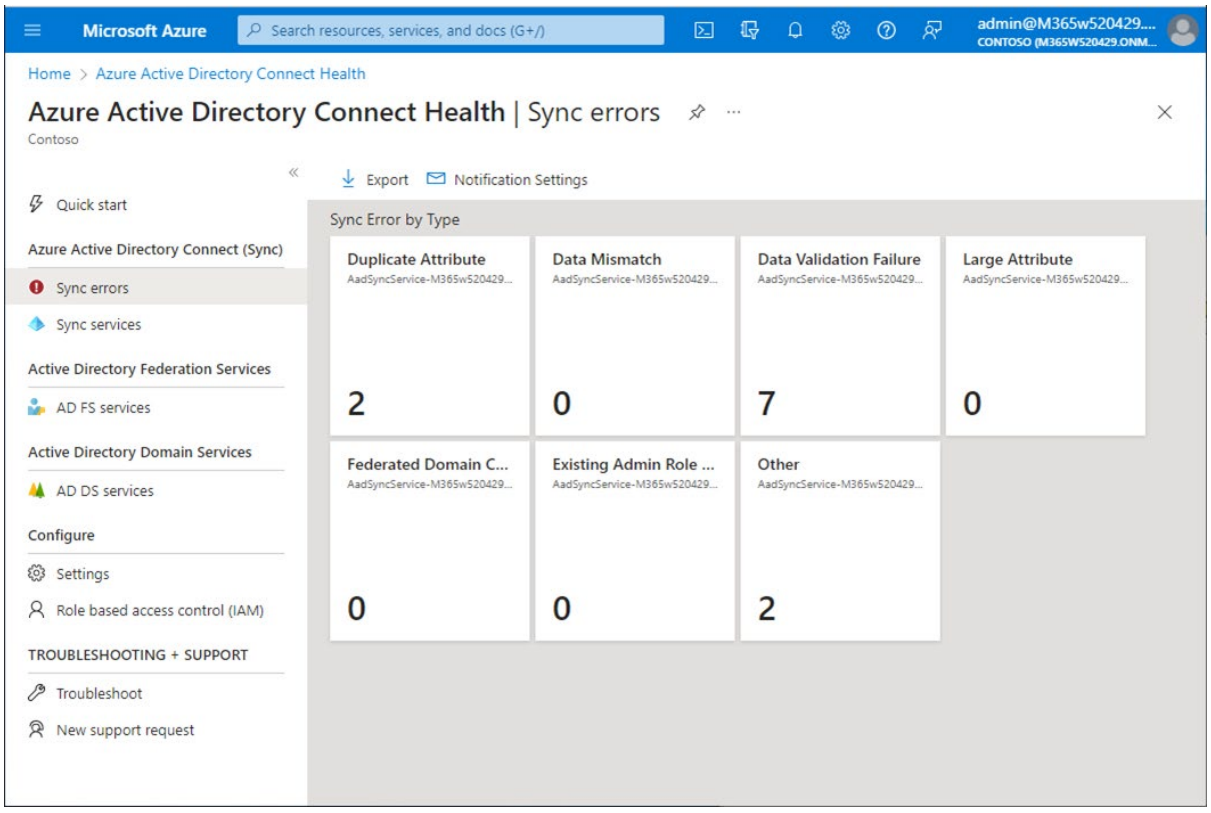

Figure 4.17 – Azure AD Connect Health Sync errors

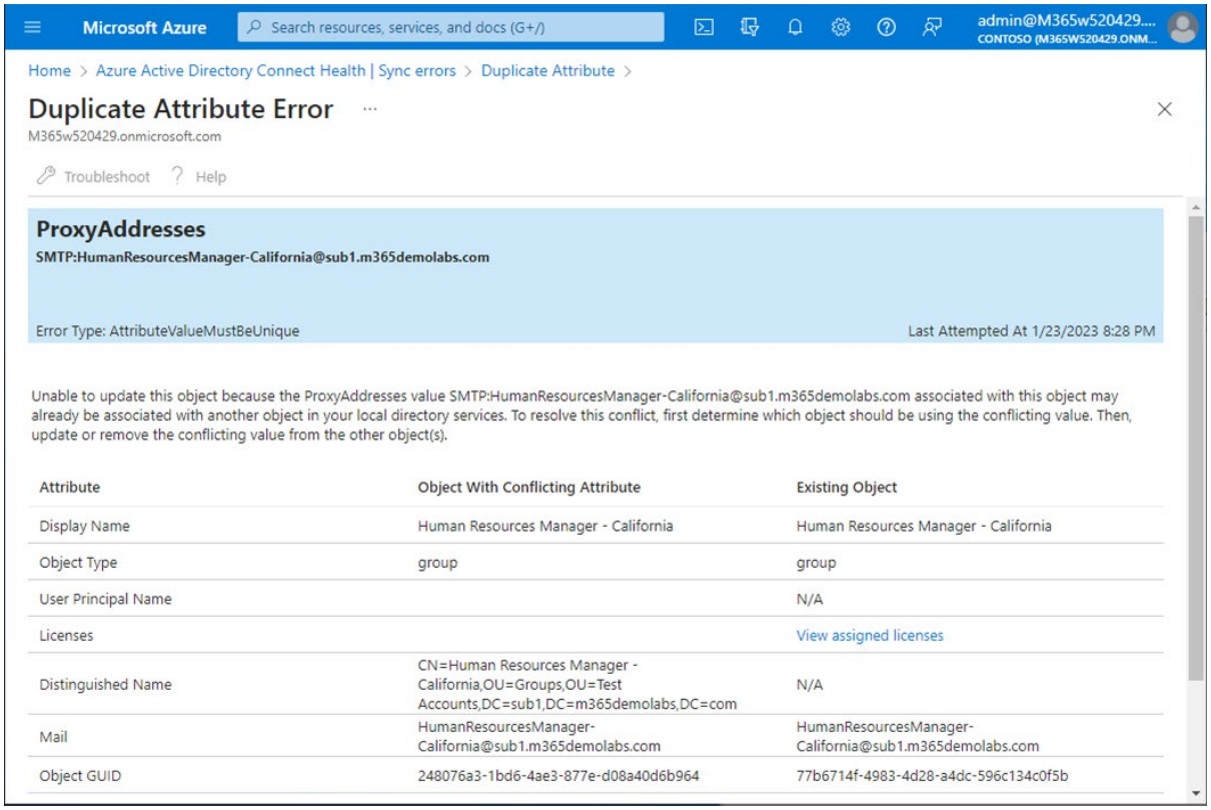

Figure 4.18 – Azure AD Connect Health error details

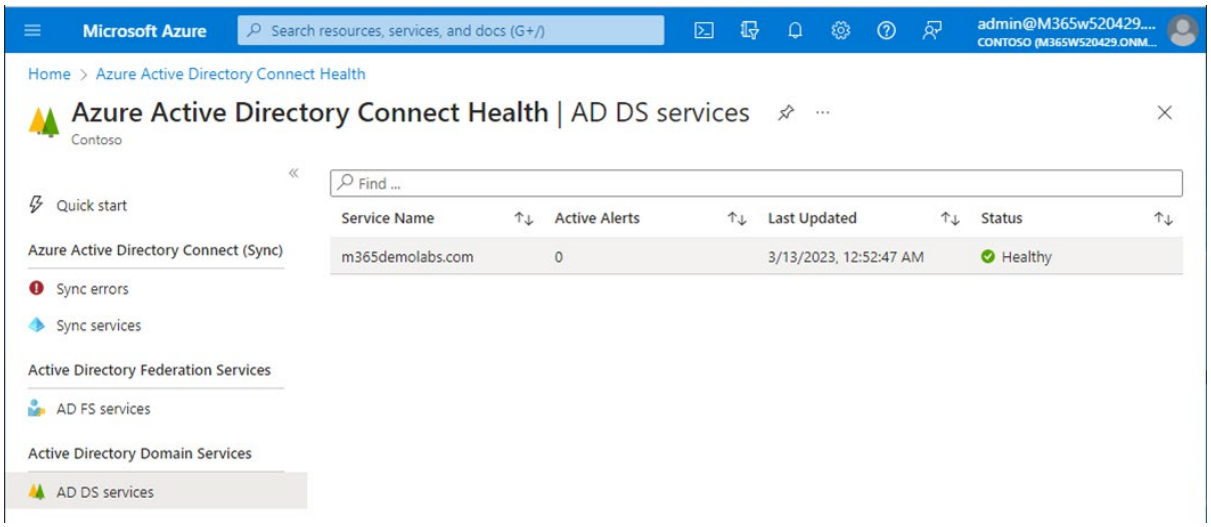

Figure 4.19 – Azure AD Connect Health AD DS services

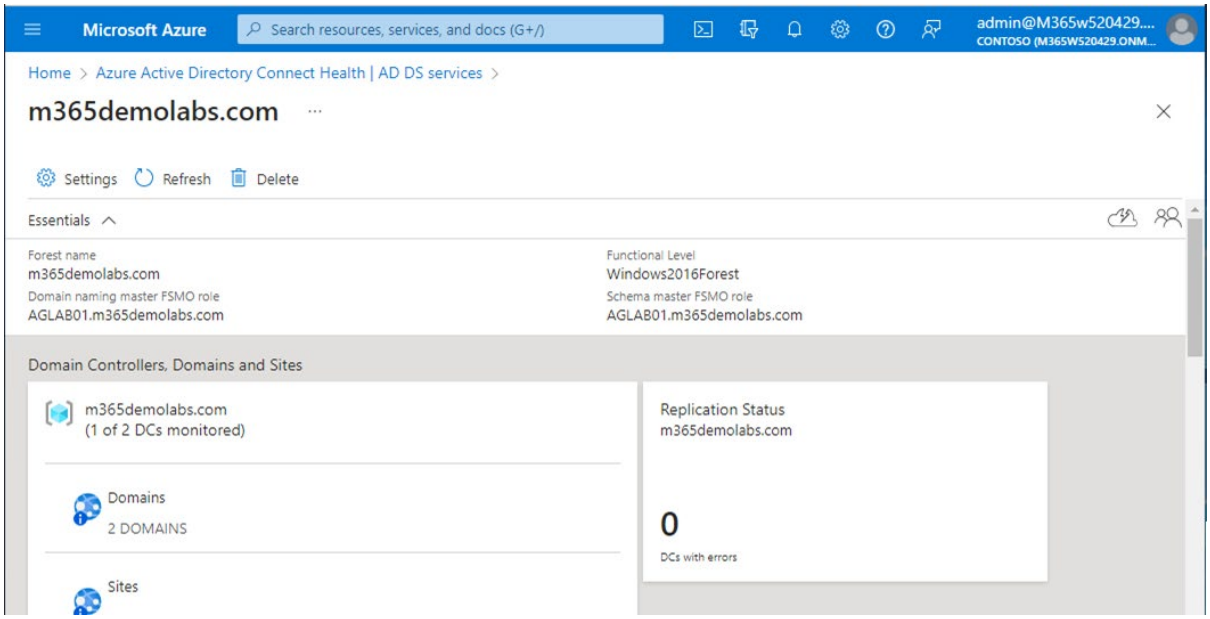

Figure 4.20 – Azure AD Connect Health for DS detail page

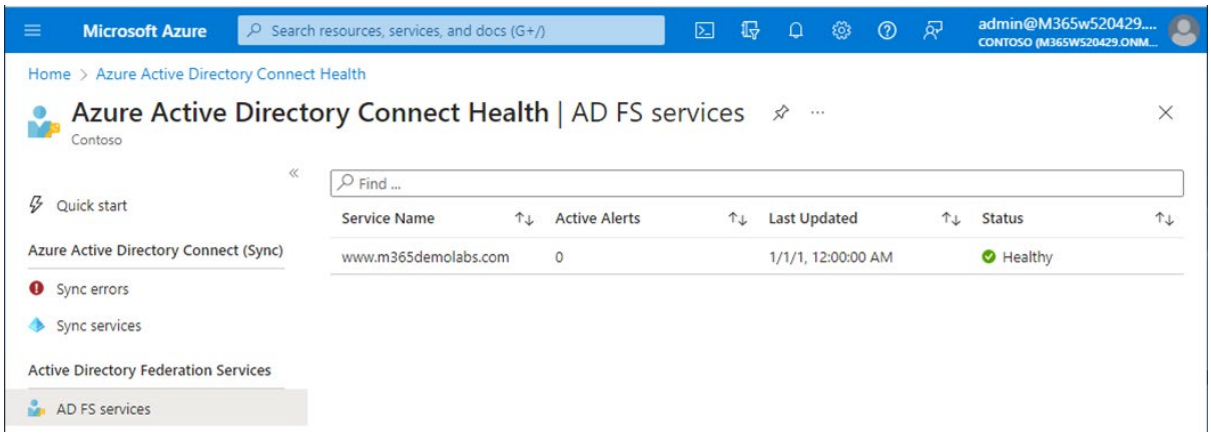

Figure 4.21 – Azure AD Connect Health for AD FS

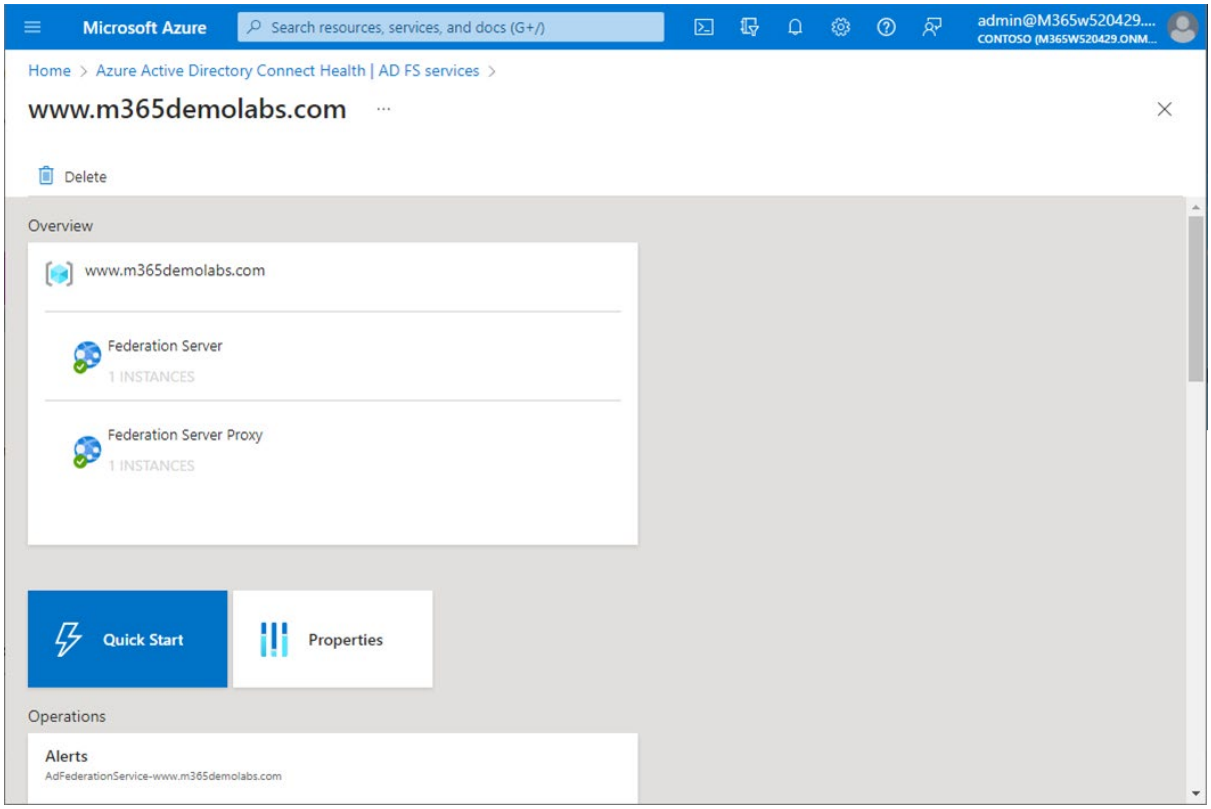

Figure 4.22 – Azure AD Connect Health for AD FS overview

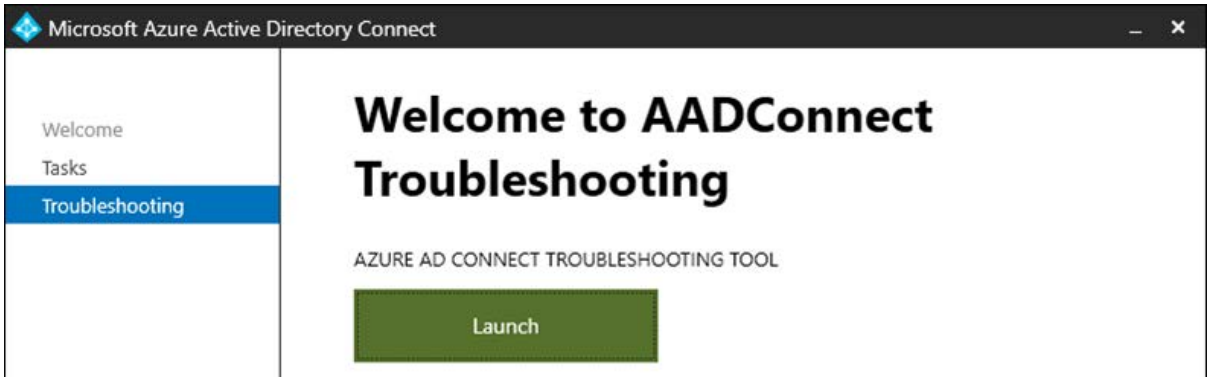

Figure 4.23 – Launching the AADConnect Troubleshooting tool

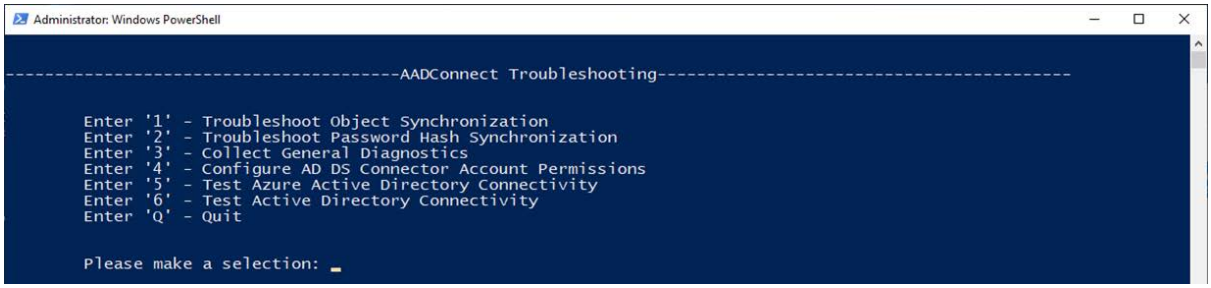

Figure 4.24 – AADConnect Troubleshooting menu

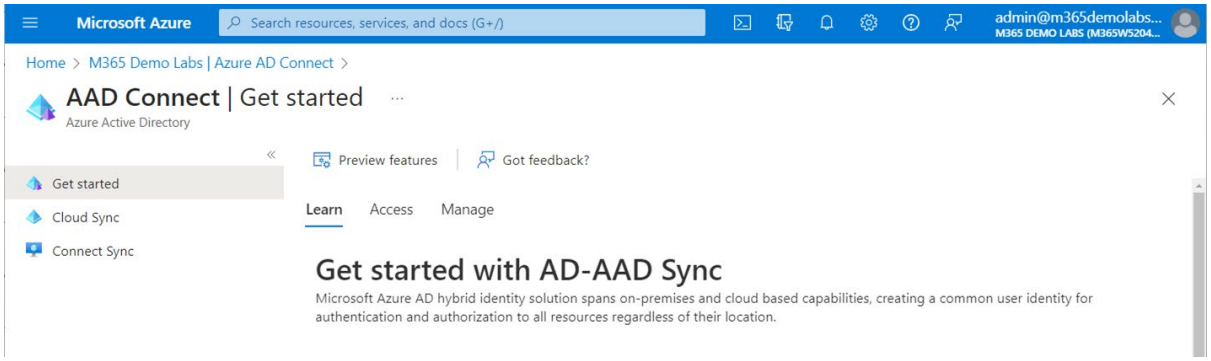

Figure 4.25 – Azure AD Connect in the Azure portal

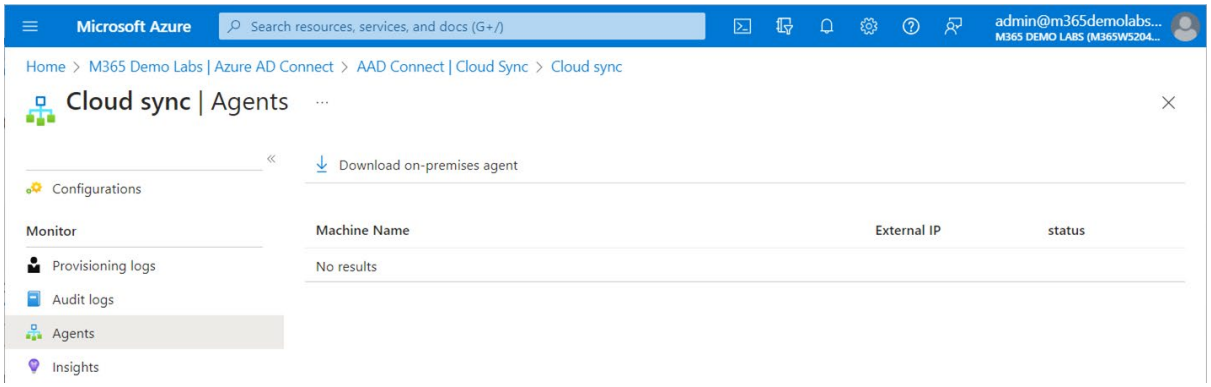

Figure 4.26 – Download on-premises agent for Azure AD Connect Cloud Sync

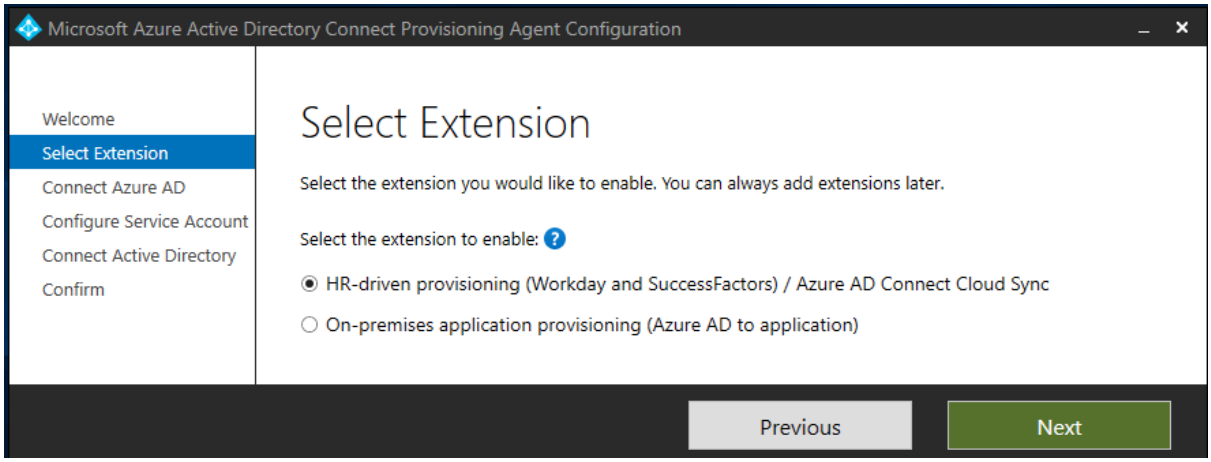

Figure 4.27 – Azure AD Connect Cloud Sync Select Extension page

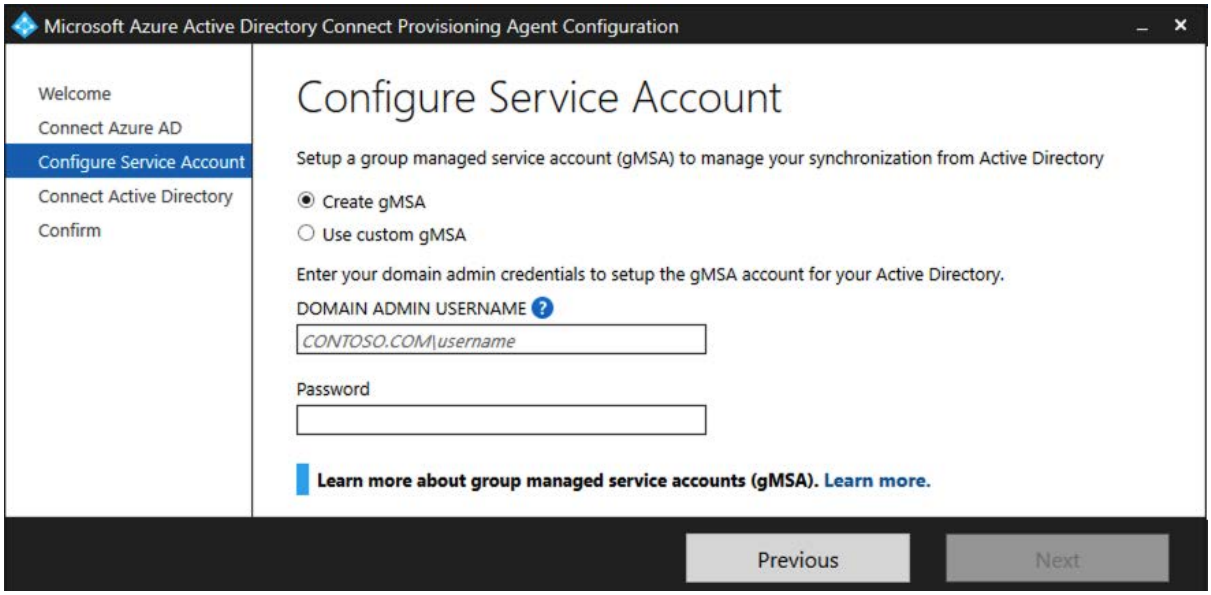

Figure 4.28 – Configure Azure AD Connect Cloud Sync service account

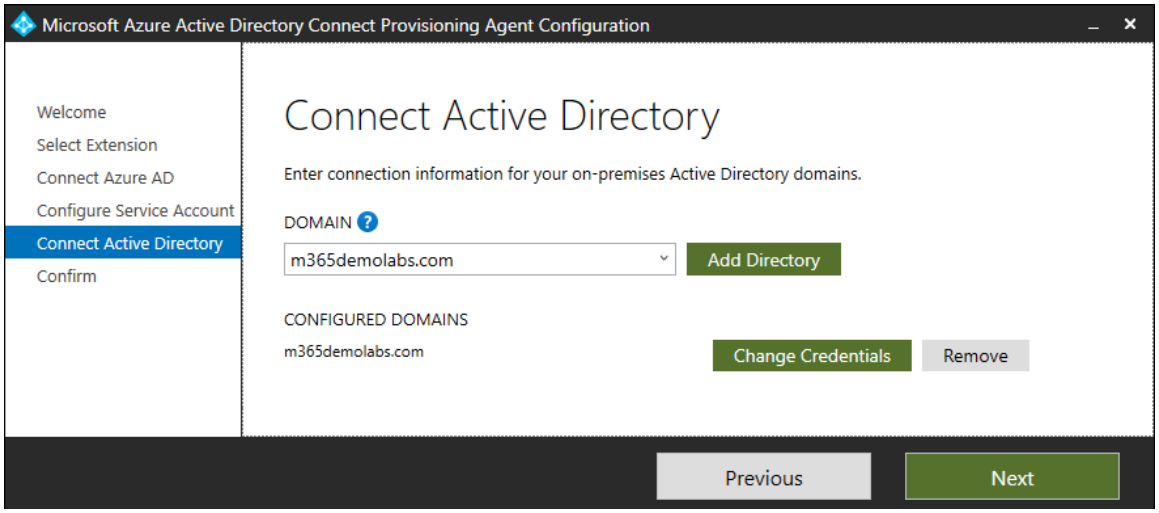

Figure 4.29 – Adding a directory to Azure AD Connect Cloud Sync

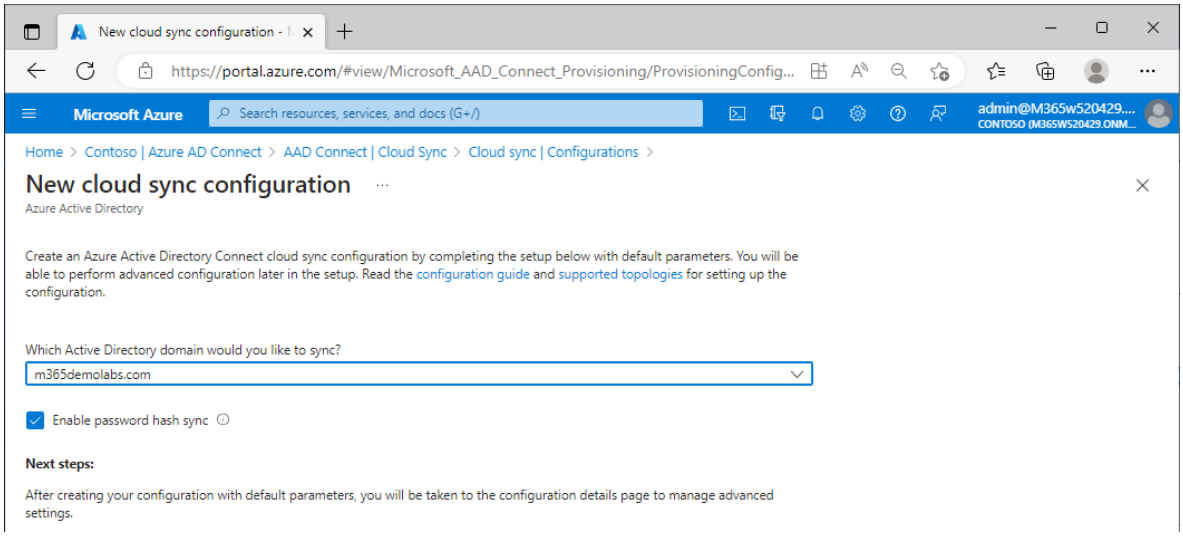

Figure 4.30 – Creating a new Azure AD Connect Cloud Sync configuration

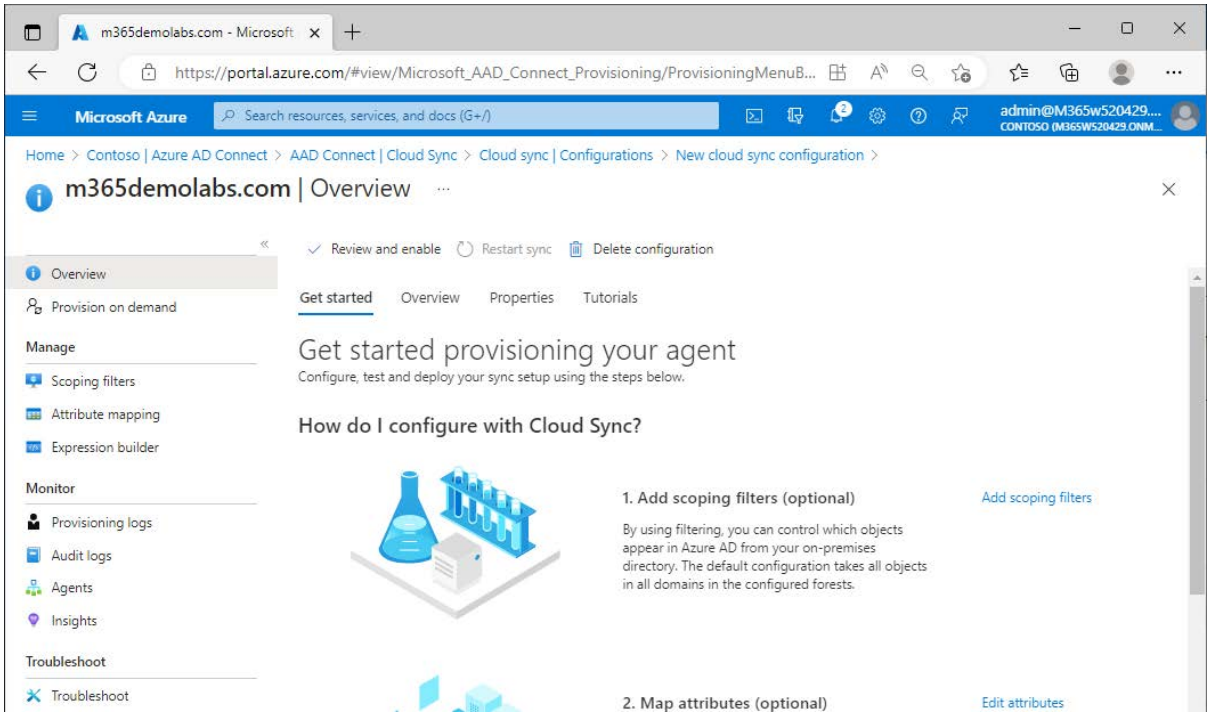

Figure 4.31 – Provisioning agent overview page

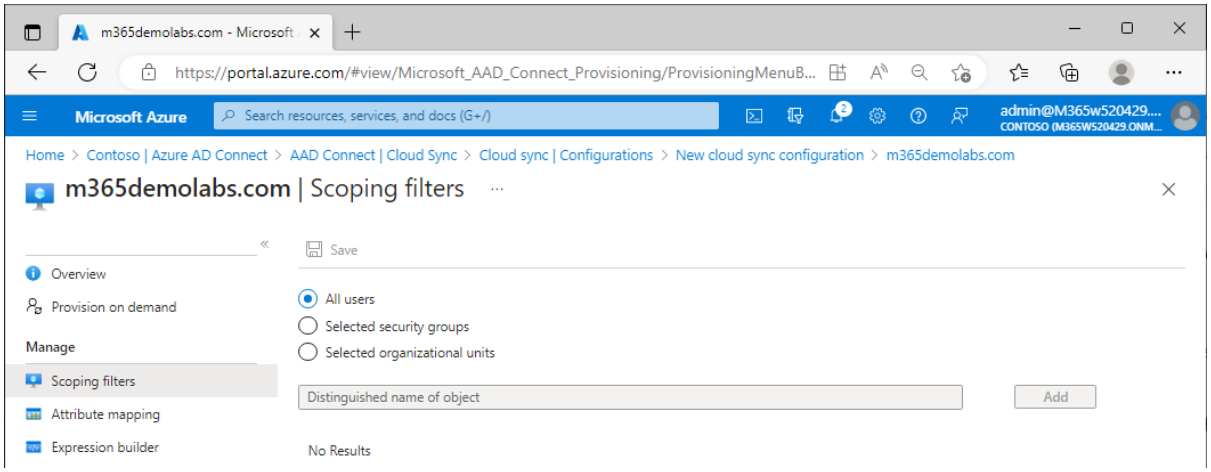

Figure 4.32 – Azure AD Connect Cloud Sync scoping filters

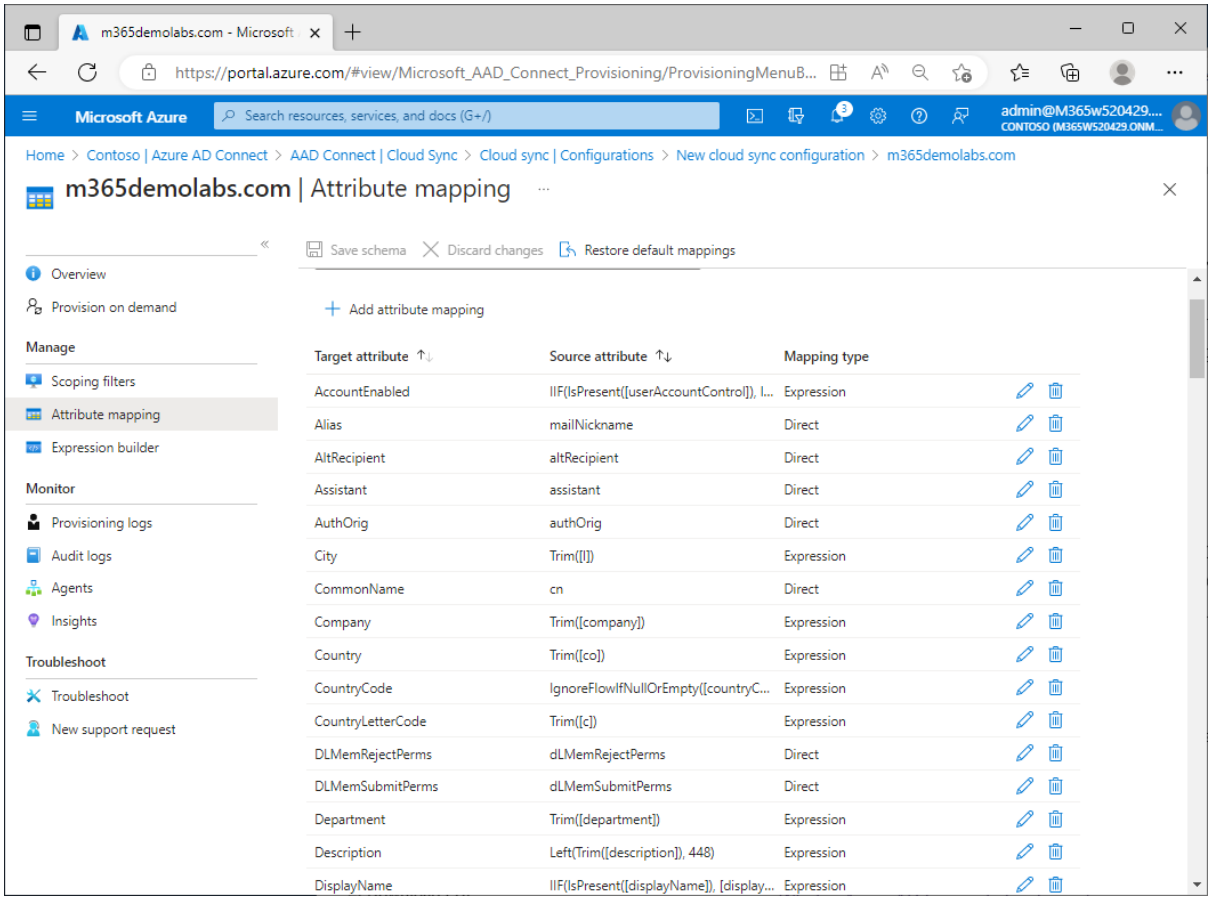

Figure 4.33 – Azure AD Connect Cloud Sync attribute mappings

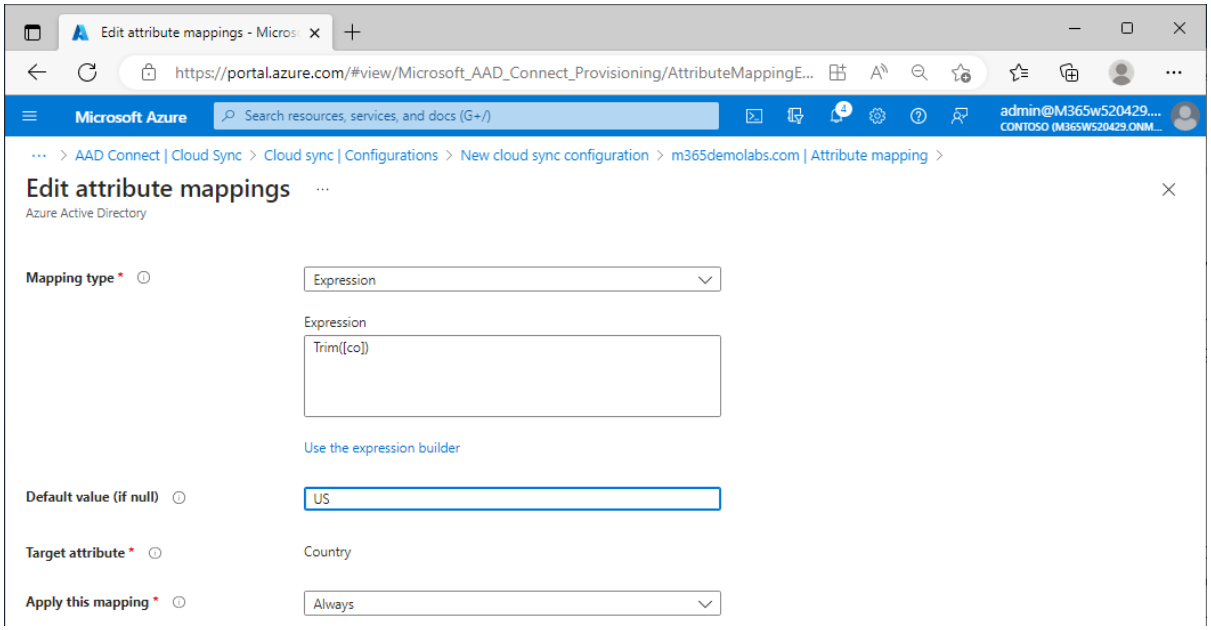

Figure 4.34 – Edit attribute mappings in Azure AD Connect Cloud Sync

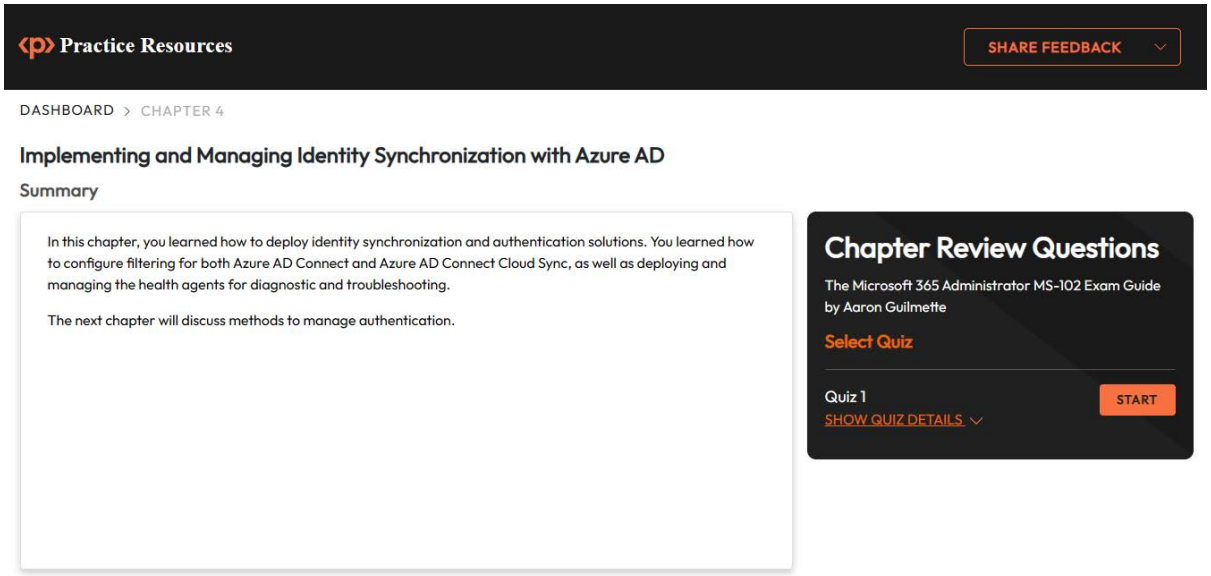

Figure 4.35 – Chapter Review Questions for Chapter 4

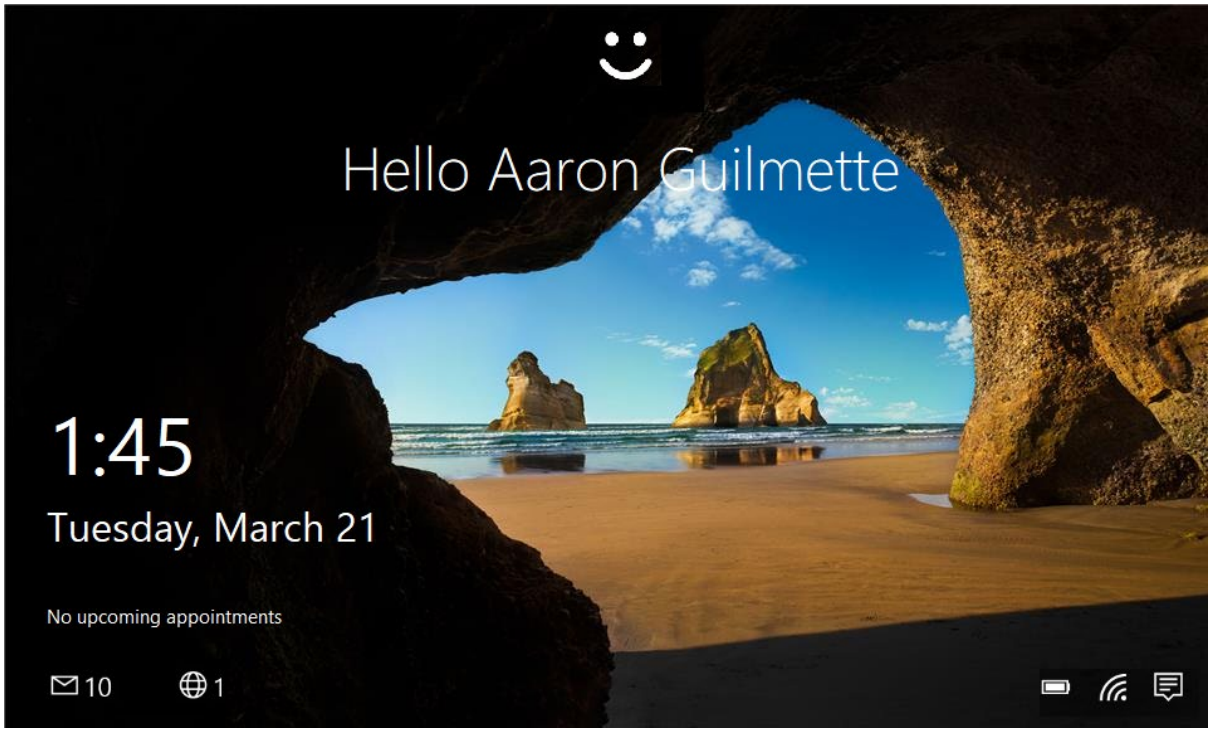

Figure 5.1 – Windows Hello for Business sign-on screen

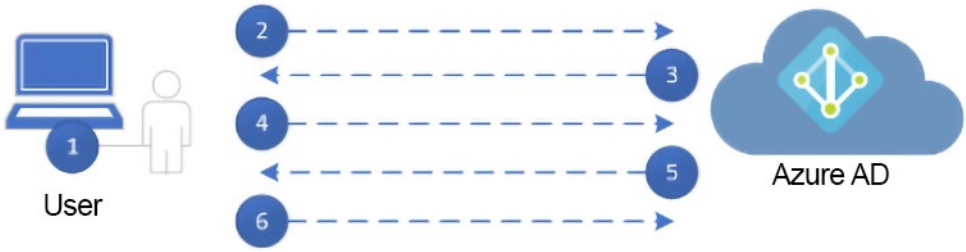

Figure 5.2 – Windows Hello authentication sequence

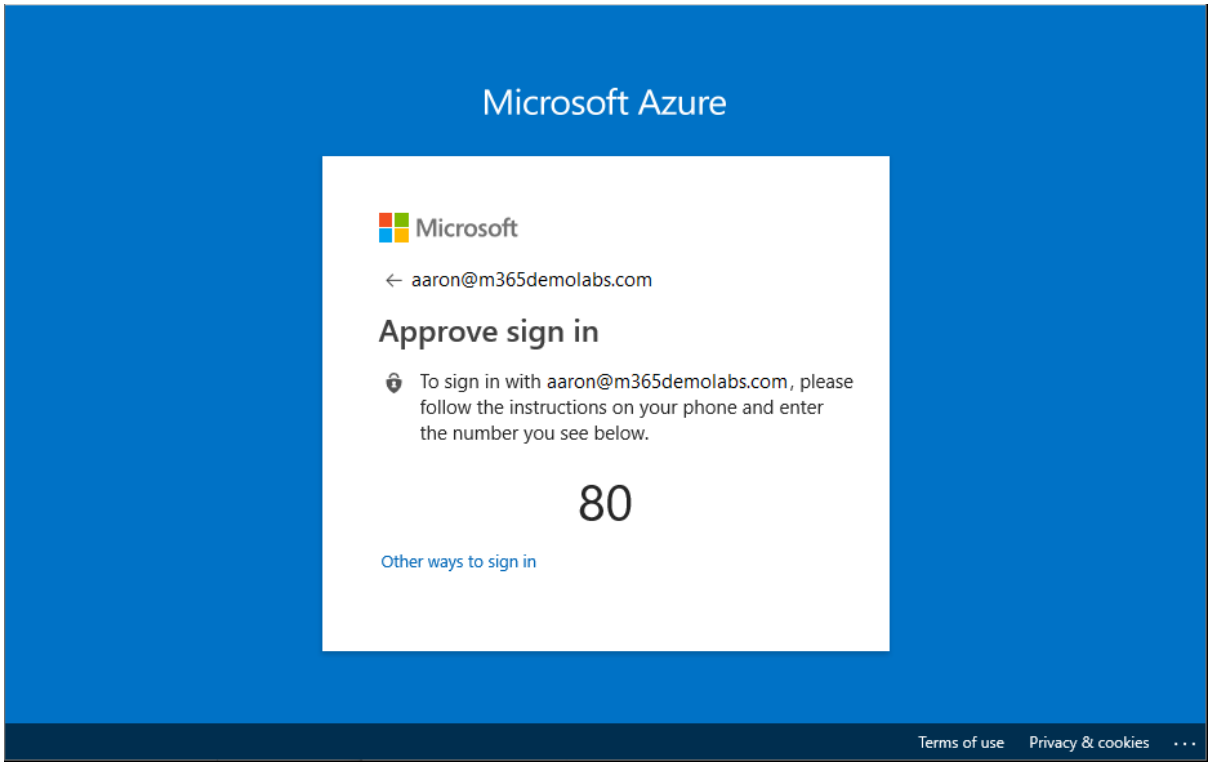

Figure 5.3 – Passwordless authentication dialog with Microsoft Authenticator

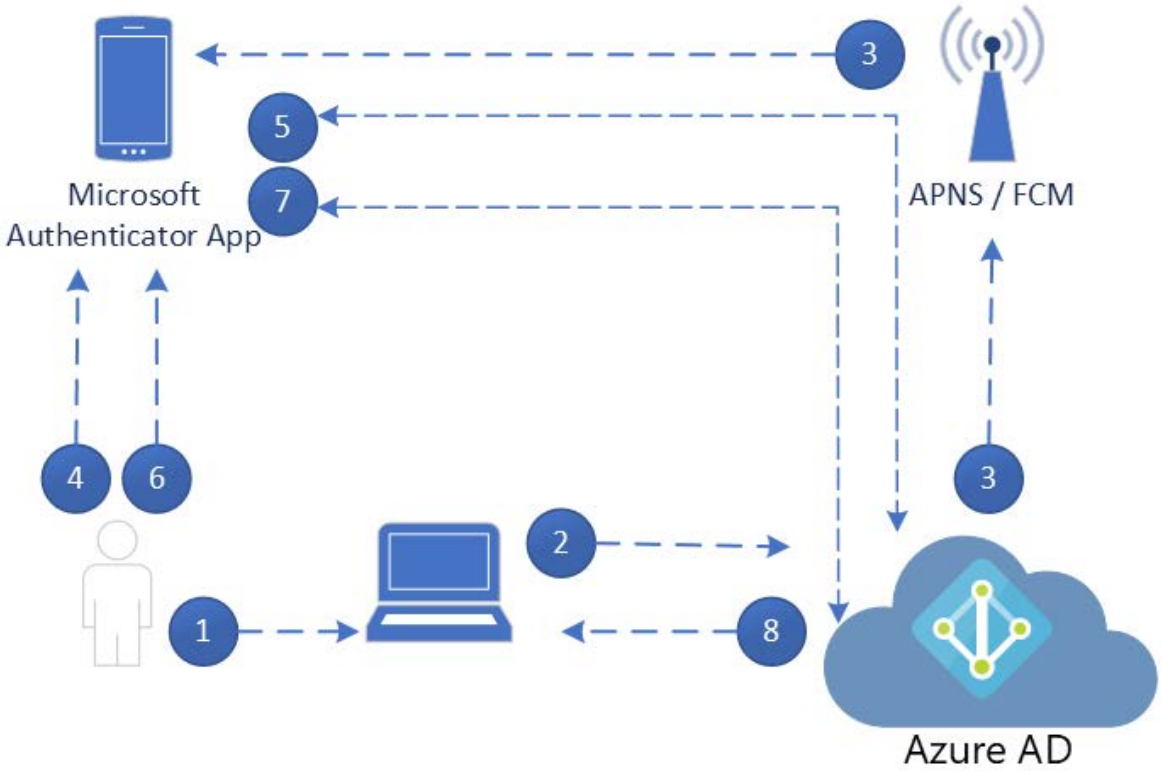

Figure 5.4 – Microsoft Authenticator authentication sequence

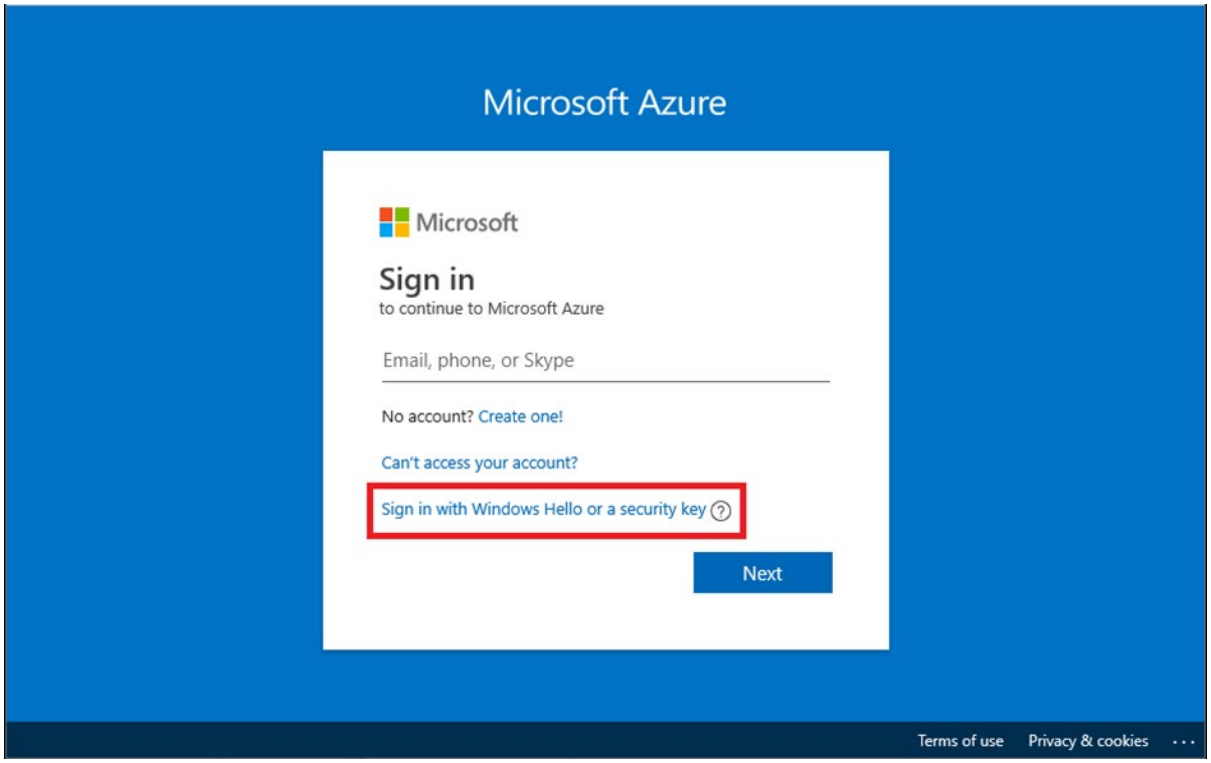

Figure 5.5 – Passwordless authentication dialog with a FIDO2 security token

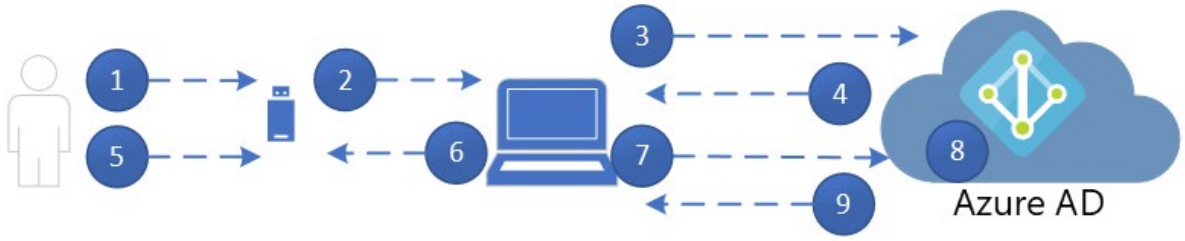

Figure 5.6 – FIDO2 authentication sequence

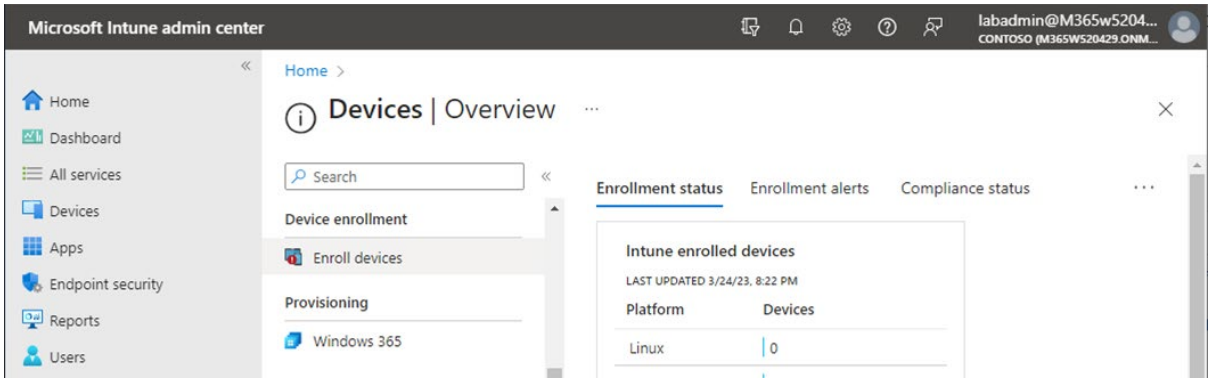

Figure 5.7 – Enroll devices

Figure 5.8 – Windows Hello for Business

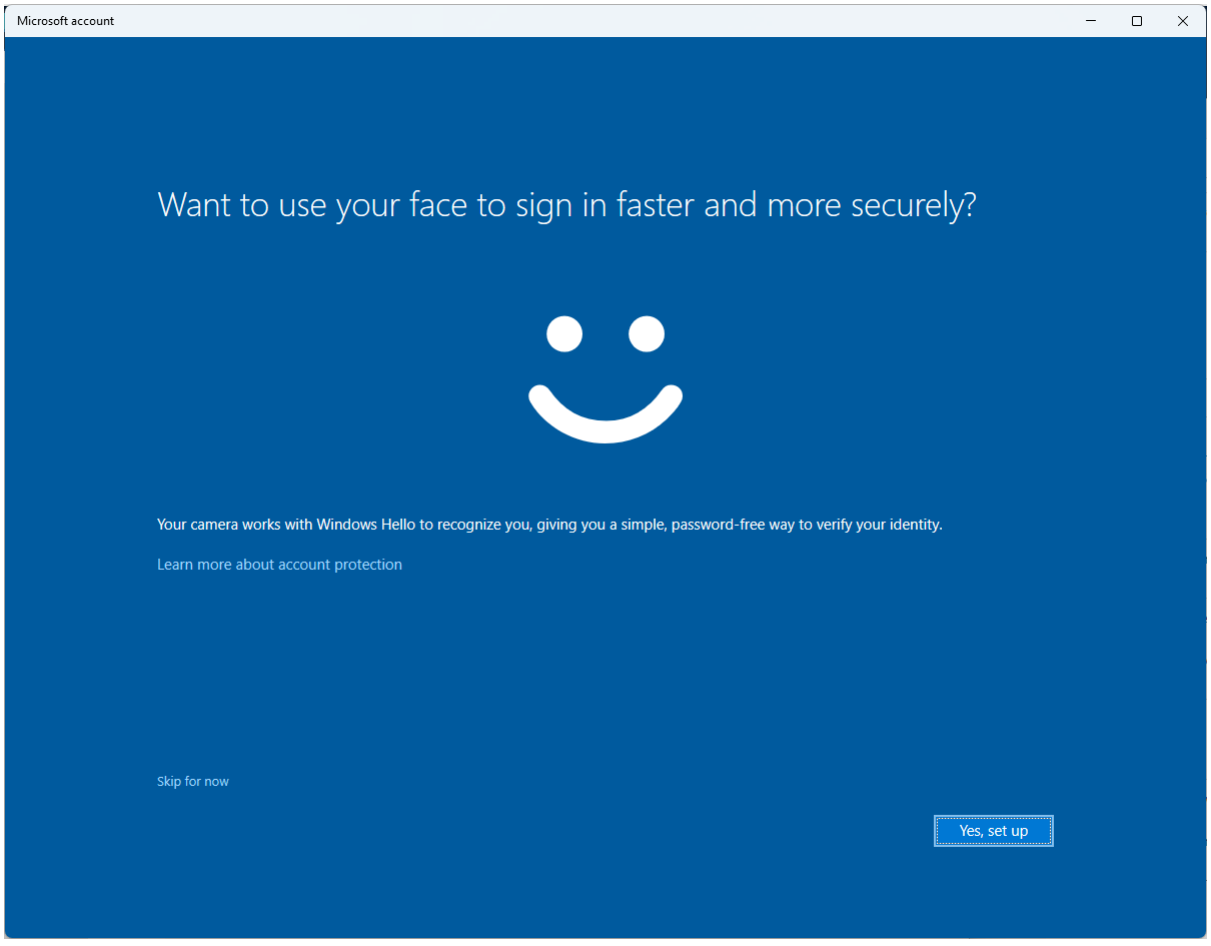

Figure 5.9 – Windows Hello for Business enrollment

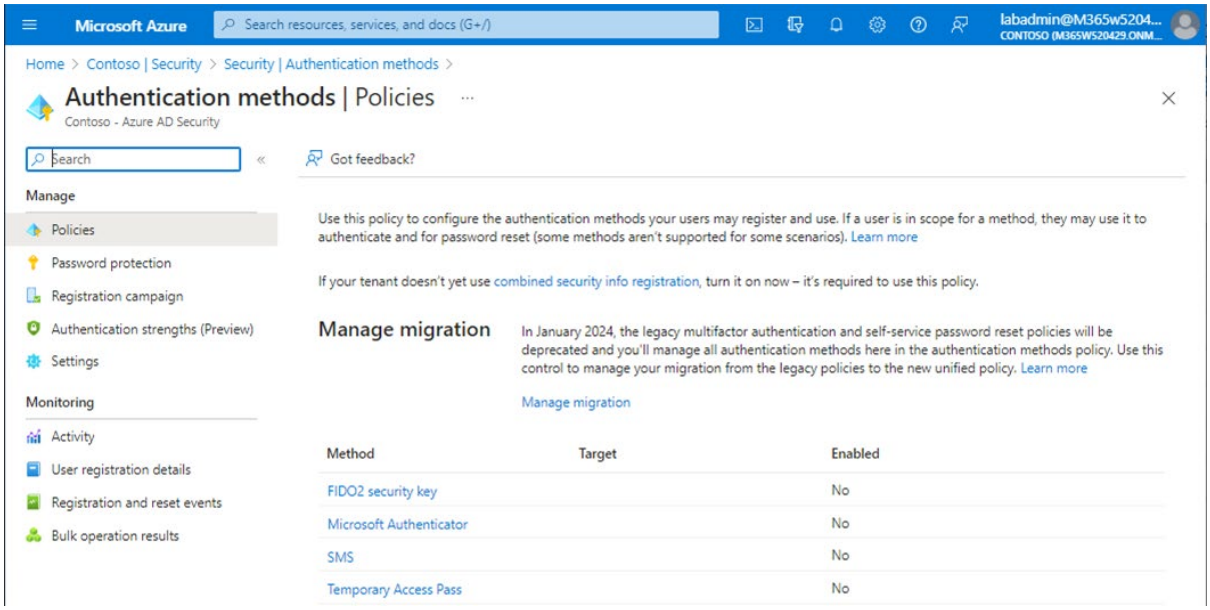

Figure 5.10 – Authentication methods

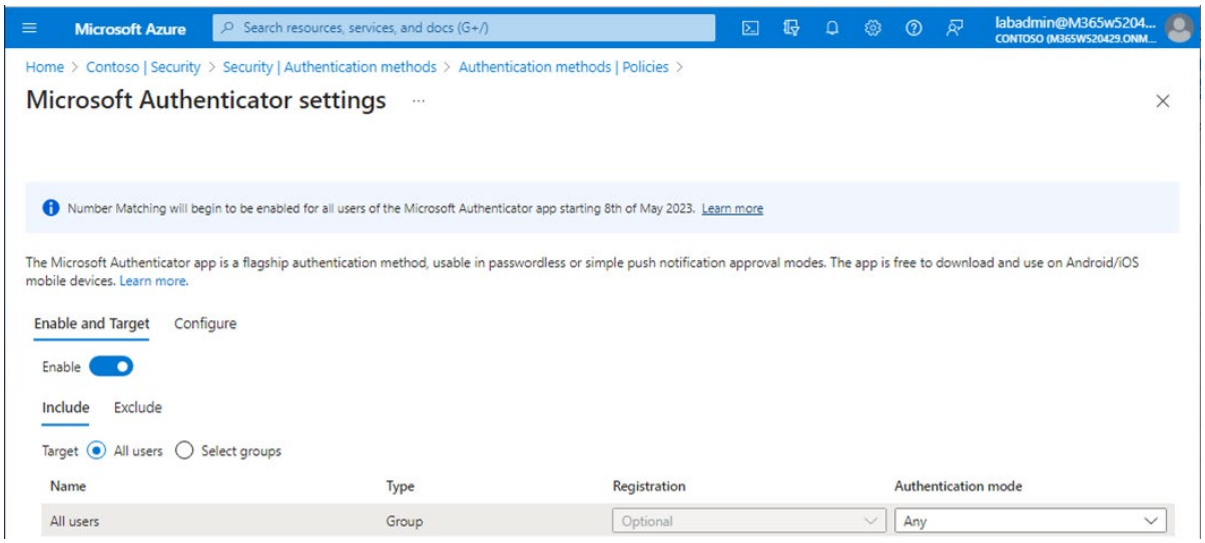

Figure 5.11 – Enabling Microsoft Authenticator

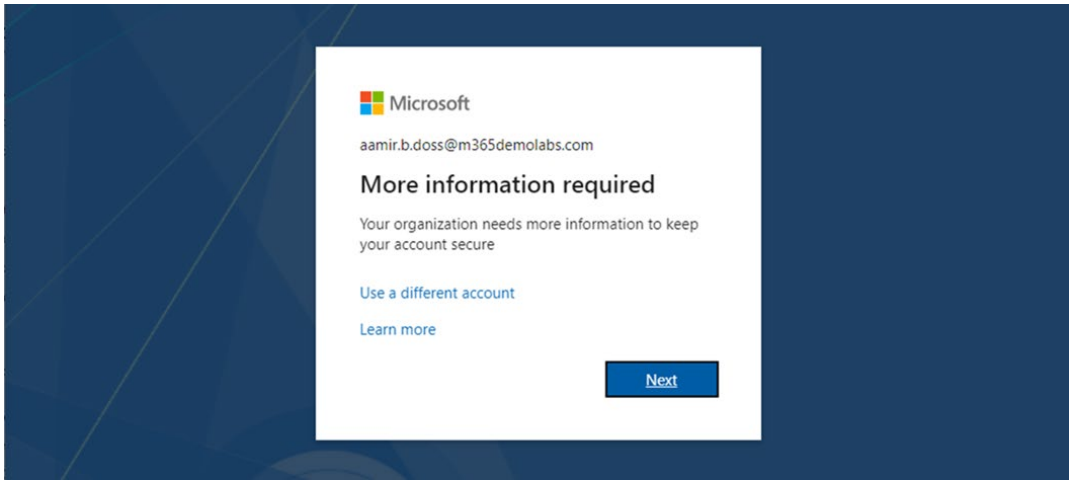

Figure 5.12 – More information required

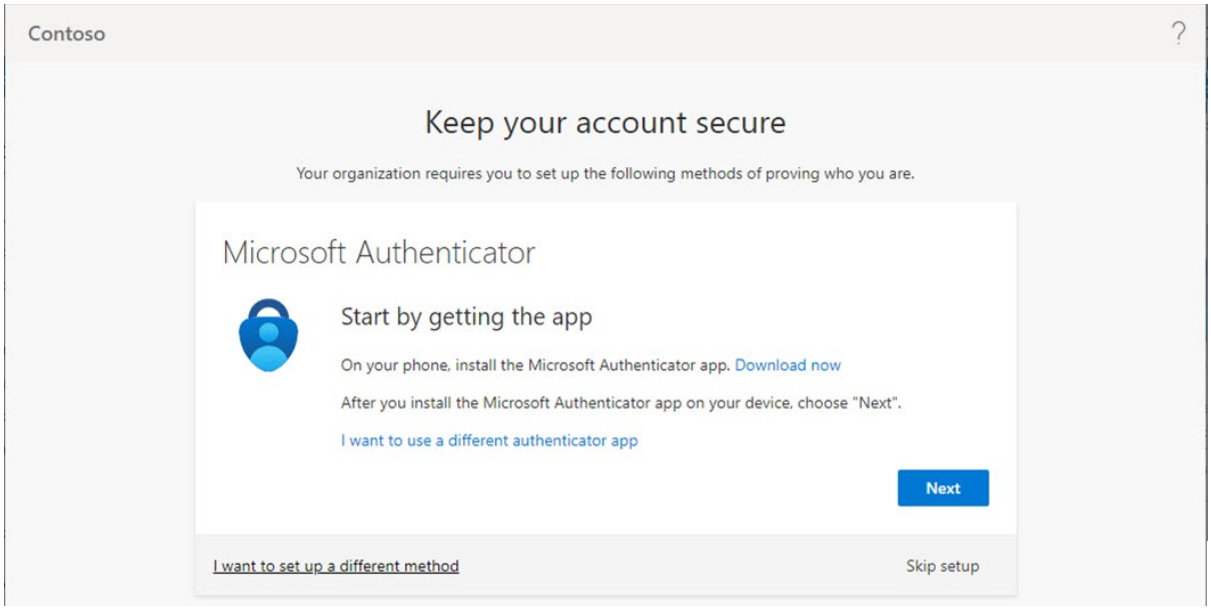

Figure 5.13 – Keep your account secure page

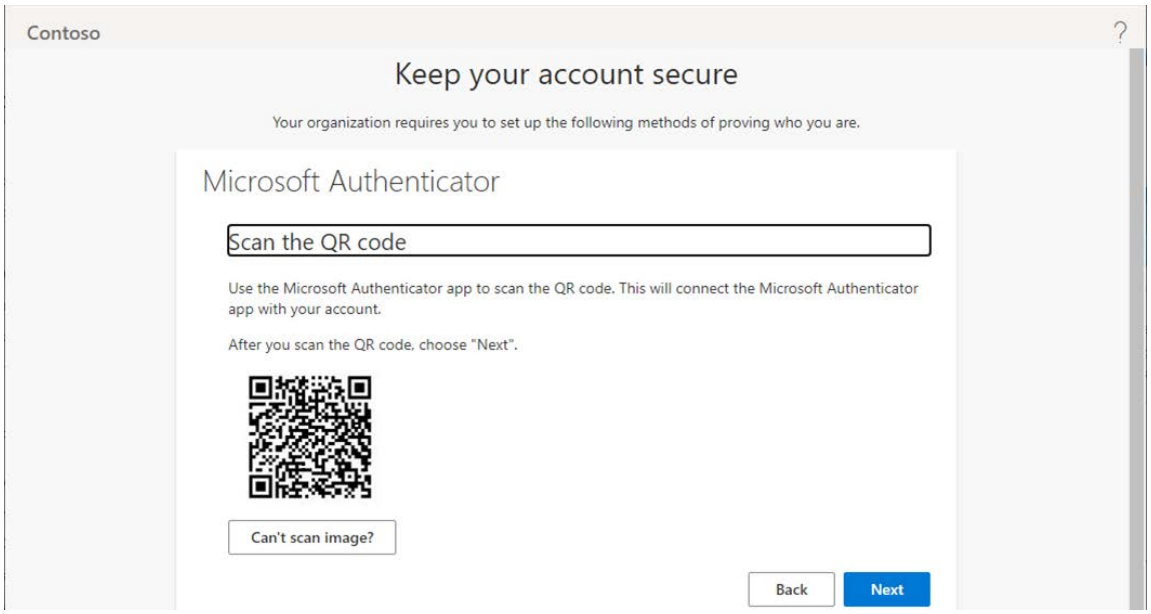

Figure 5.14 – Registering a device

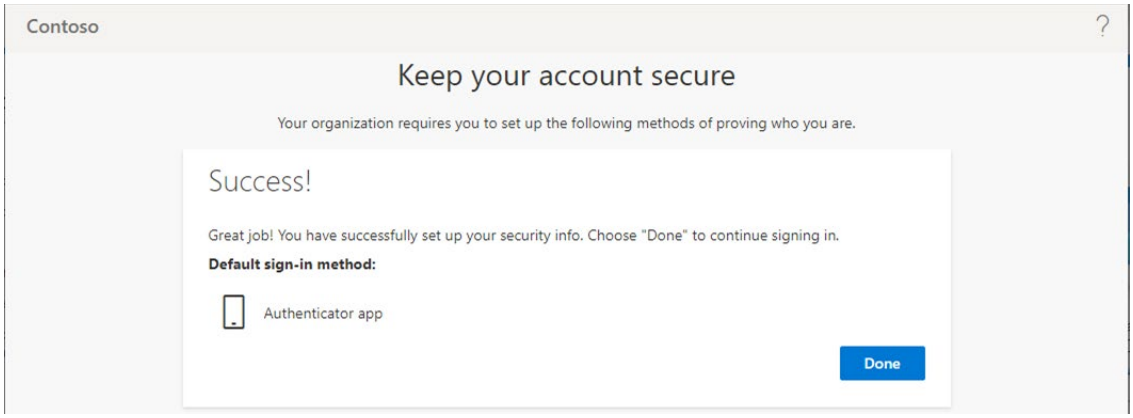

Figure 5.15 – Authenticator registration screen

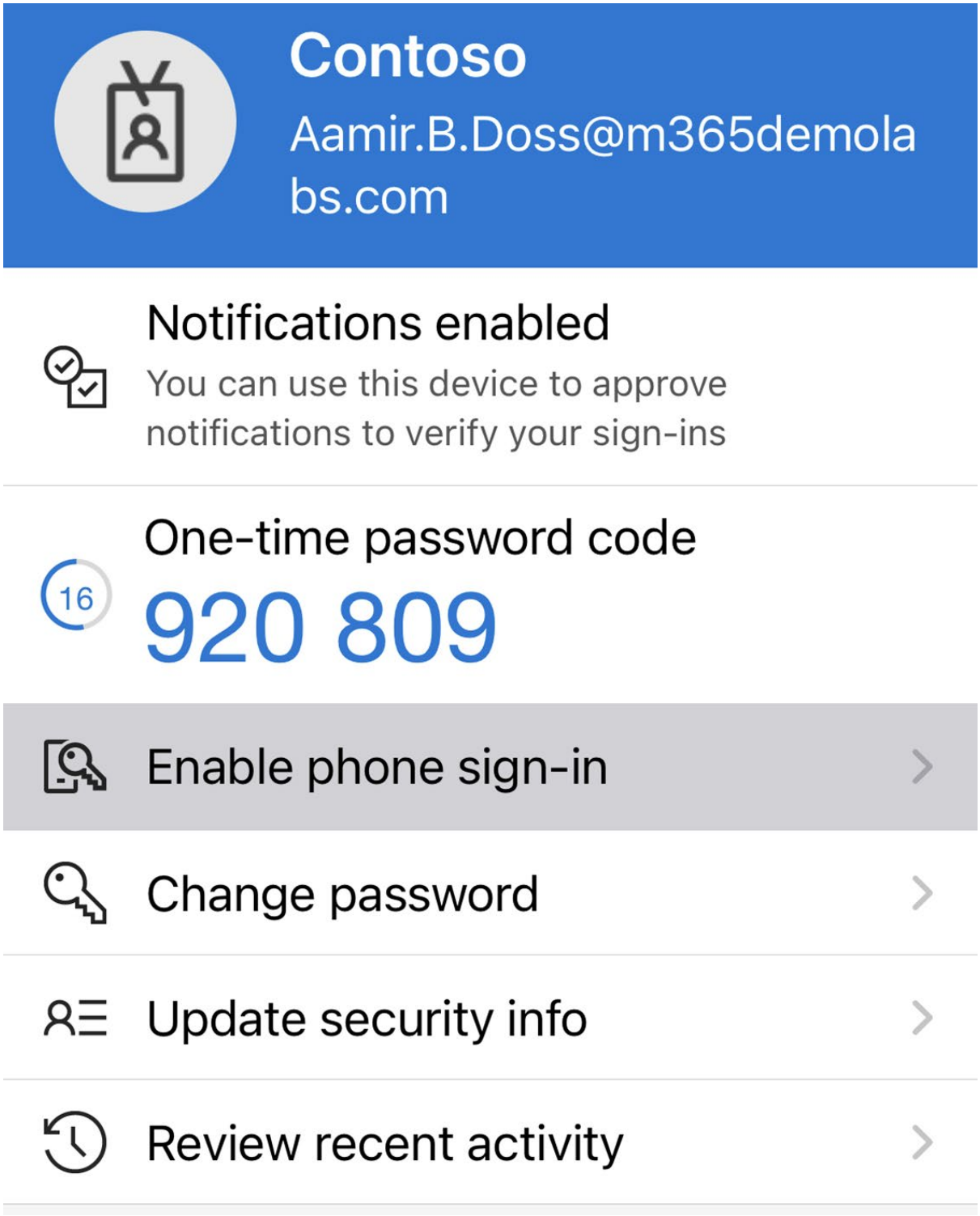

Figure 5.16 – Microsoft Authenticator Enable phone sign-in

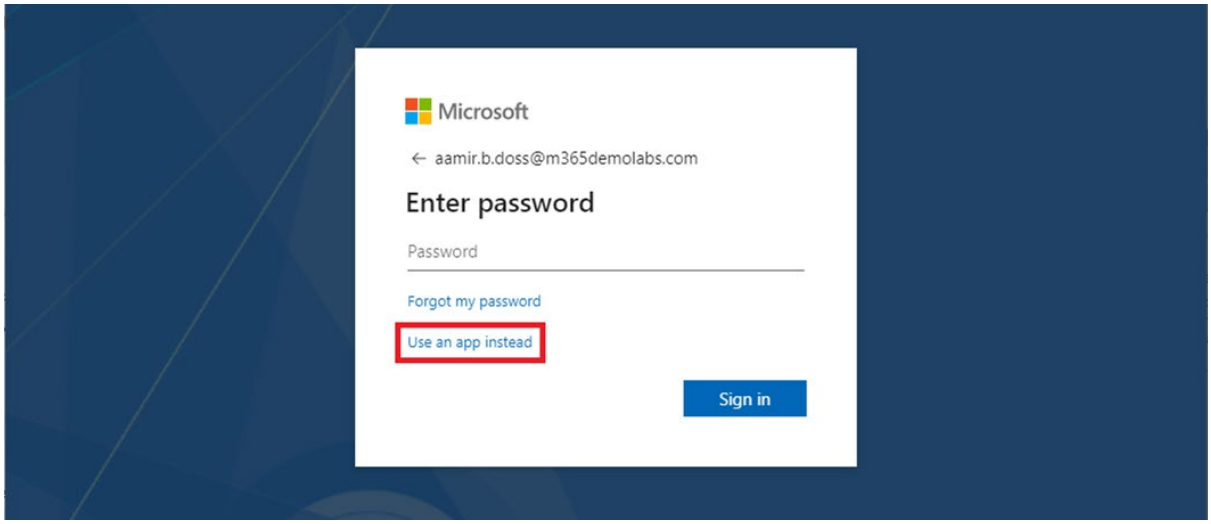

Figure 5.17 – Launching passwordless sign-in

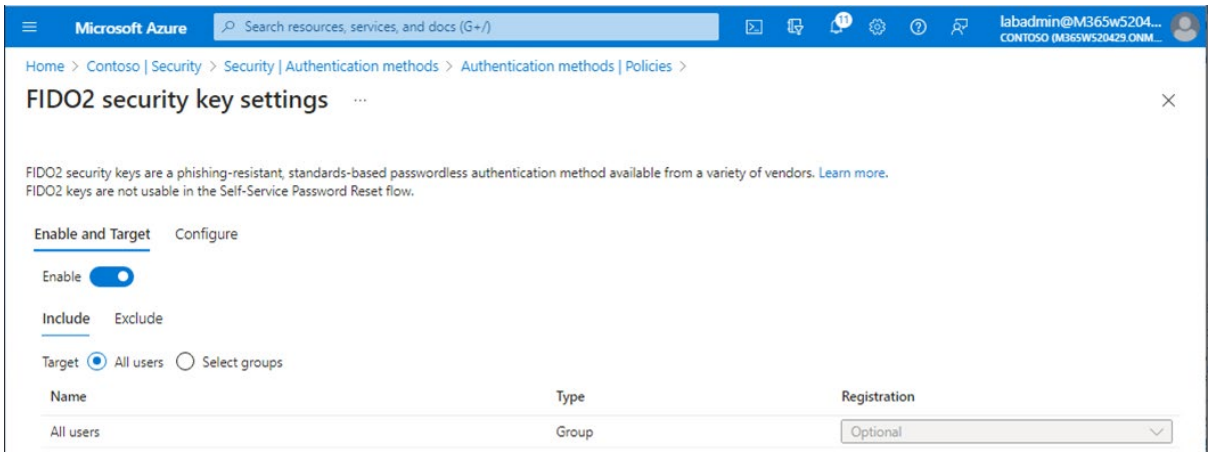

Figure 5.18 – Enabling Microsoft Authenticator

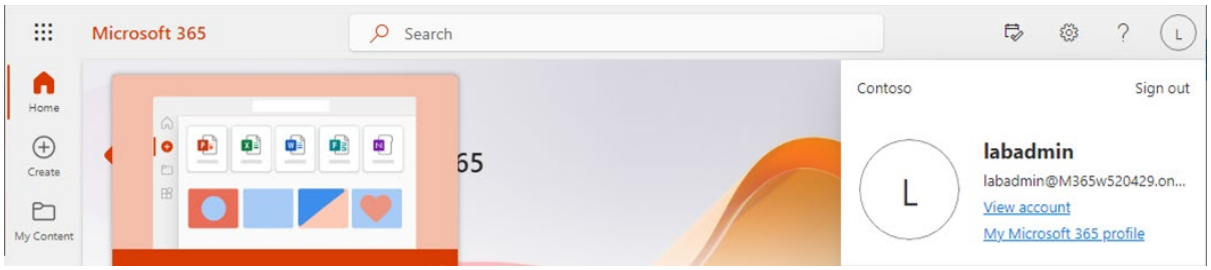

Figure 5.19 – Accessing My account

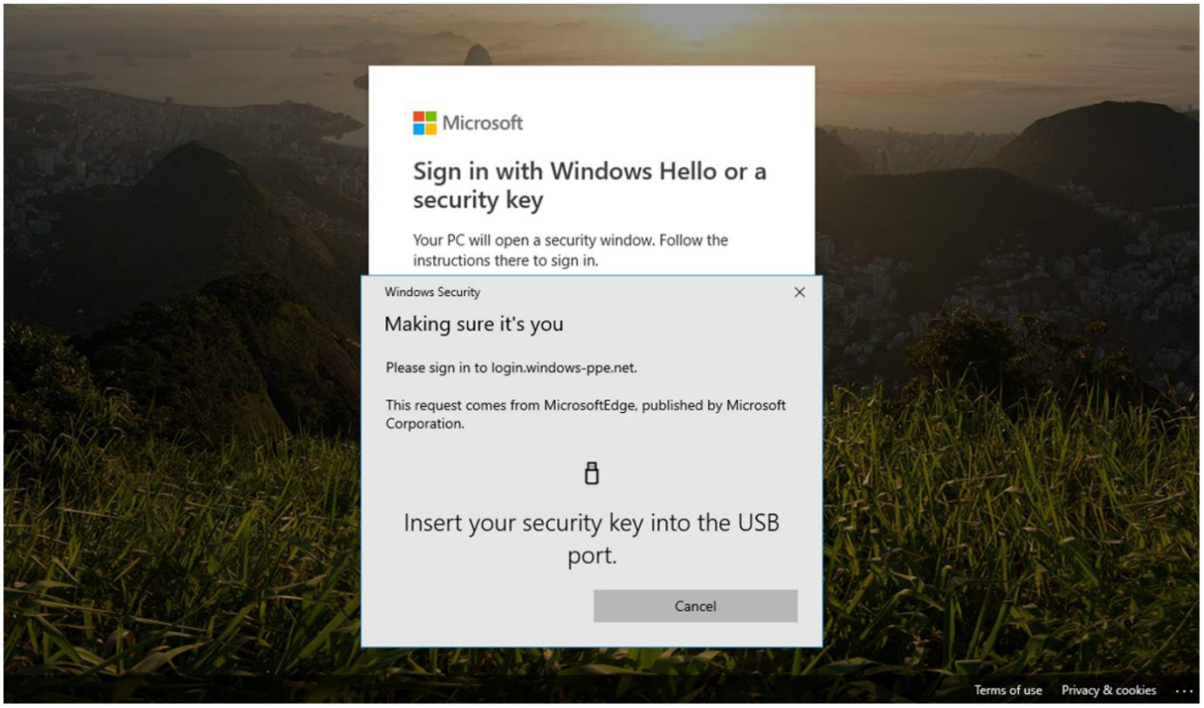

Figure 5.20 – Sign in with Windows Hello or a security key

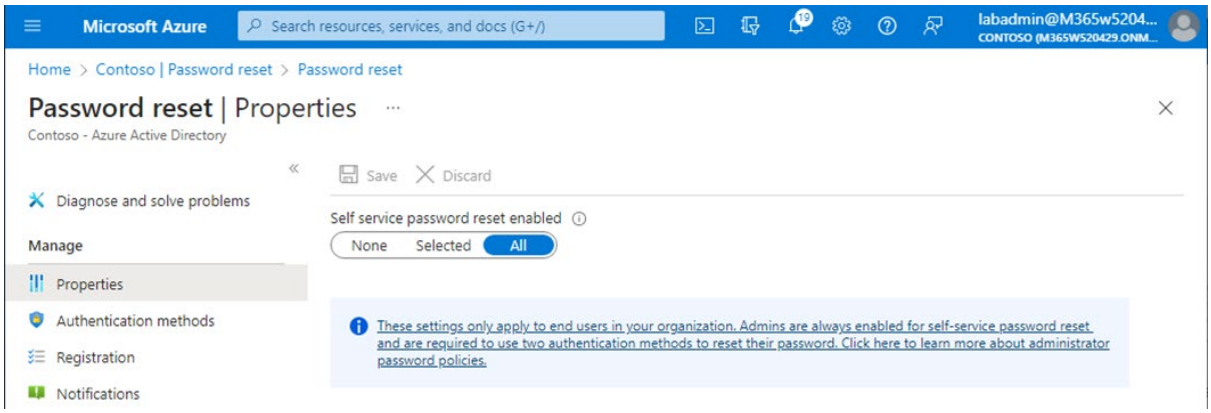

Figure 5.21 – Enabling self-service password reset

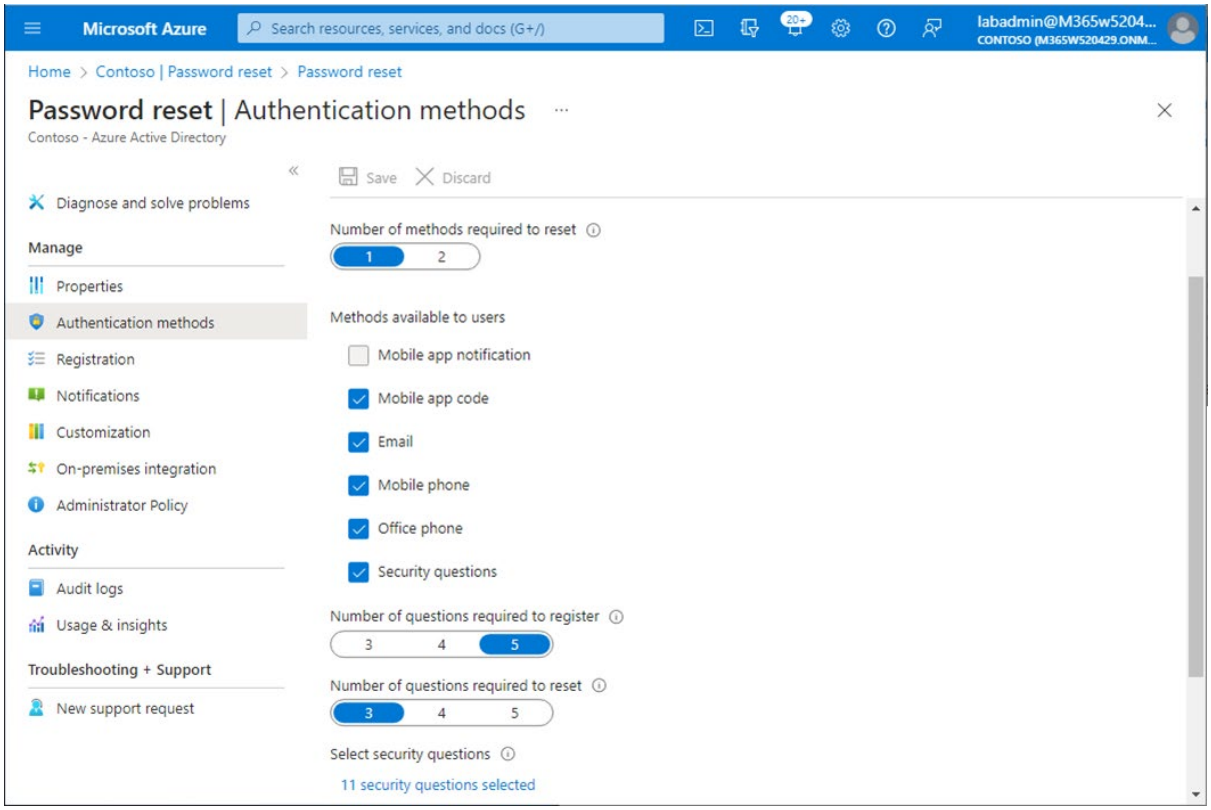

Figure 5.22 – Authentication methods

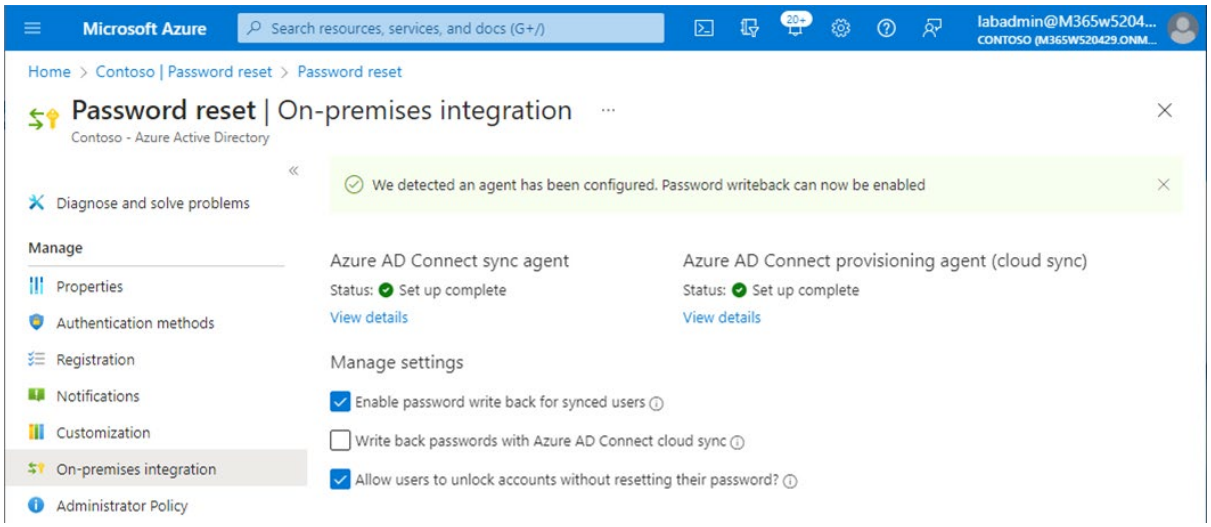

Figure 5.23 – On-premises integration

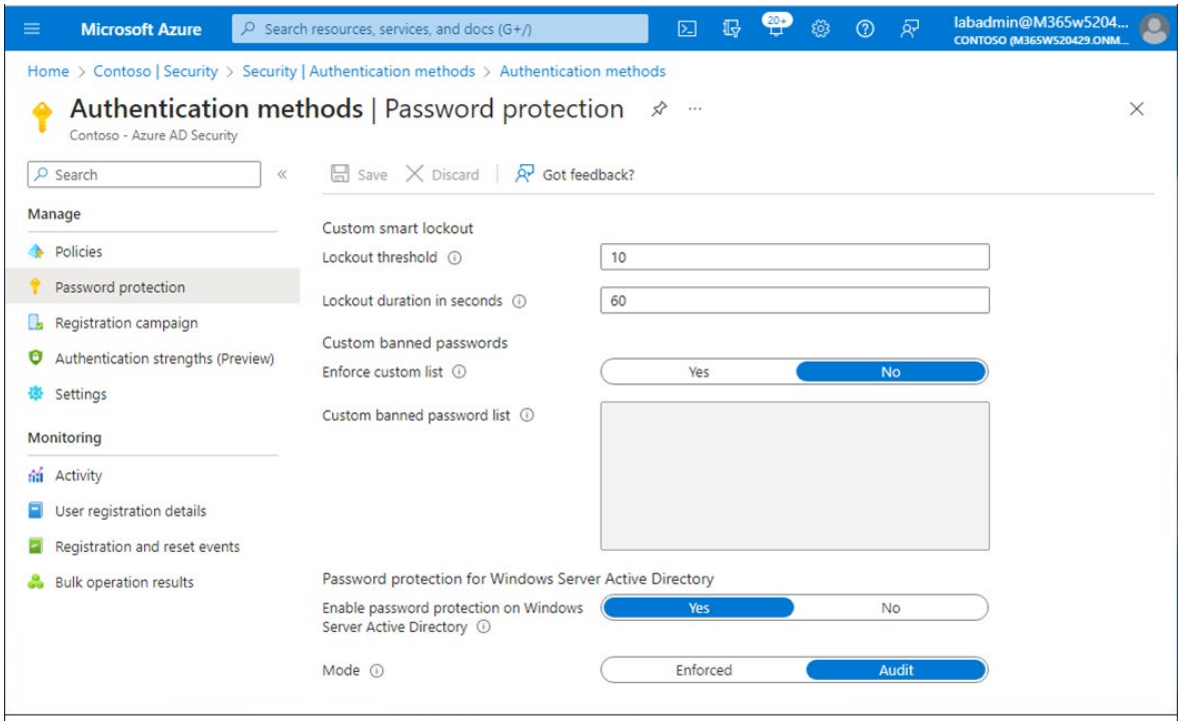

Figure 5.24 – Password protection

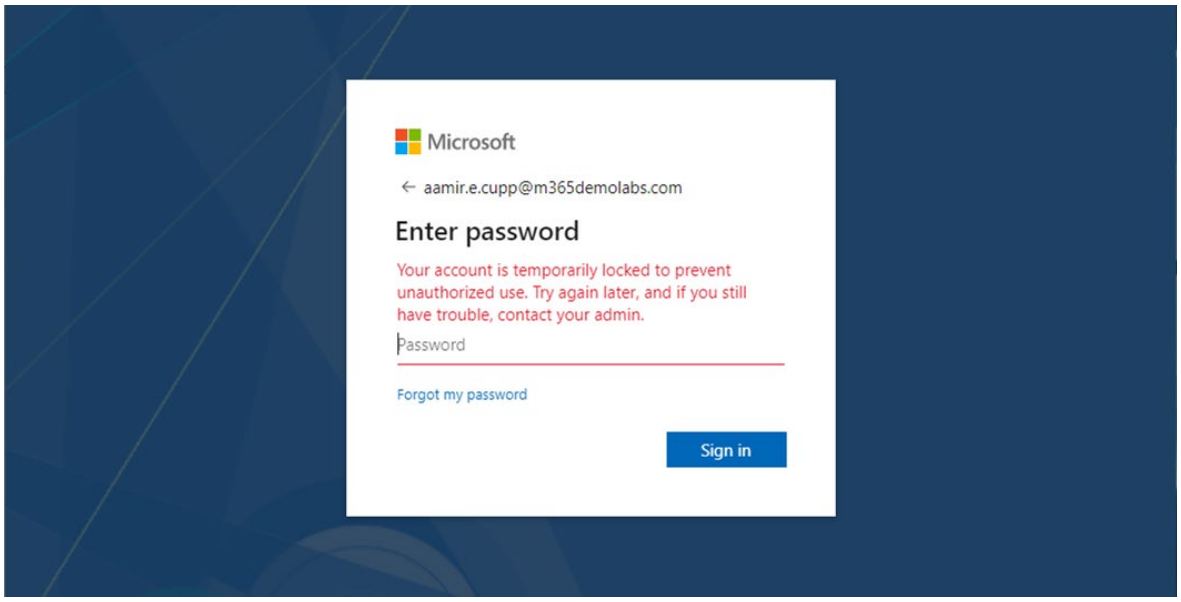

Figure 5.25 – Account lockout

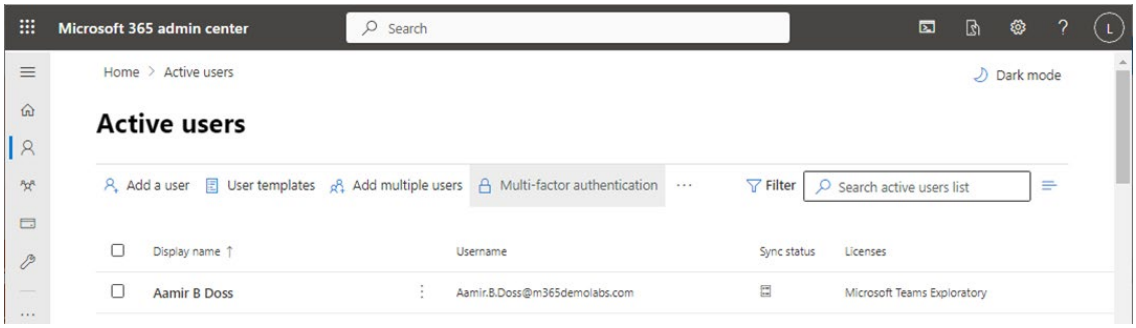

Figure 5.26 – Active users page

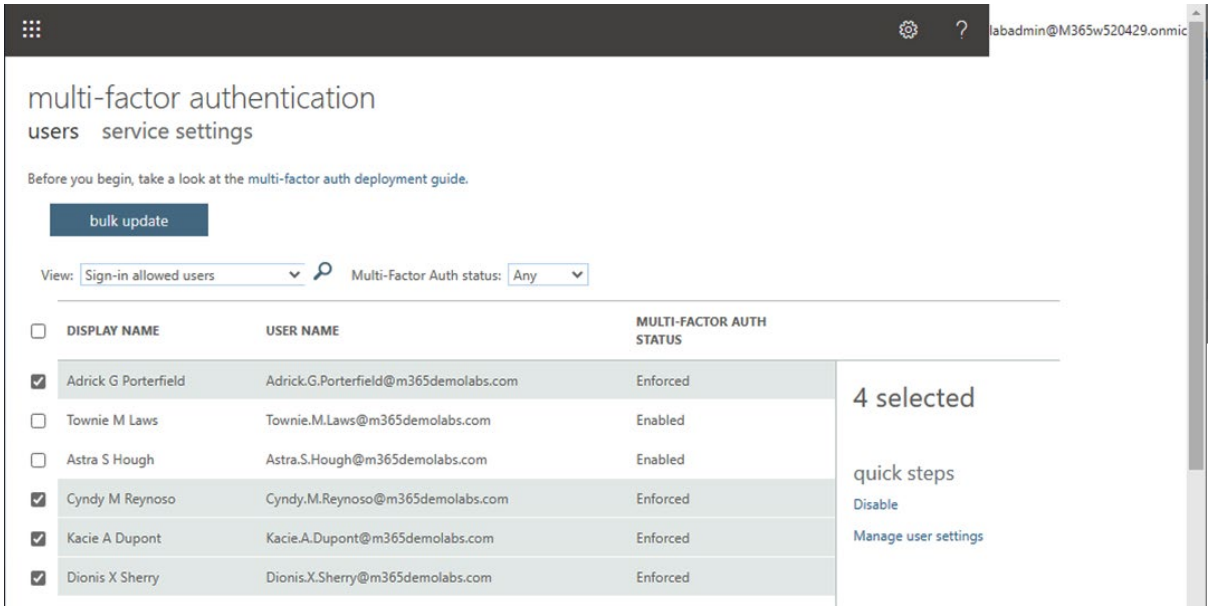

Figure 5.27 – Selecting users

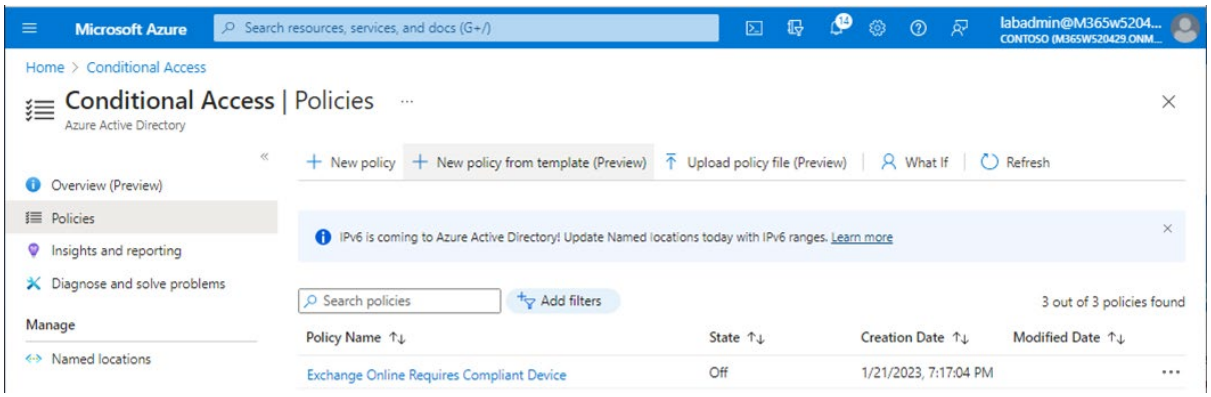

Figure 5.28 – Creating a new Conditional Access policy from a template

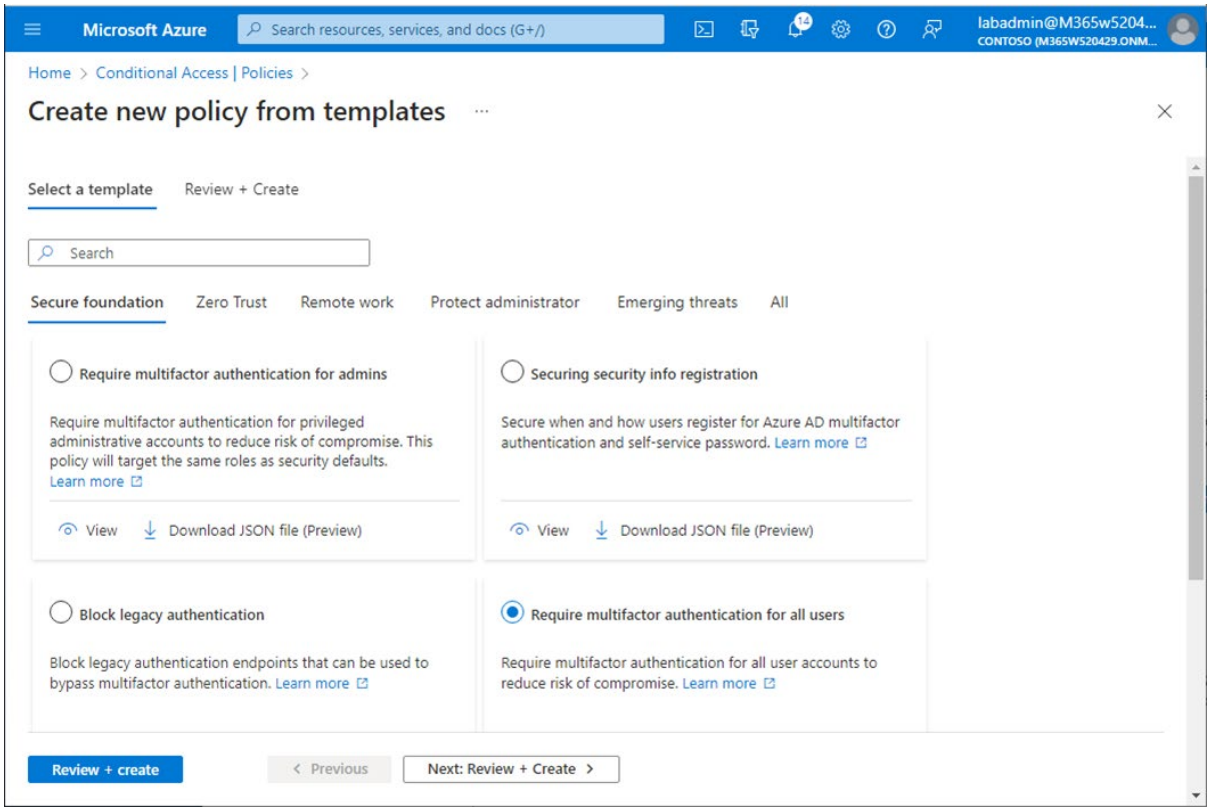

Figure 5.29 – Selecting a template

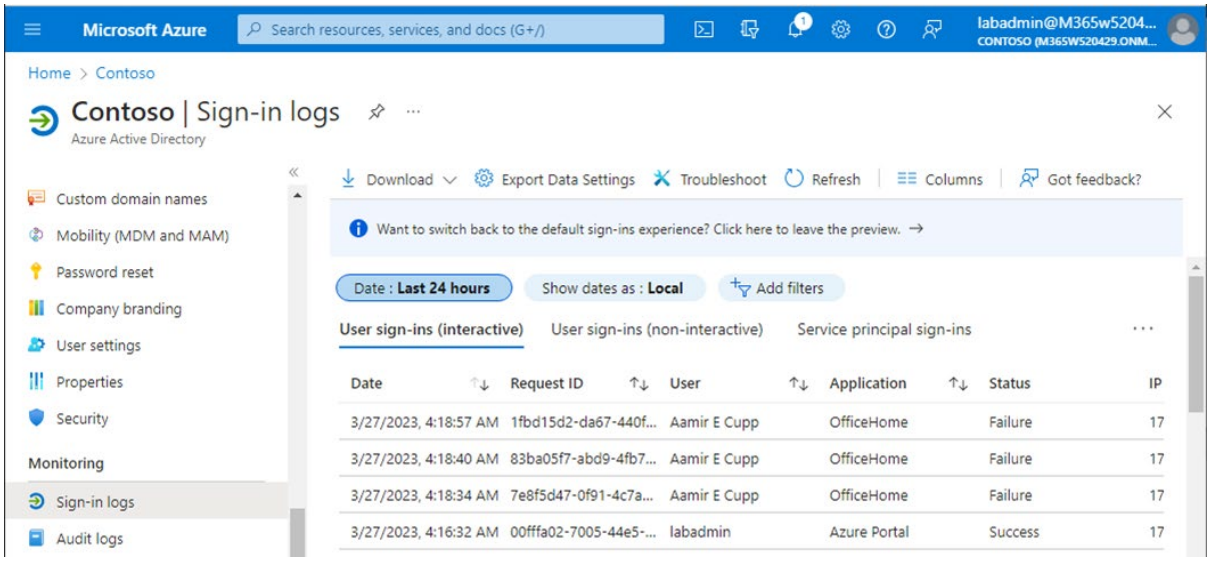

Figure 5.30 – Sign-in logs

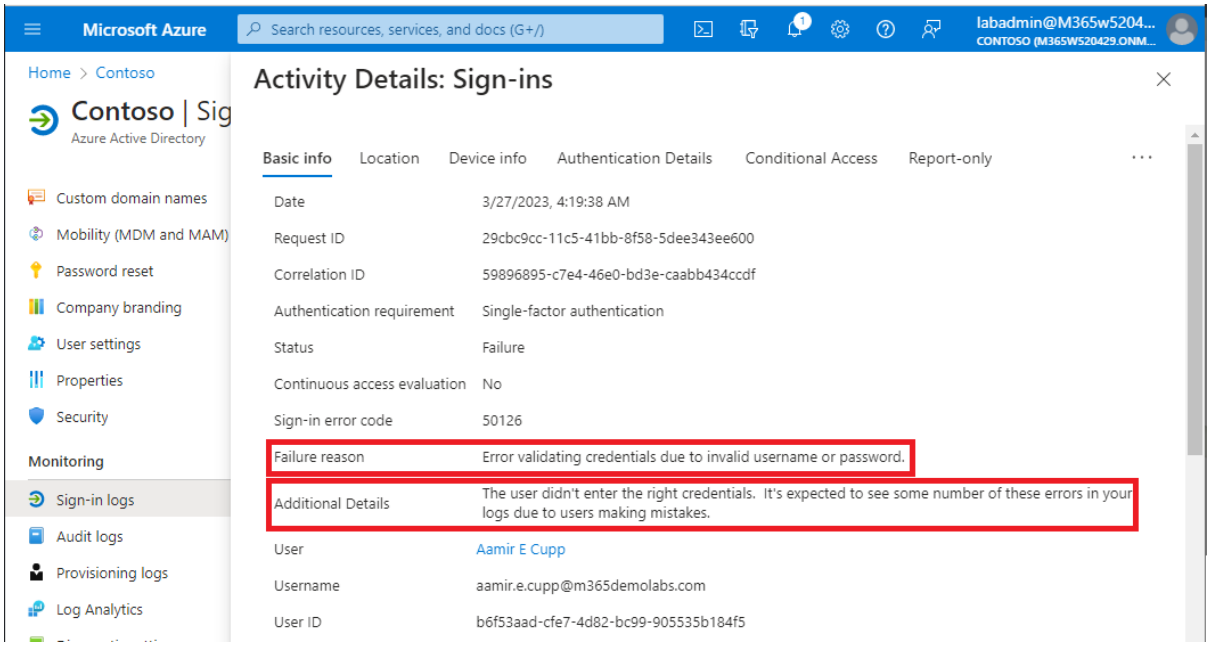

Figure 5.31 – Activity details

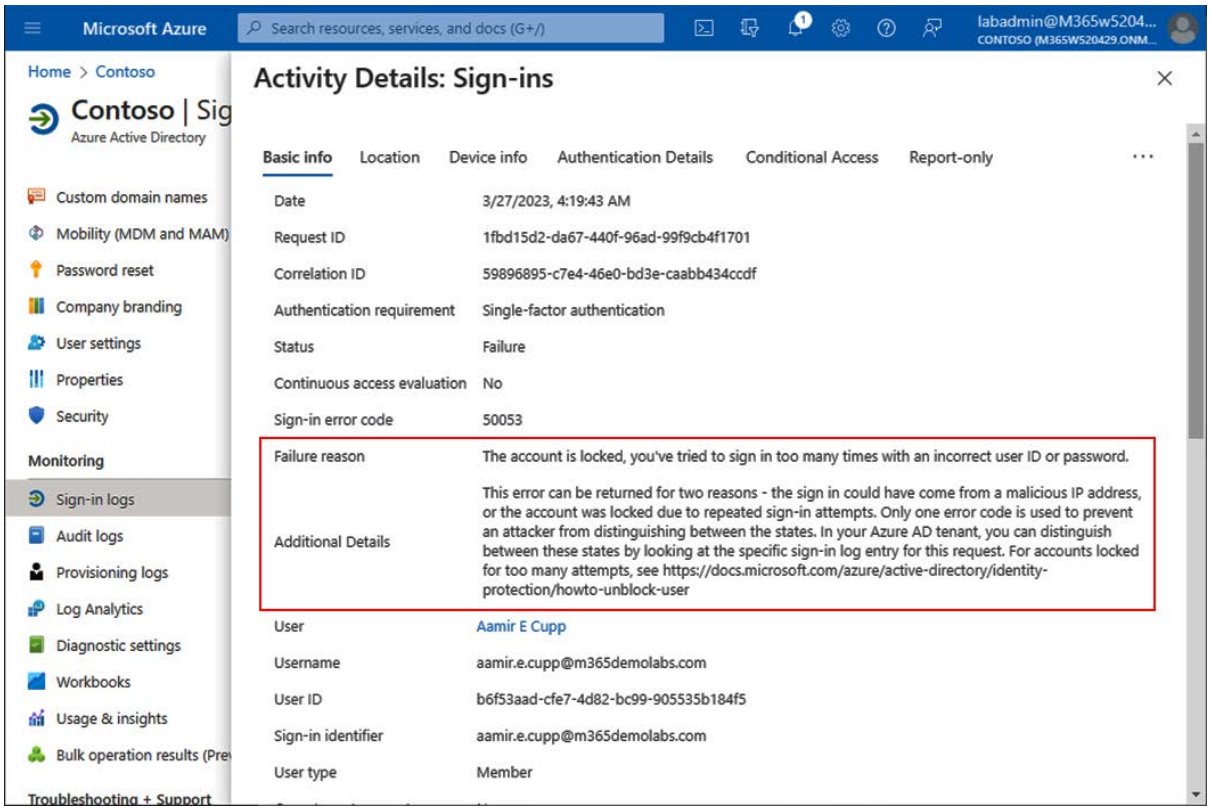

Figure 5.32 – Sign-in detail showing locked-out account

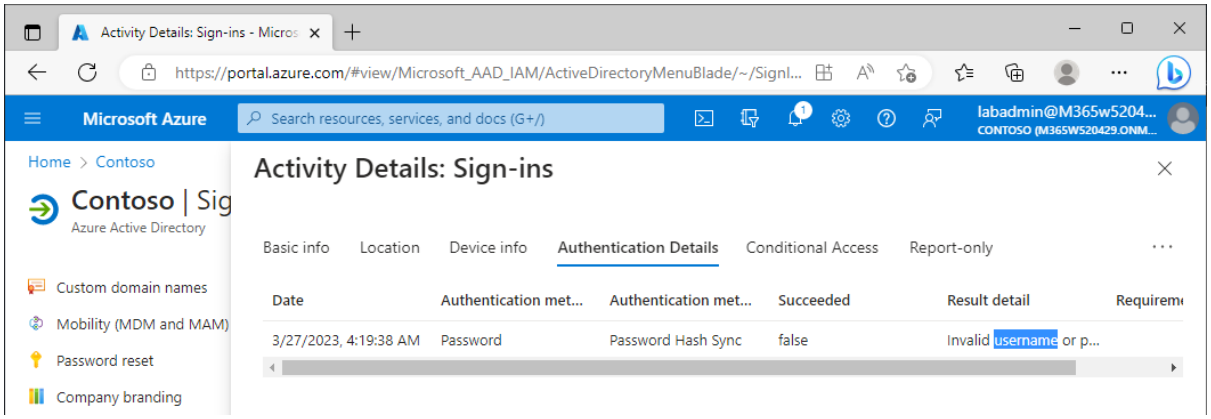

Figure 5.33 – Authentication details

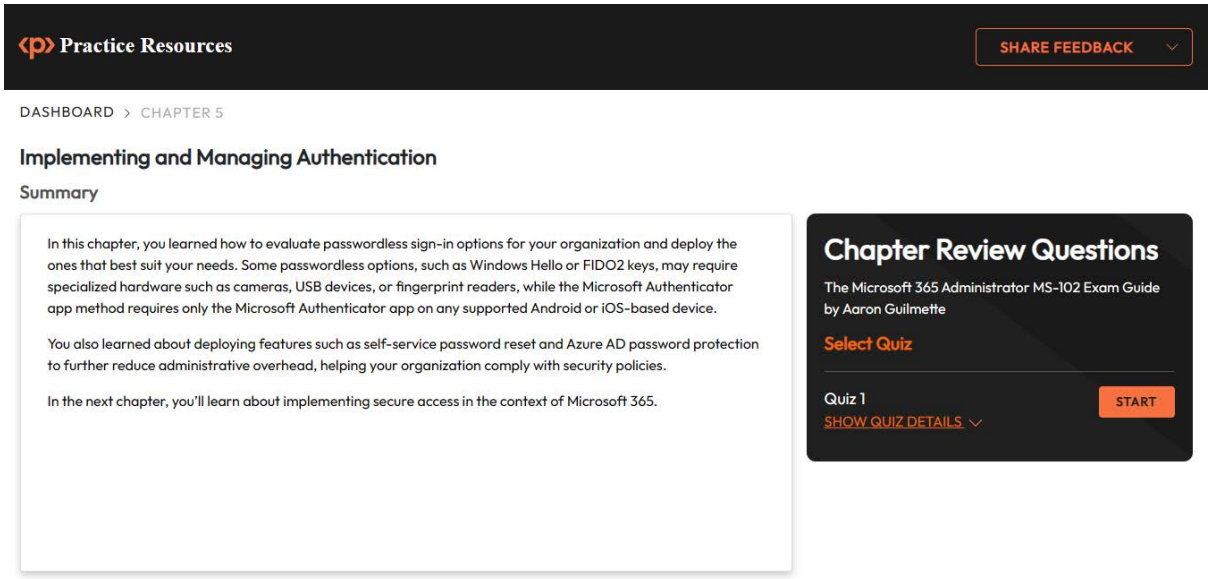

Figure 5.34 – Chapter Review Questions for Chapter 5

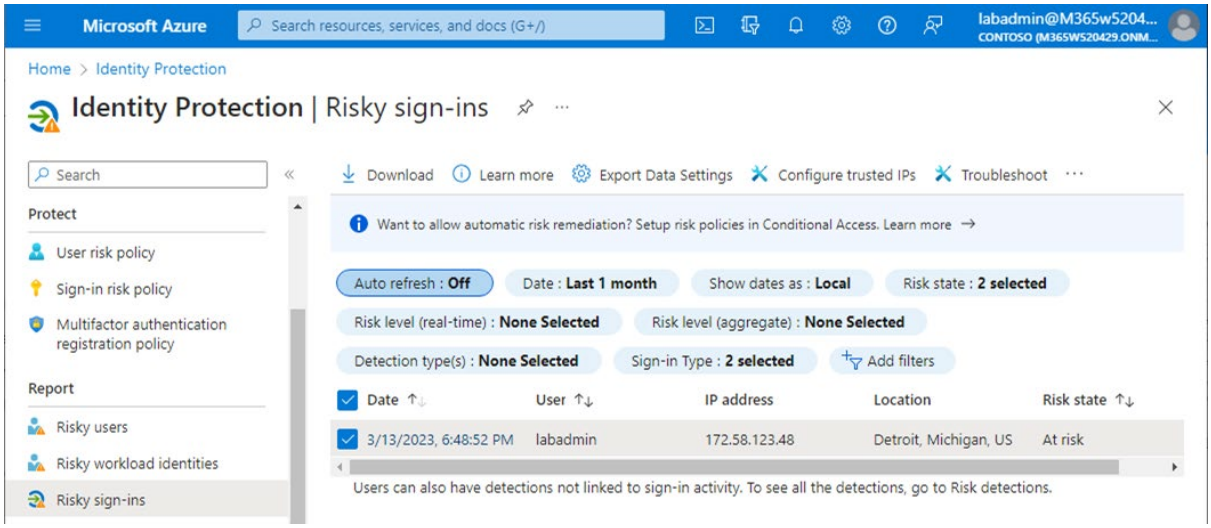

Figure 6.1 – Identity protection reports

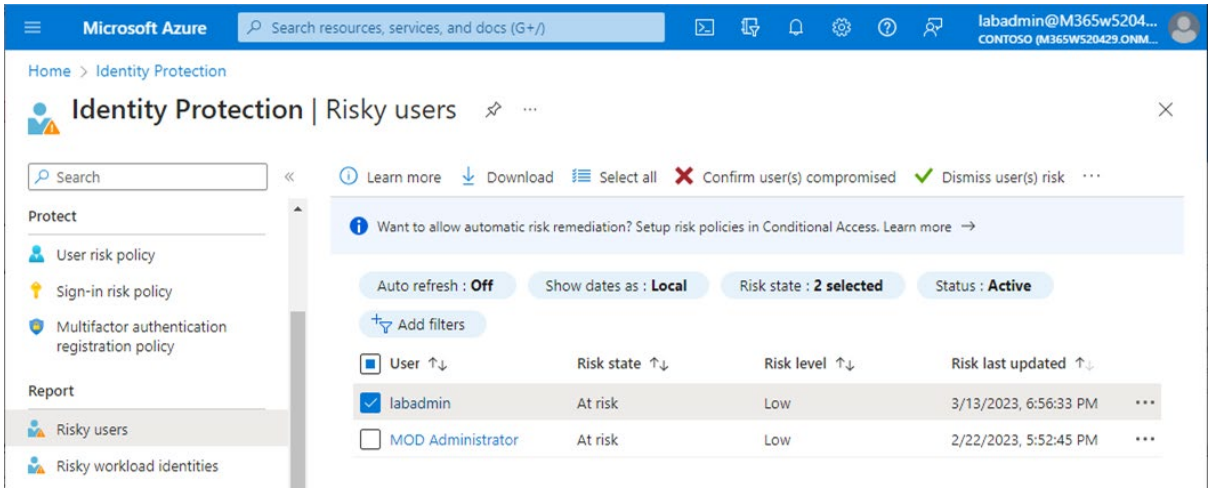

Figure 6.2 – Risky users report

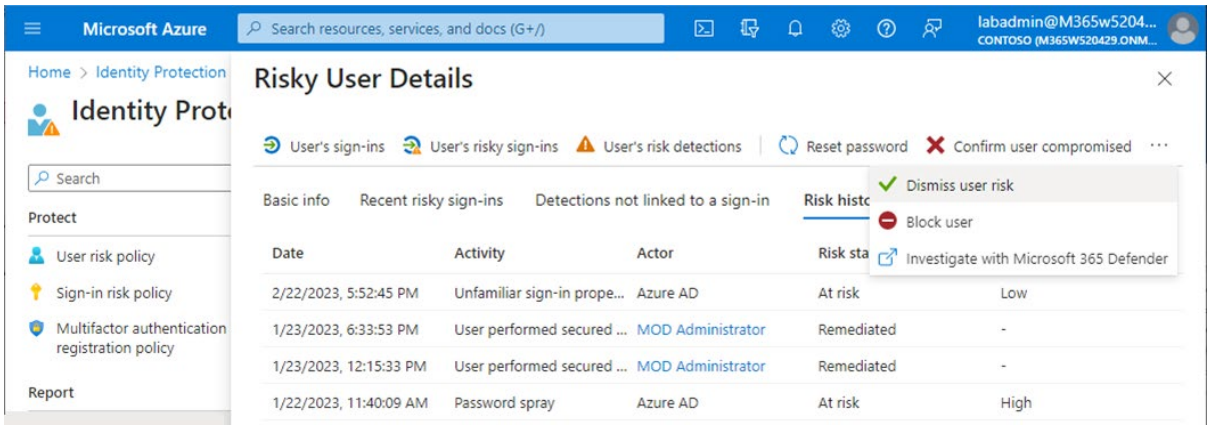

Figure 6.3 – Risky User Details pane

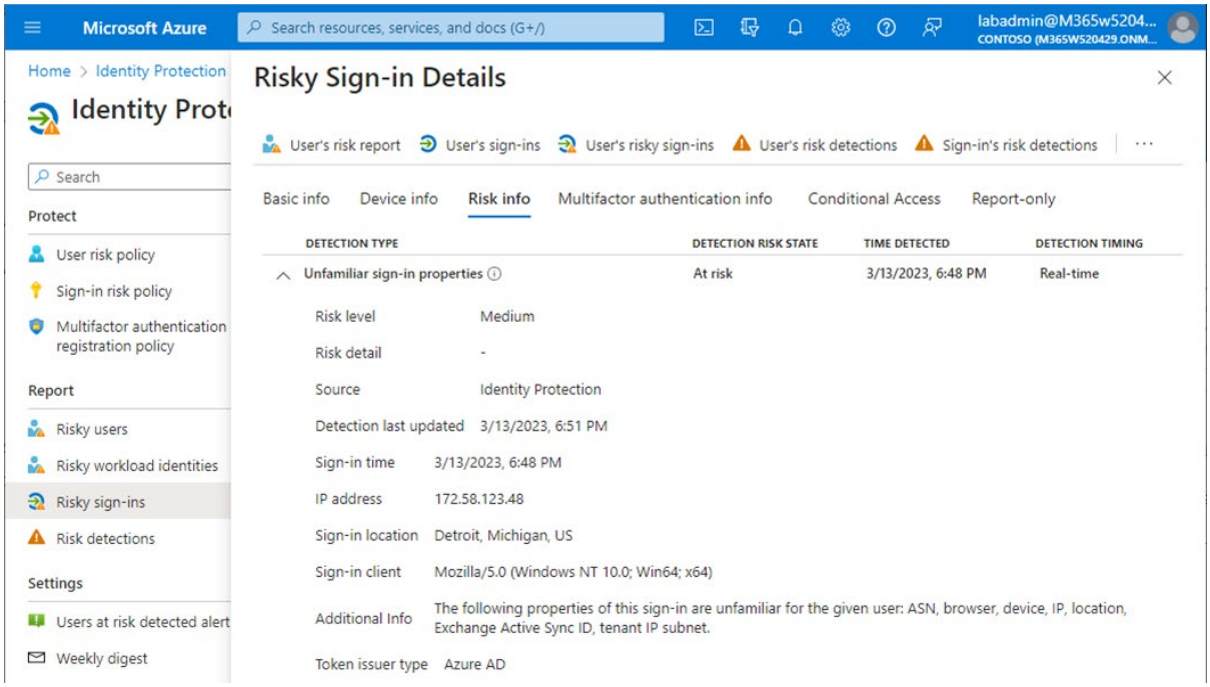

Figure 6.4 – Risky Sign-in Details page

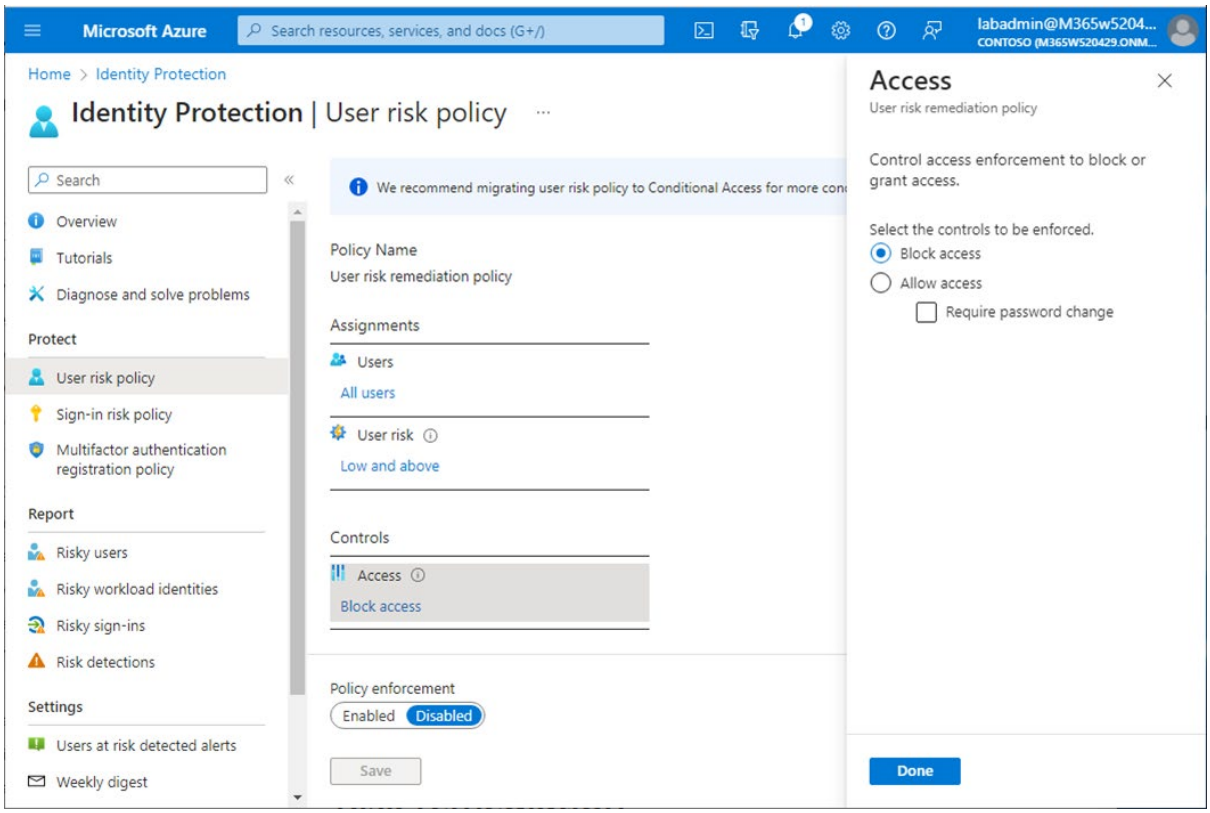

Figure 6.5 – User risk policy

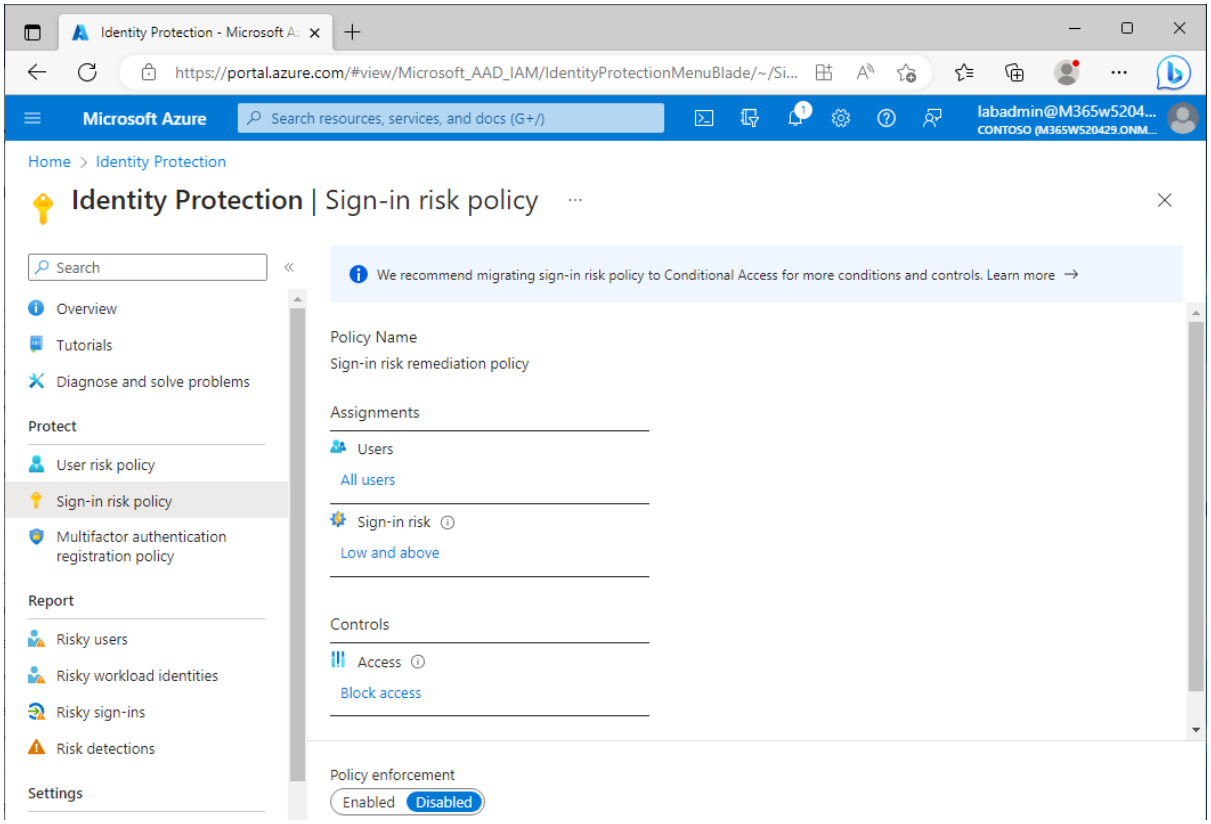

Figure 6.6 – Sign-in risk policy

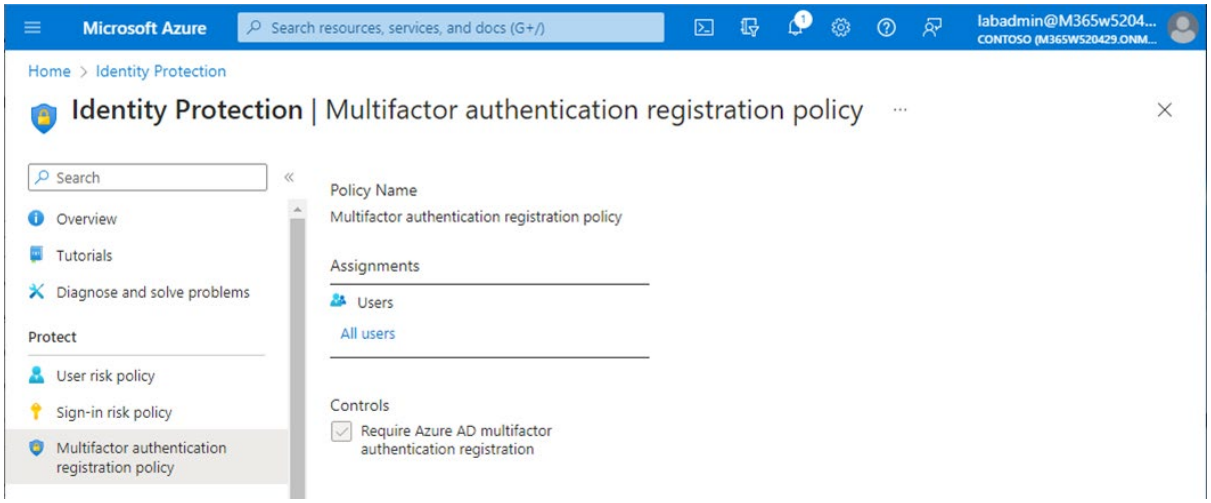

Figure 6.7 – Multifactor authentication registration policy

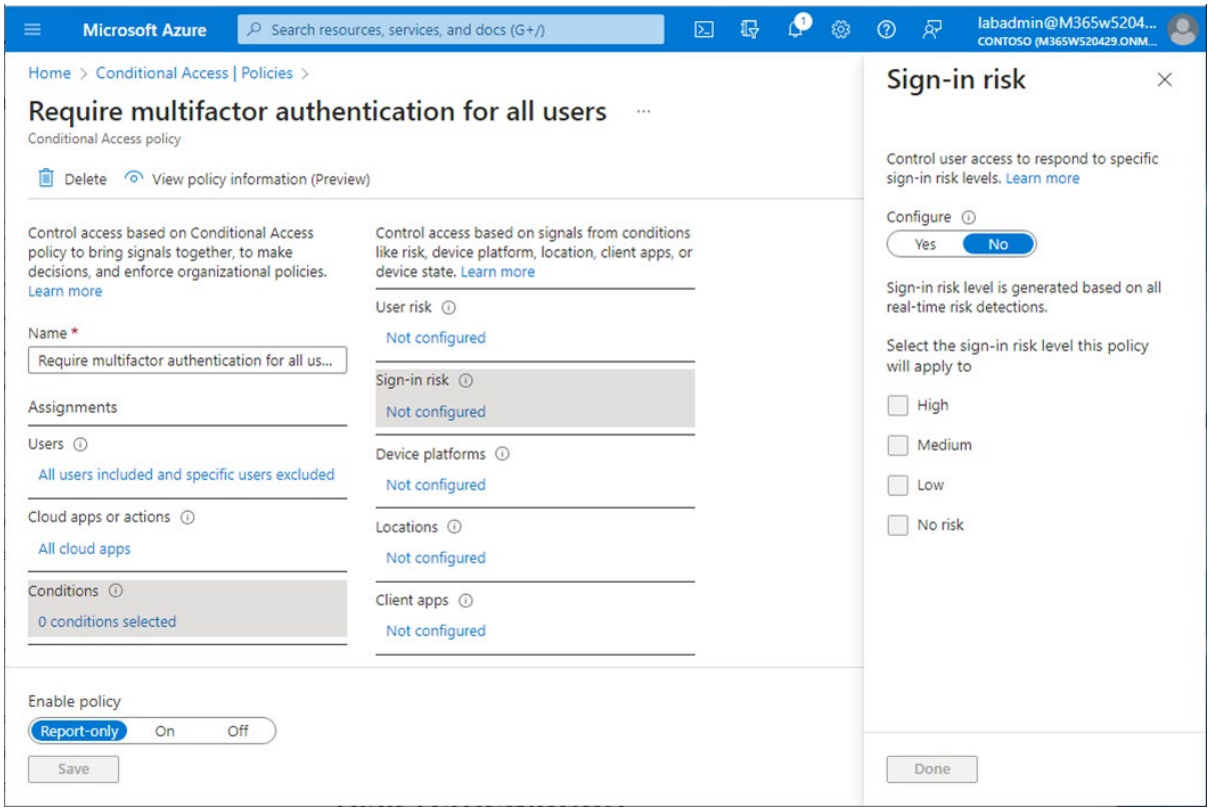

Figure 6.8 – Migrating Identity Protection policies to Conditional Access

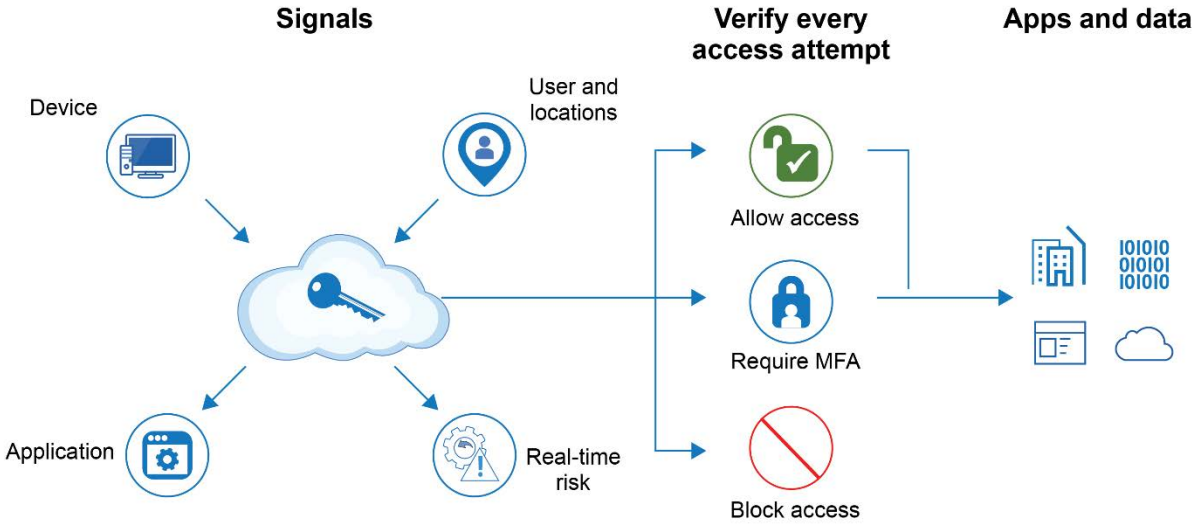

Figure 6.9 – Conditional Access signals

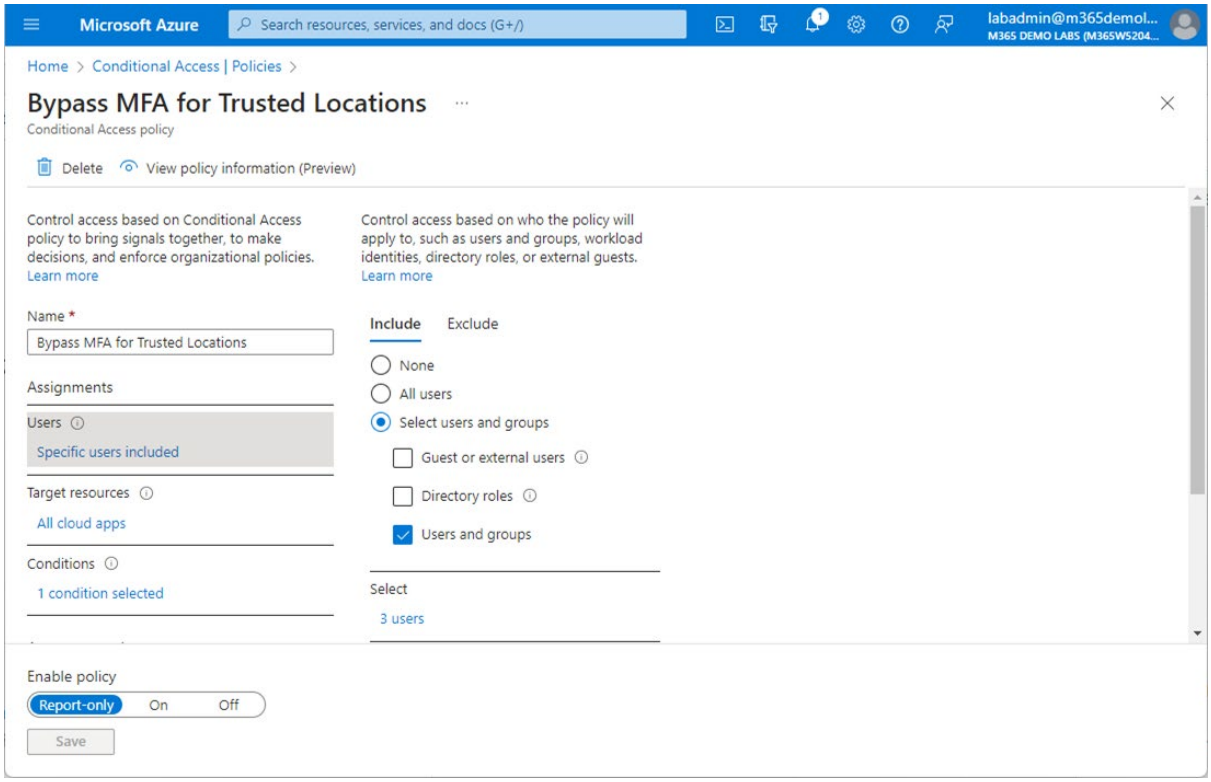

Figure 6.10 – Conditional Access policy user assignments

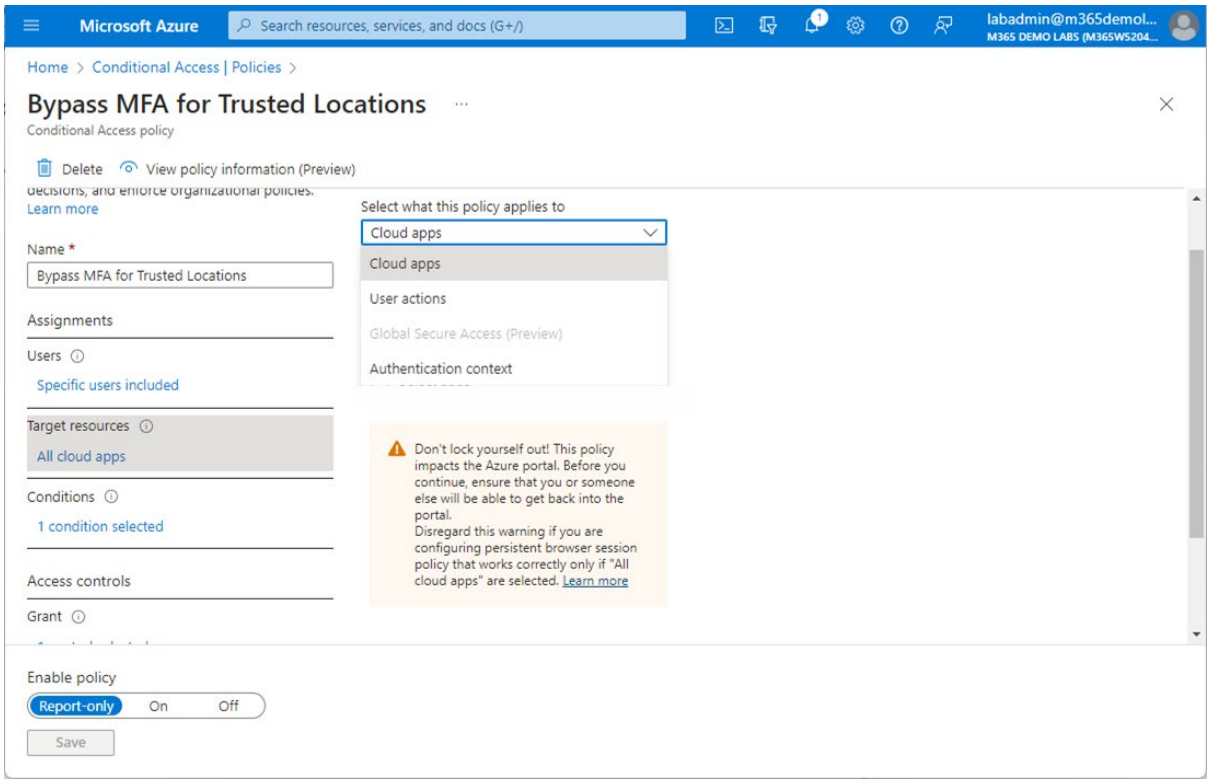

Figure 6.11 – Conditional Access policy target resources assignments

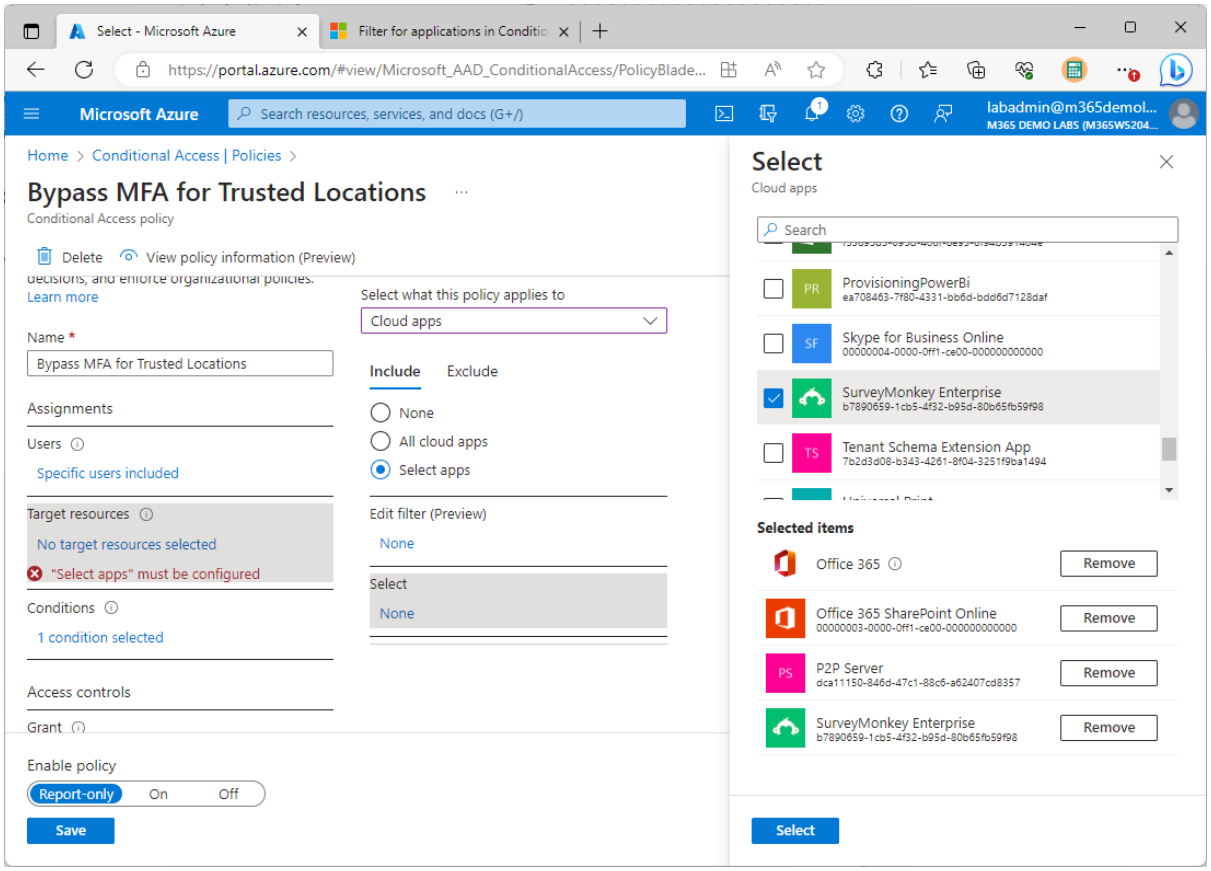

Figure 6.12 – Conditional Access policy cloud apps

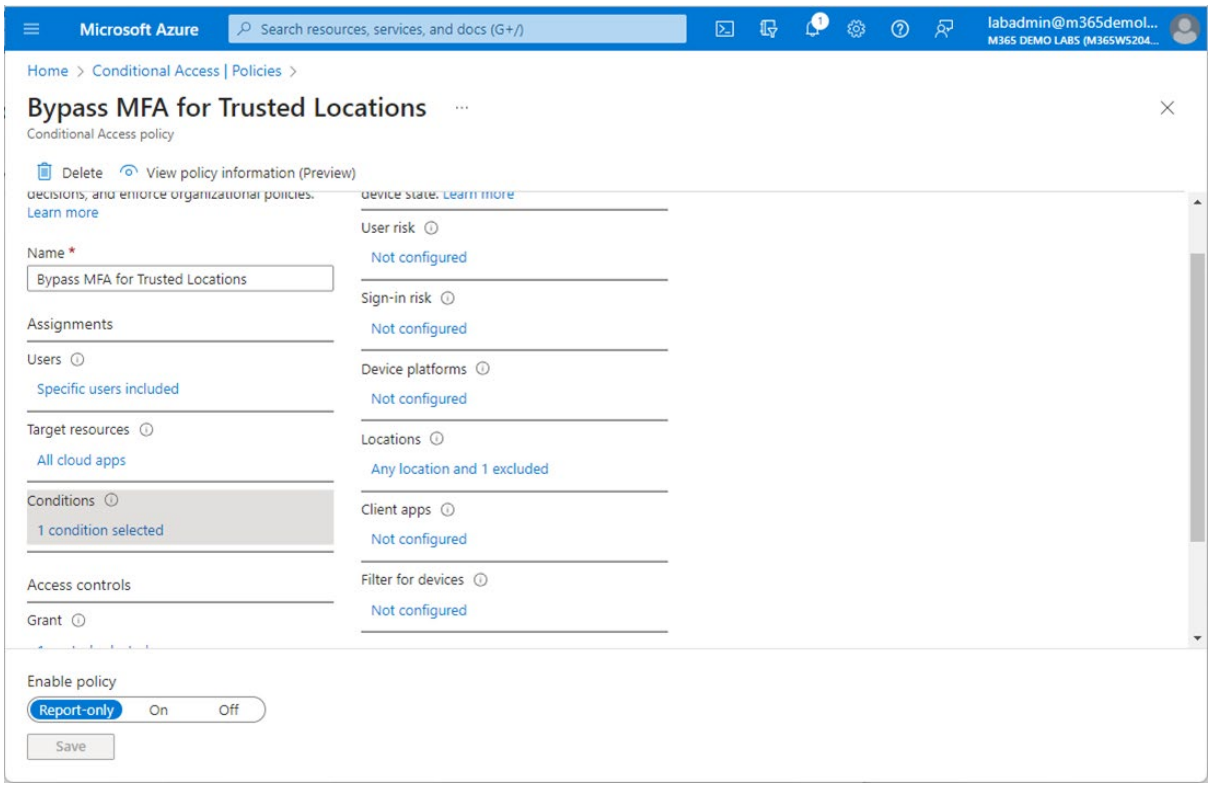

Figure 6.13 – Conditional Access policy conditions

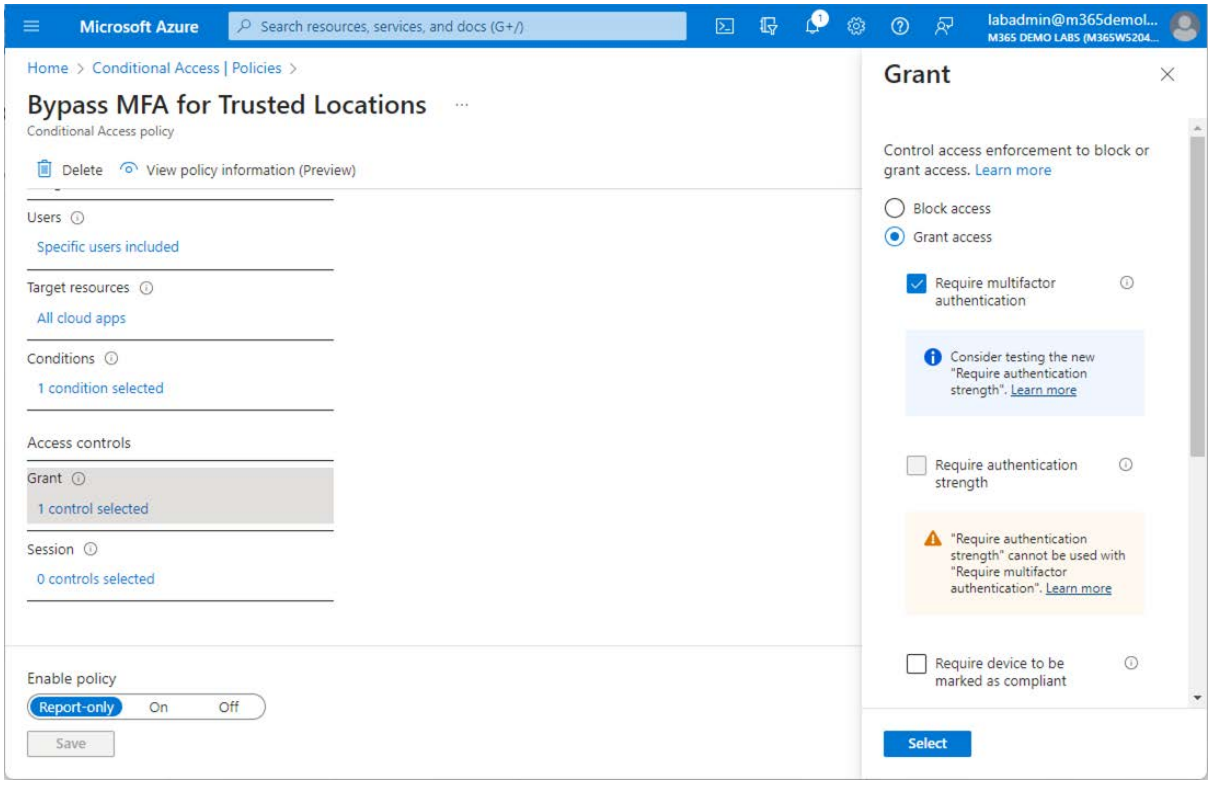

Figure 6.14 – Granting access control with the Conditional Access policy

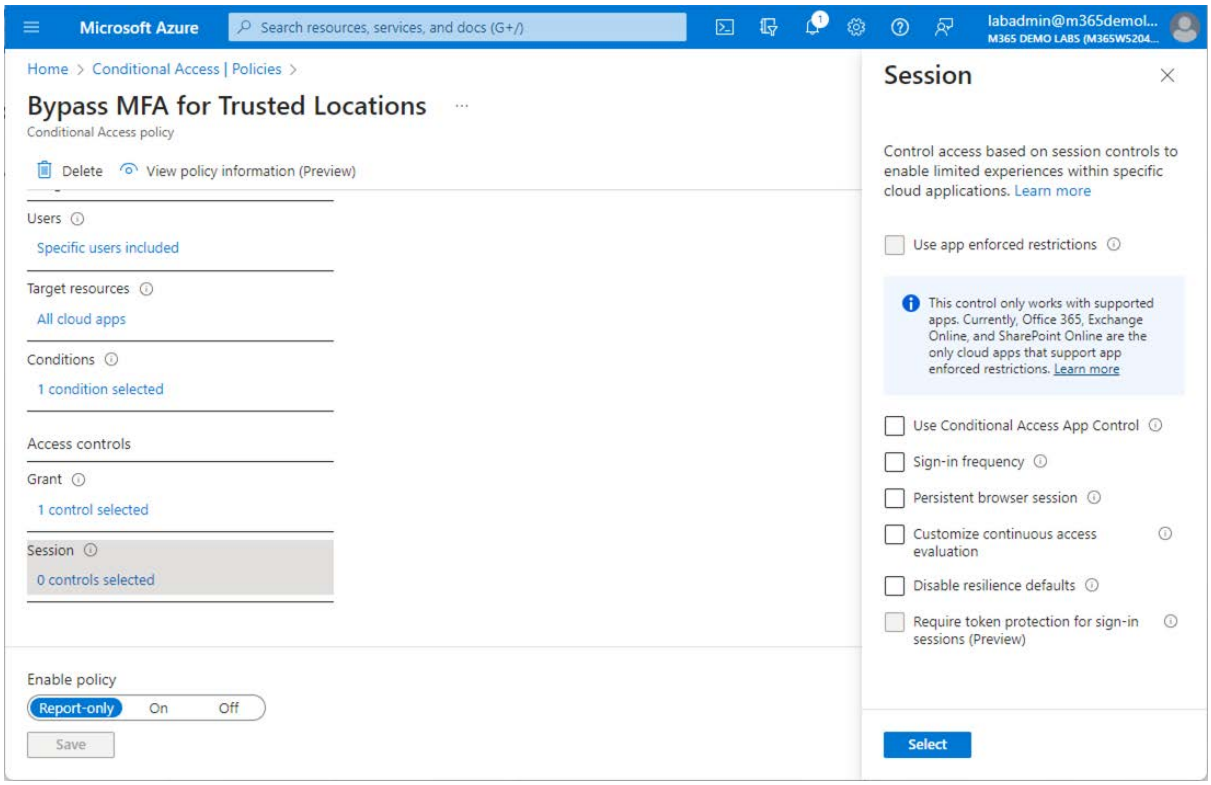

Figure 6.15 – Conditional Access policy session controls

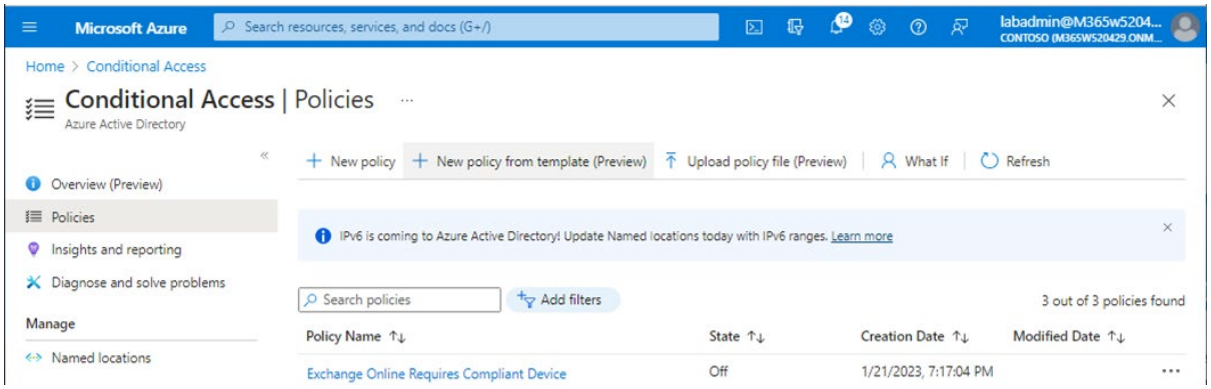

Figure 6.16 – Creating a new Conditional Access policy from a template

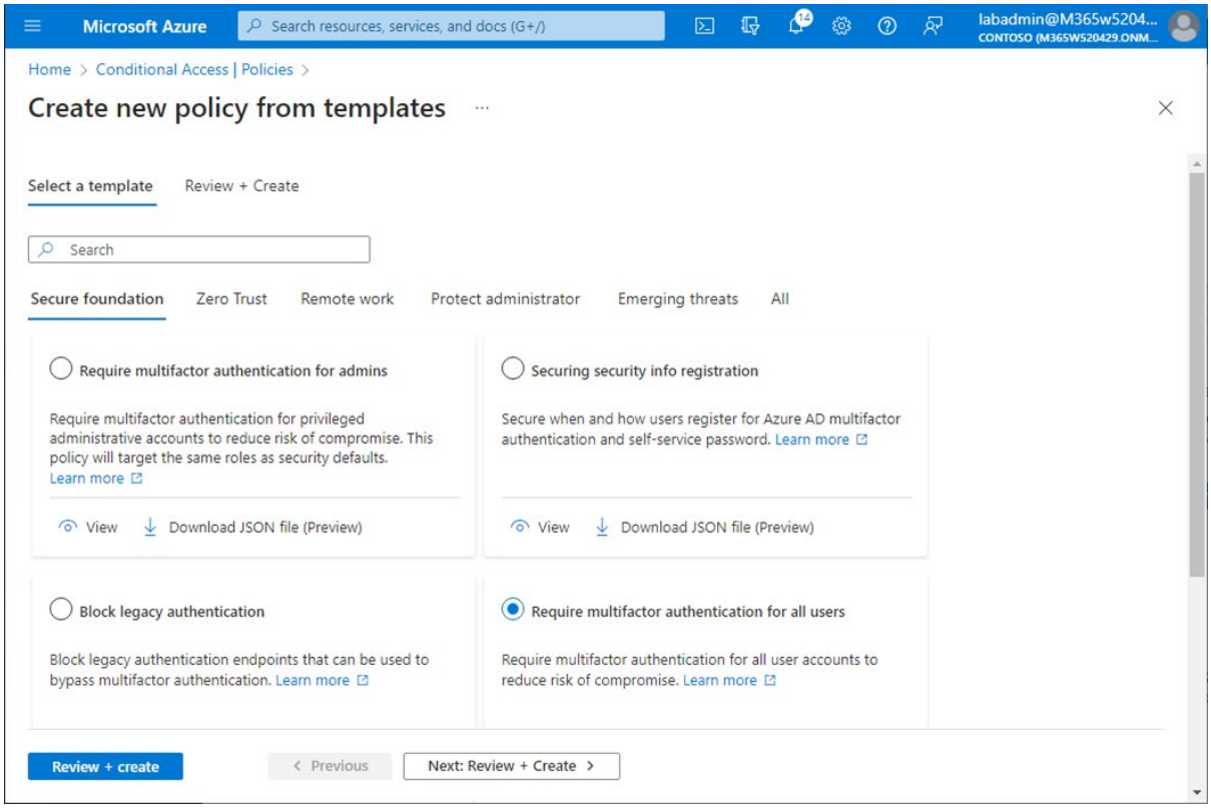

Figure 6.17 – Selecting a template

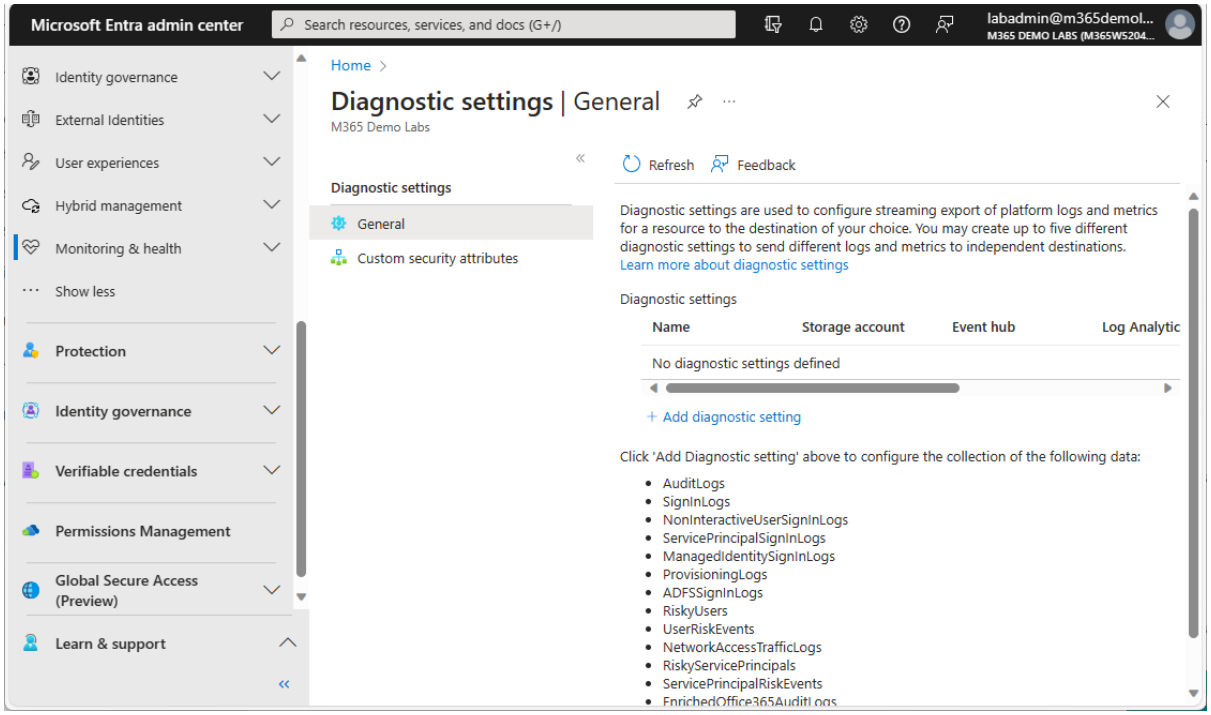

Figure 6.18 – Entra ID Diagnostic settings page

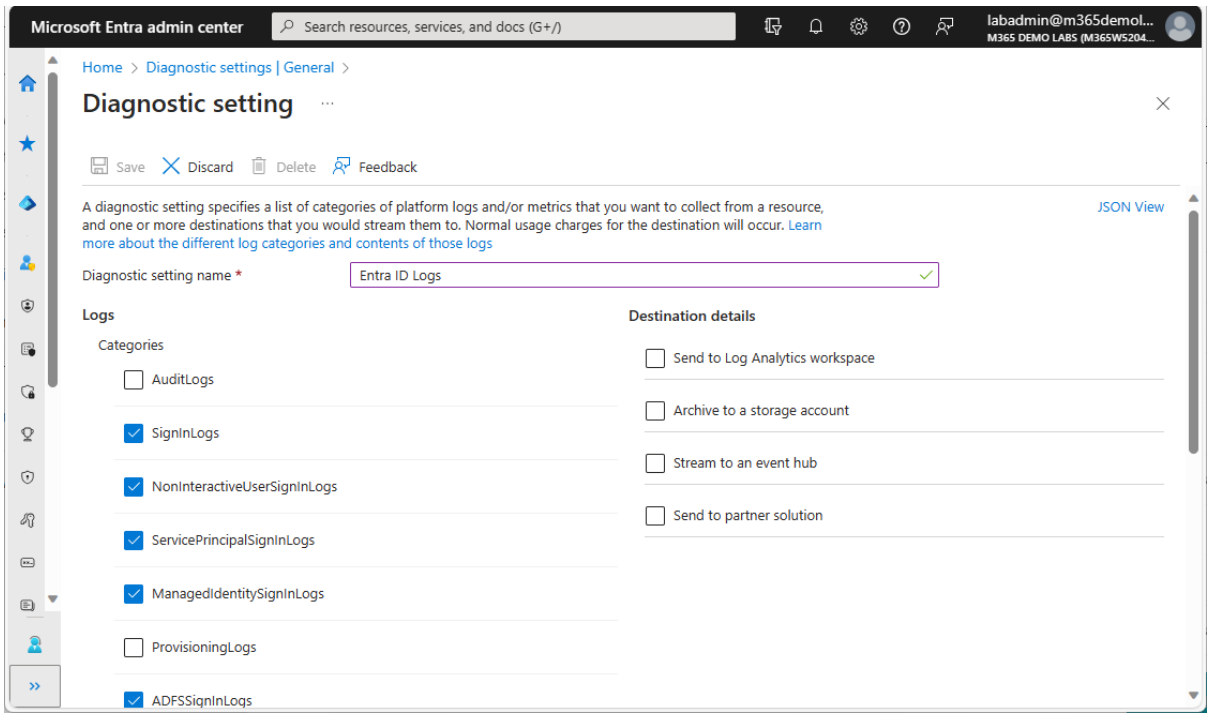

Figure 6.19 – Selecting log categories

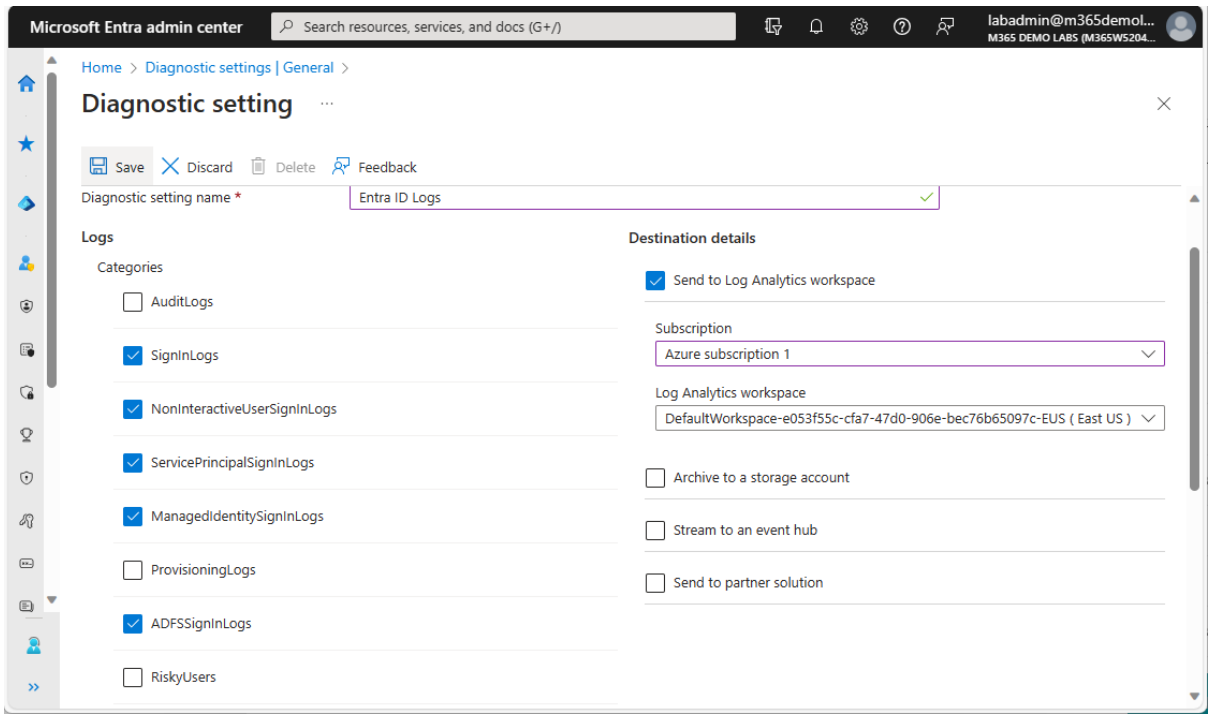

Figure 6.20 – Selecting the destination

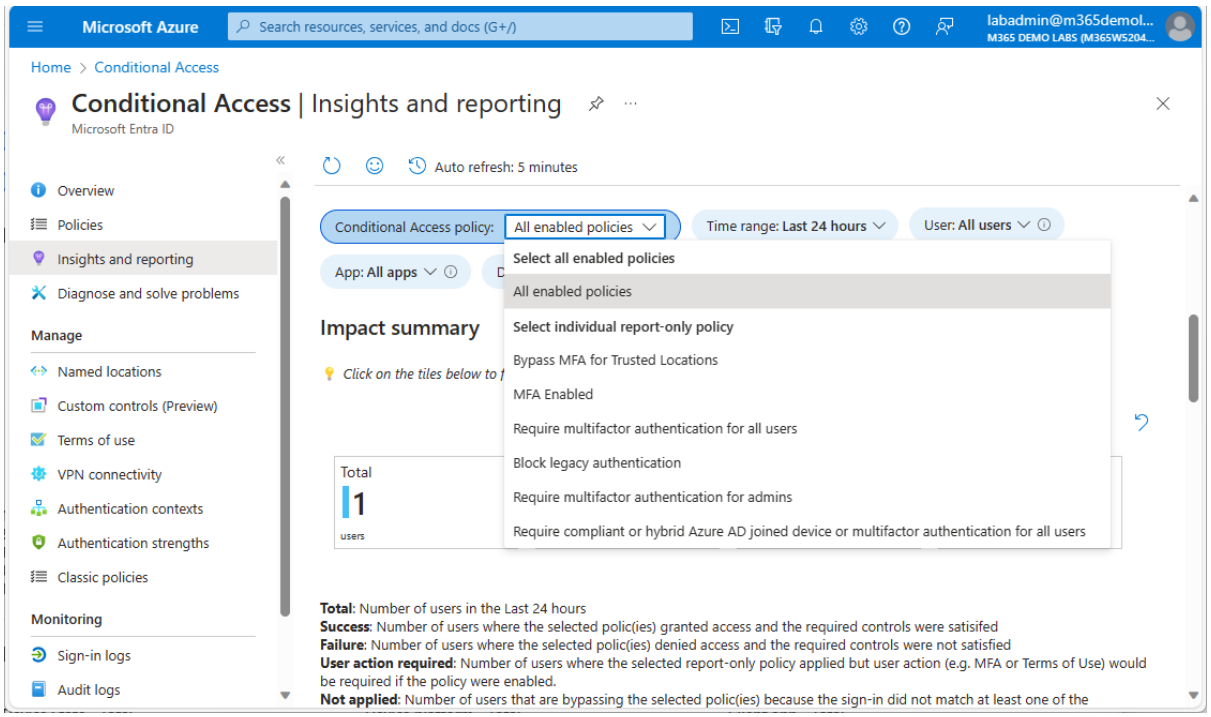

Figure 6.21 – Setting filters to display data

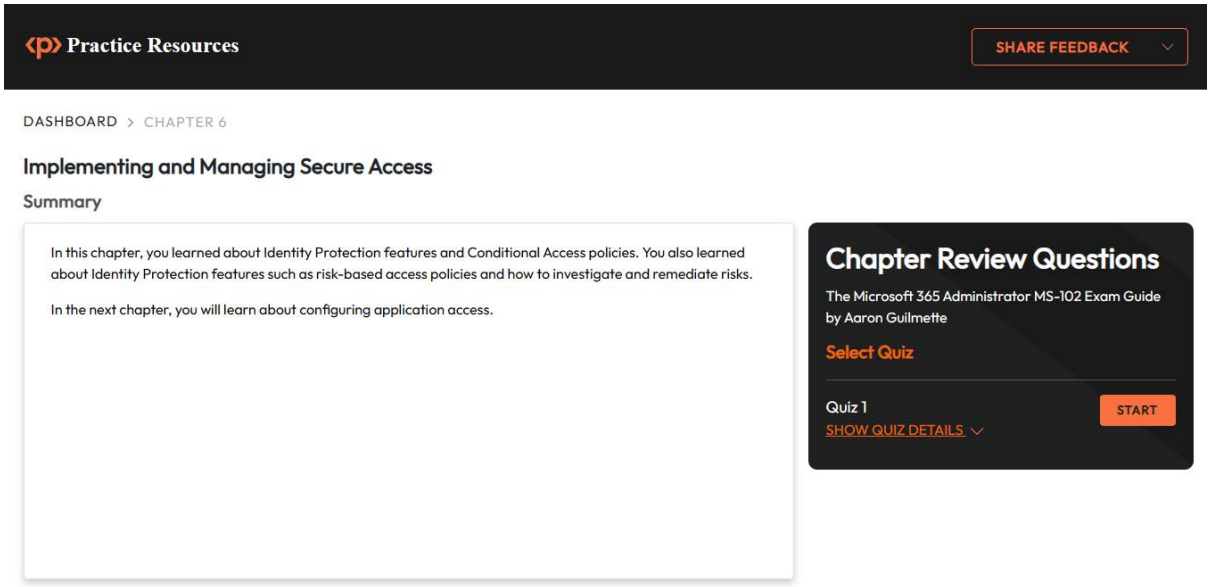

Figure 6.22 – Chapter Review Questions for Chapter 6

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

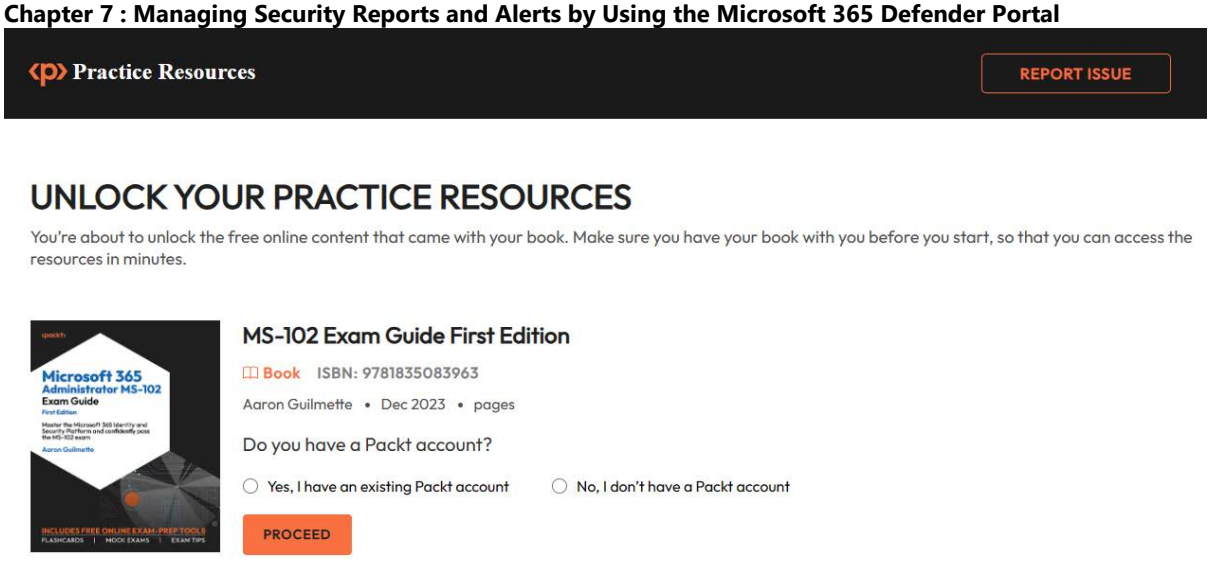

Figure 7.1 – Unlock page for MS-102 Exam Guide First Edition Practice Resources

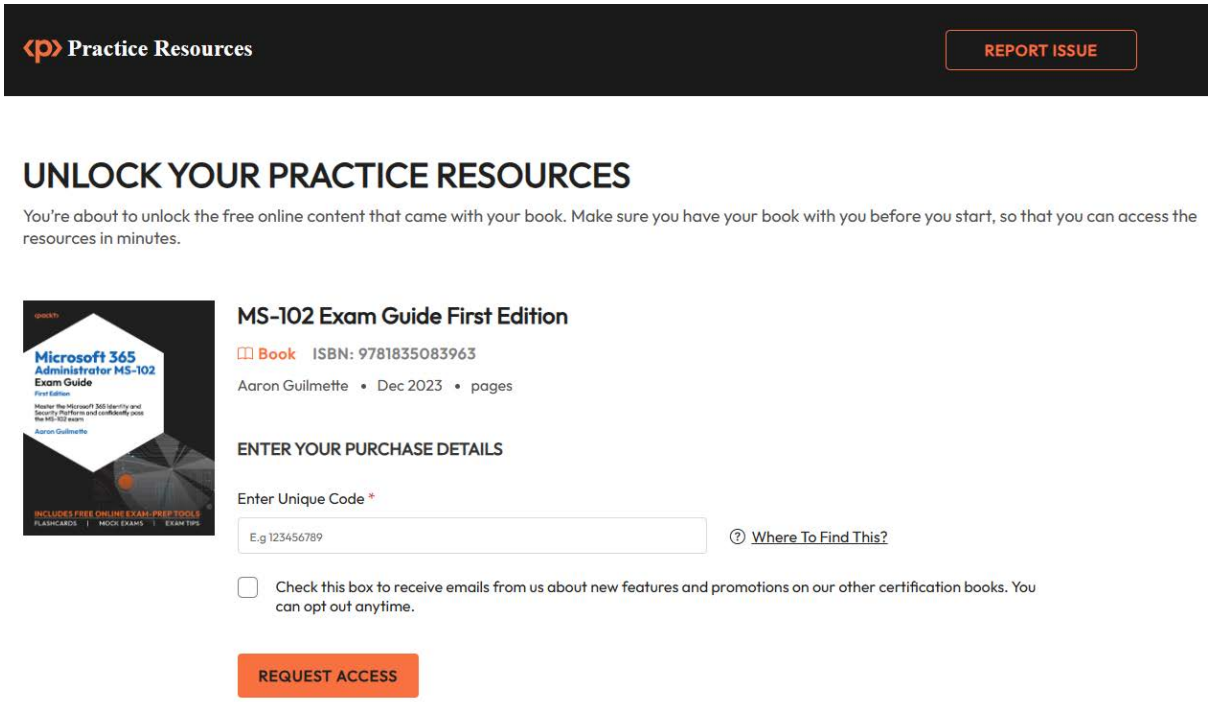

Figure 7.2 – Enter your unique sign-up code to unlock the resources

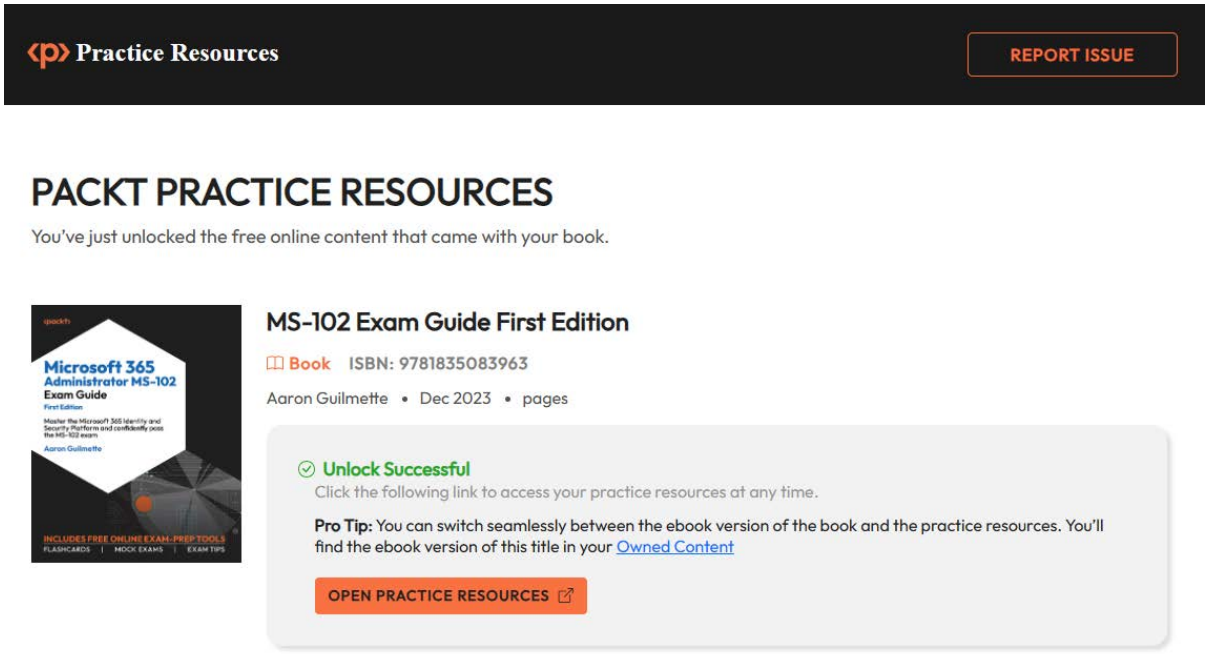

Figure 7.3 – Page that shows up when you've successfully unlocked the free online content

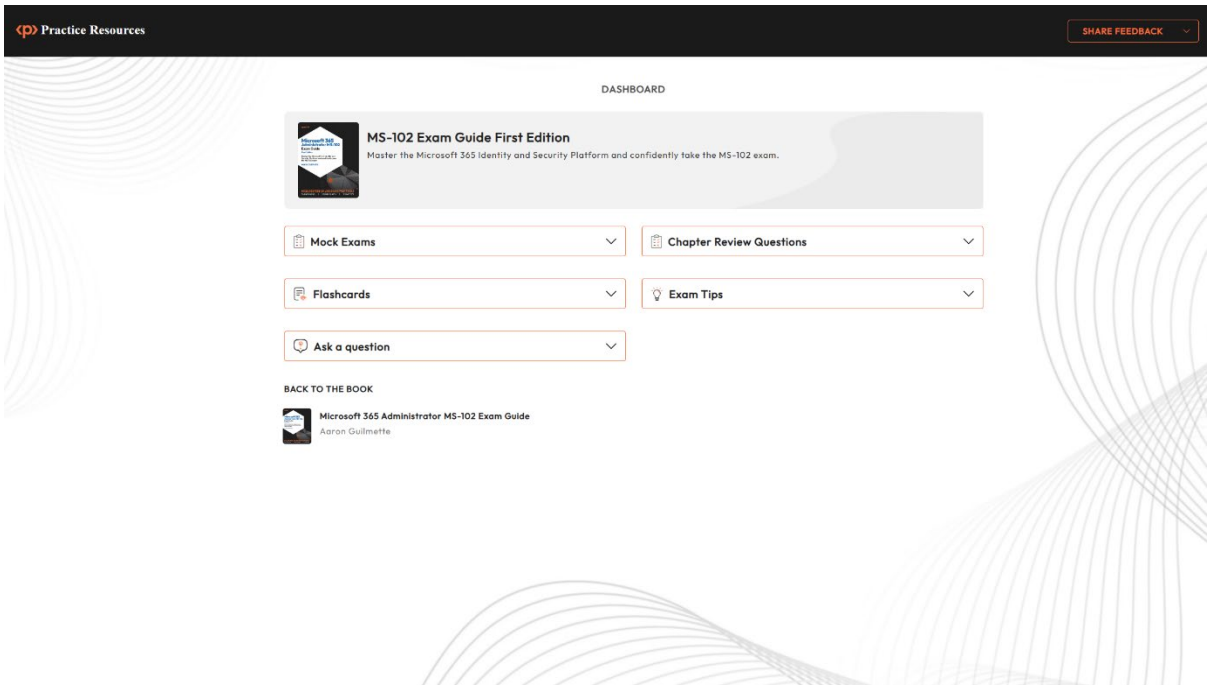

Figure 7.4 – Dashboard page upon successful unlock of practice resources

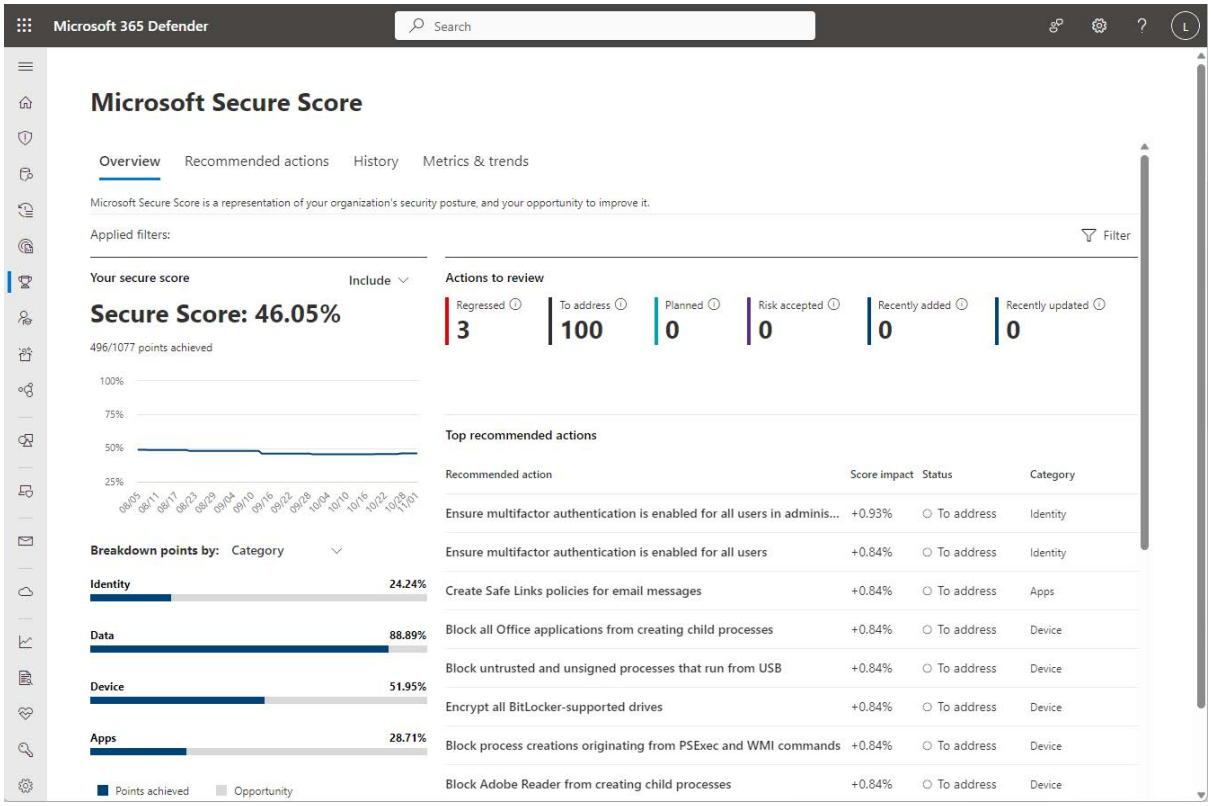

Figure 7.5 – Microsoft Secure Score

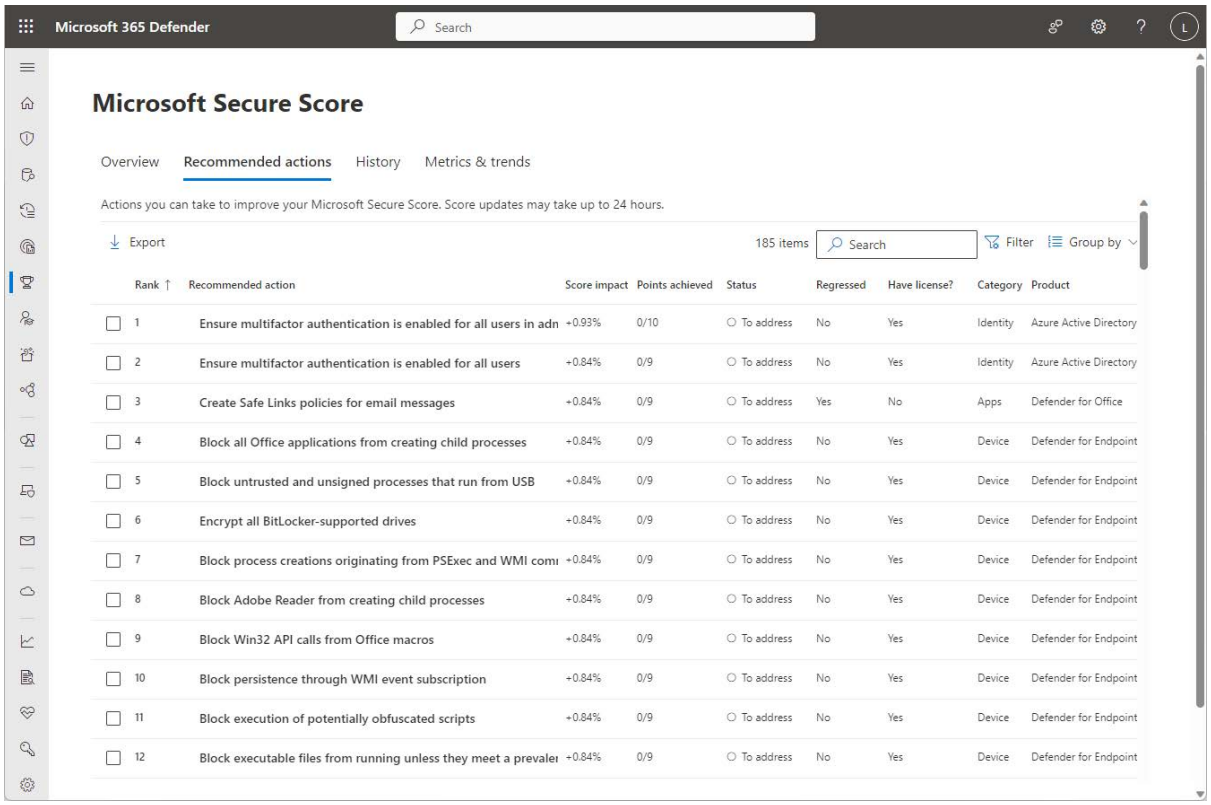

Figure 7.6 – Microsoft Secure Score improvement actions

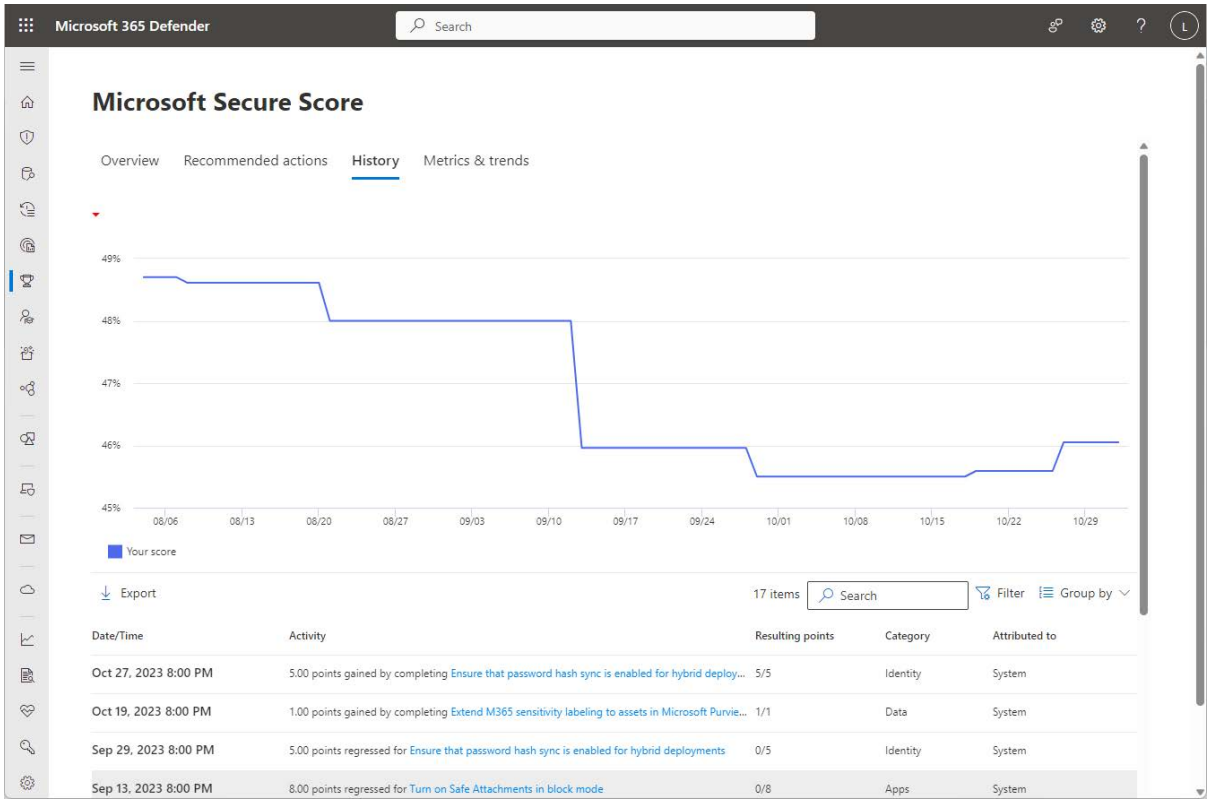

Figure 7.7 – Viewing the Secure Score history

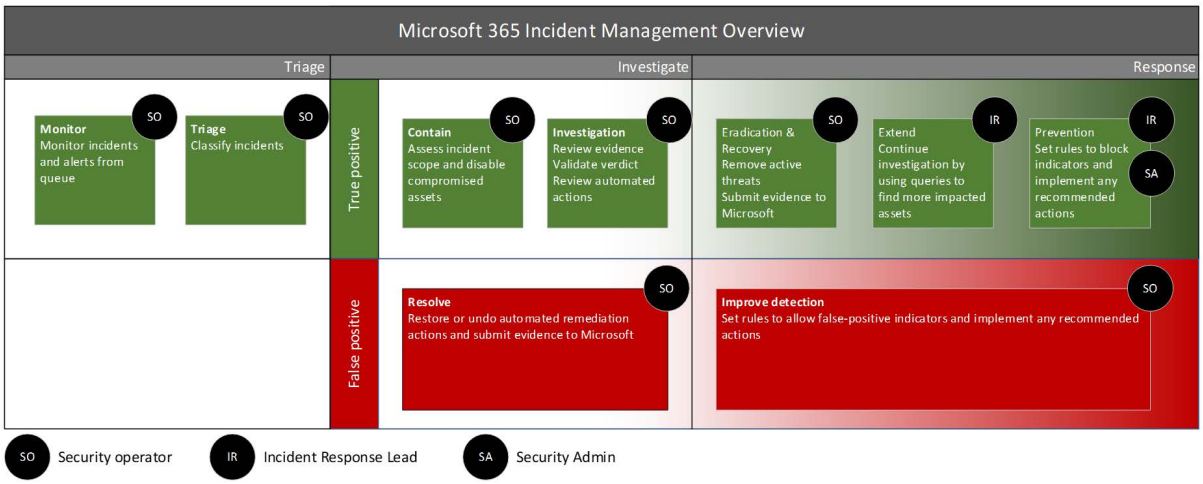

Figure 7.8 – The Microsoft 365 Incident Management phases

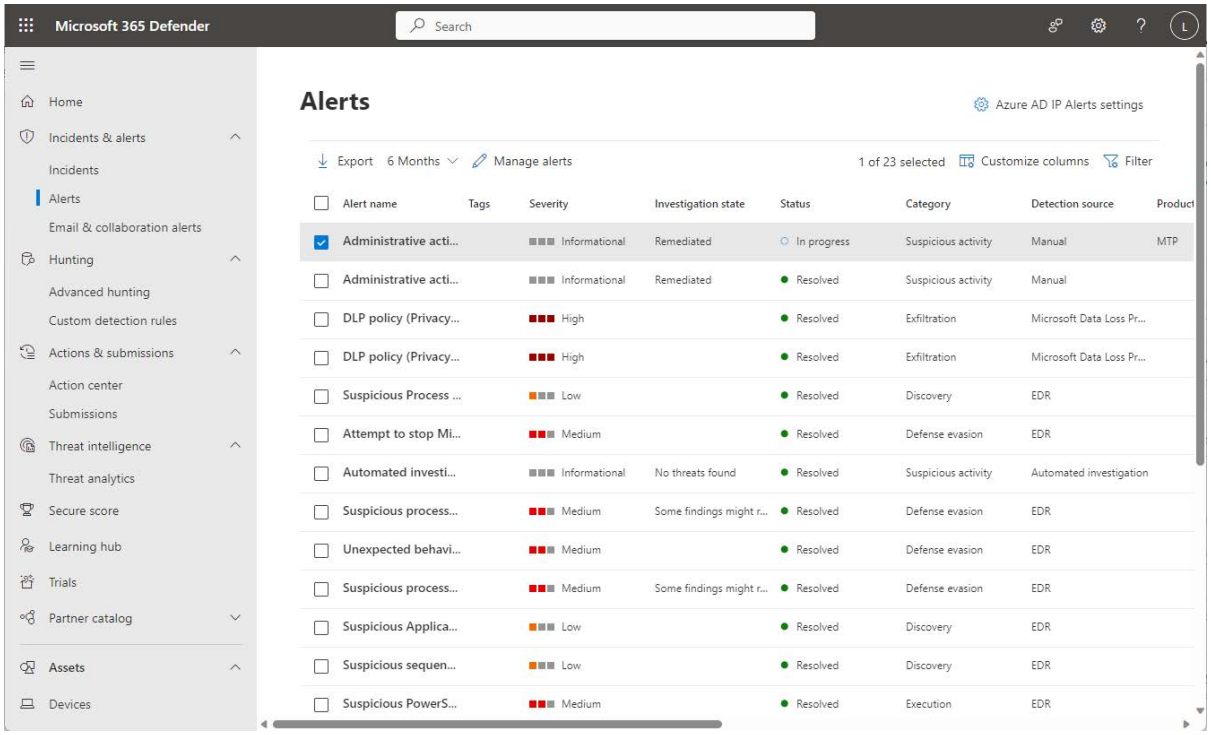

Figure 7.09 – Viewing the Alerts page in the Microsoft 365 Defender portal

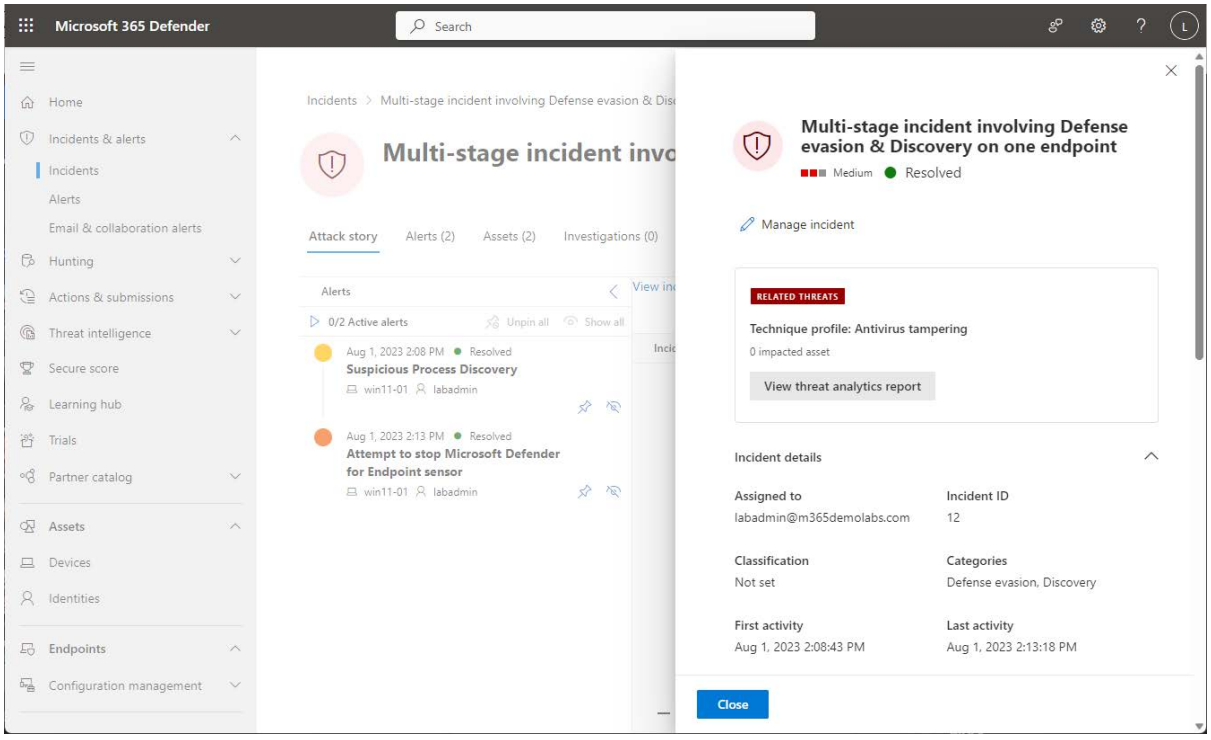

Figure 7.10 – Reviewing an incident

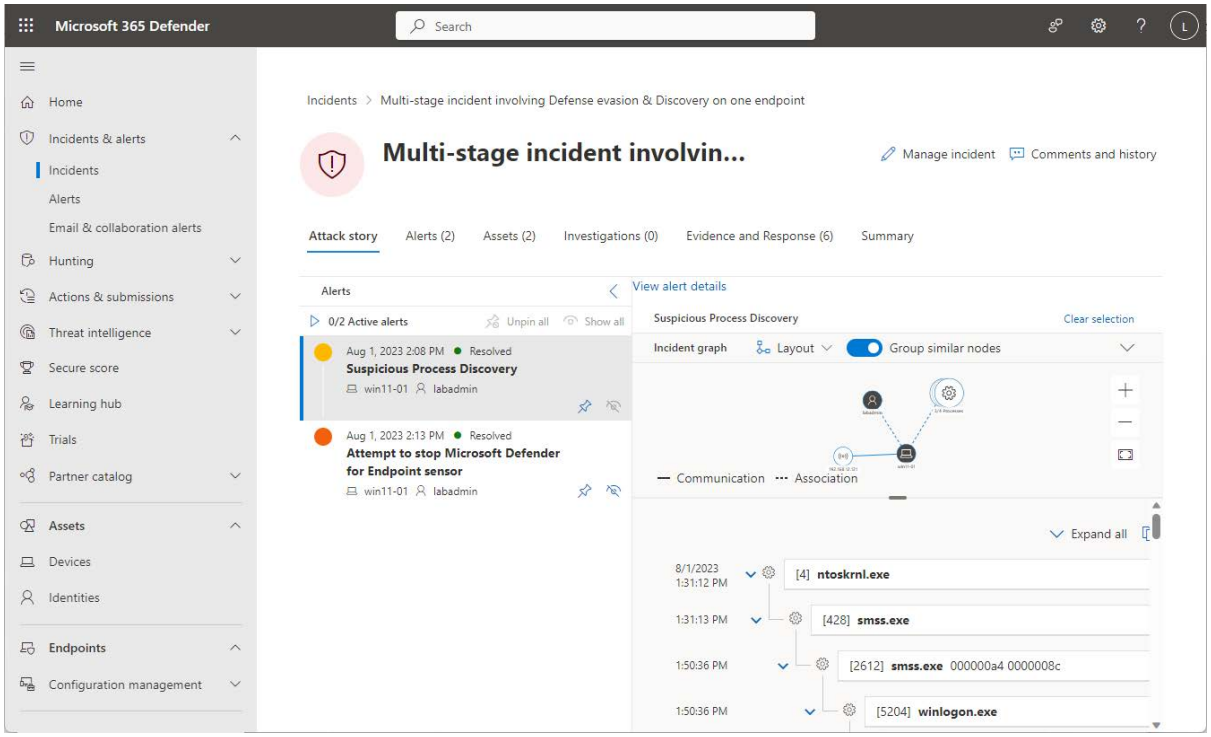

Figure 7.11 – Reviewing the Incident graph as part of an Attack story

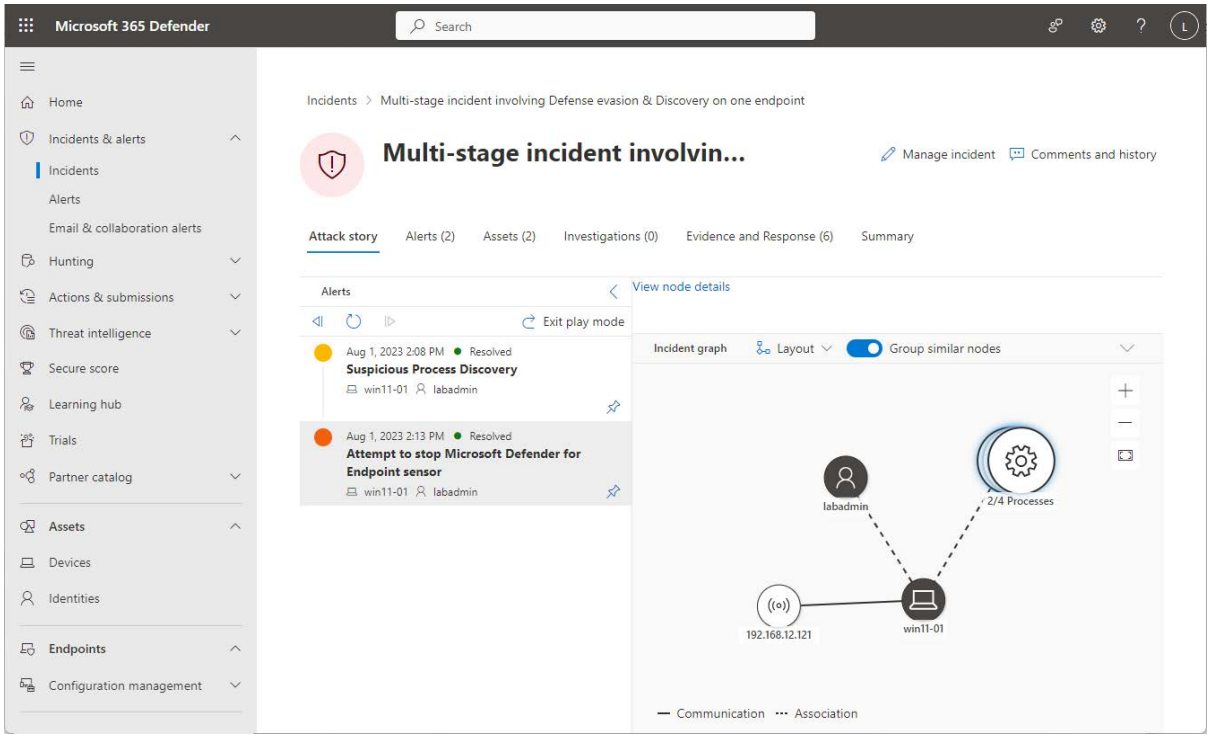

Figure 7.12 – Reviewing an alert in the Attack story

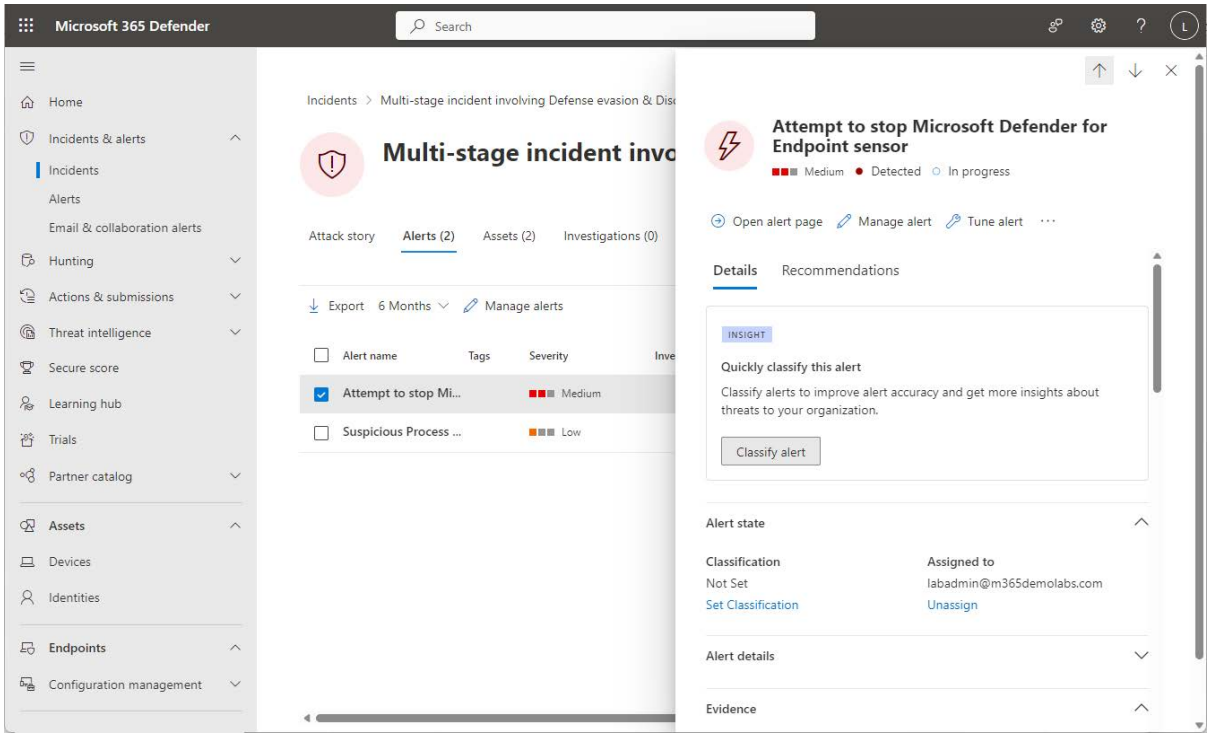

Figure 7.13 – Reviewing an alert's details

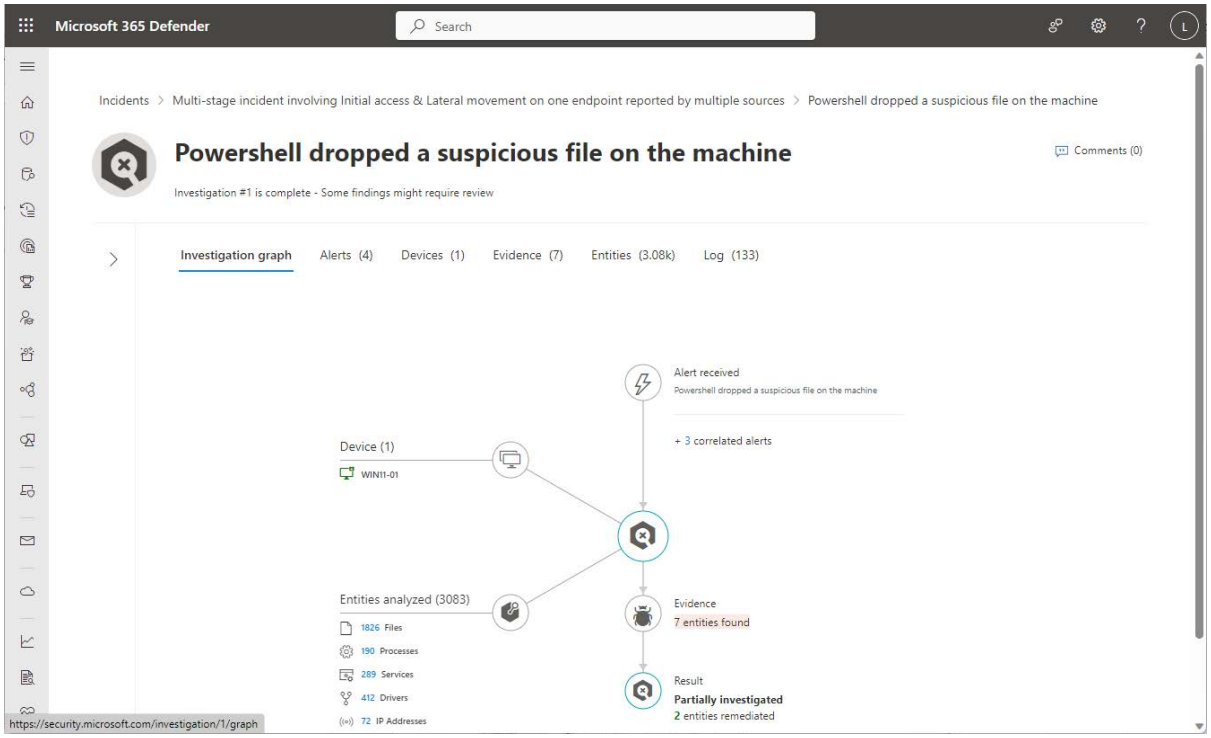

Figure 7.14 – Reviewing an investigation

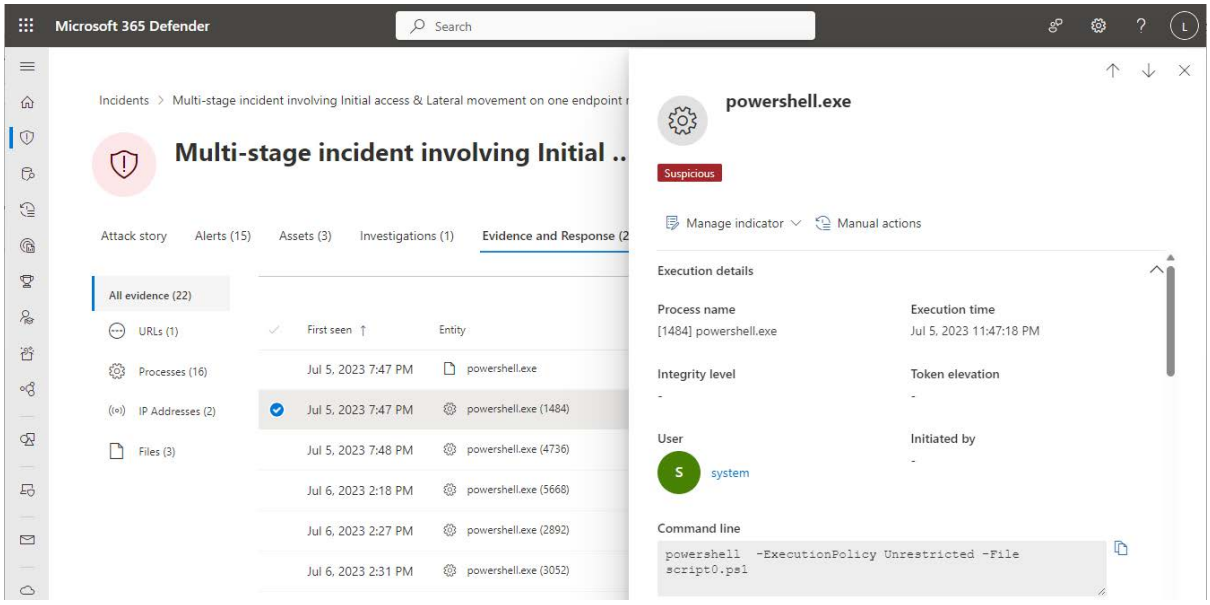

Figure 7.15 – Reviewing data on the Evidence and Response tab

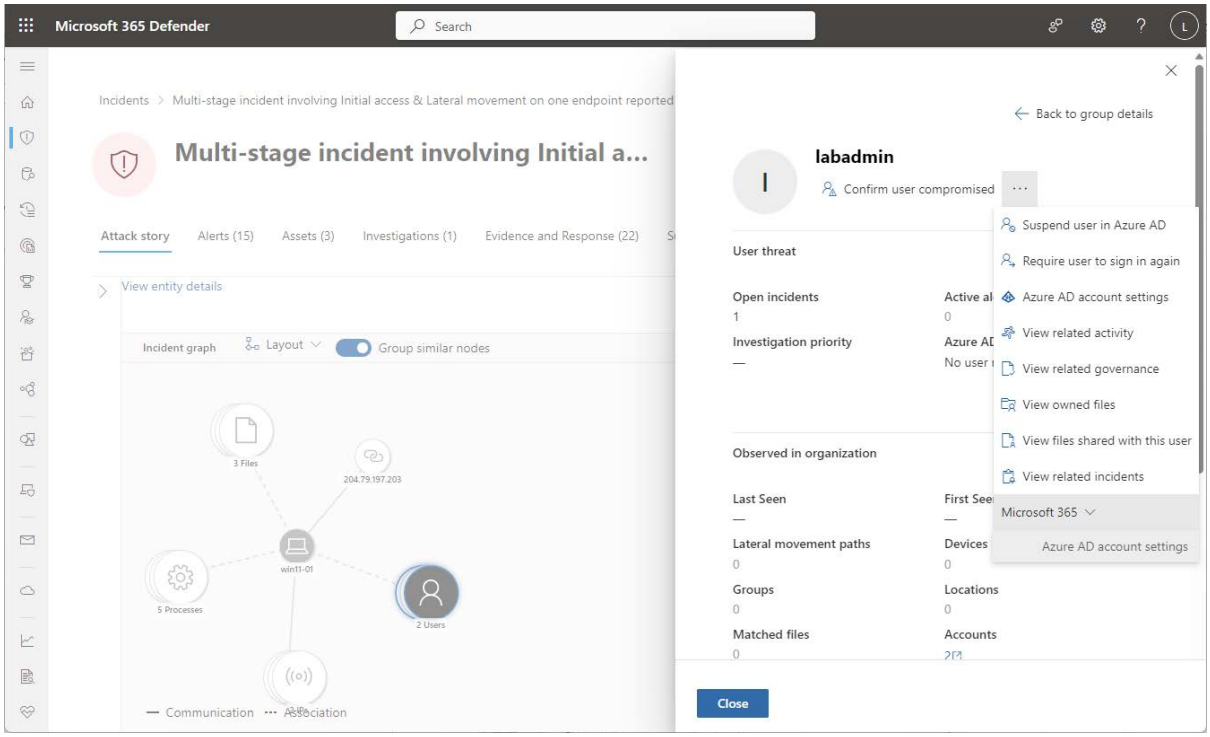

Figure 7.16 – Taking action on a user in the Attack story

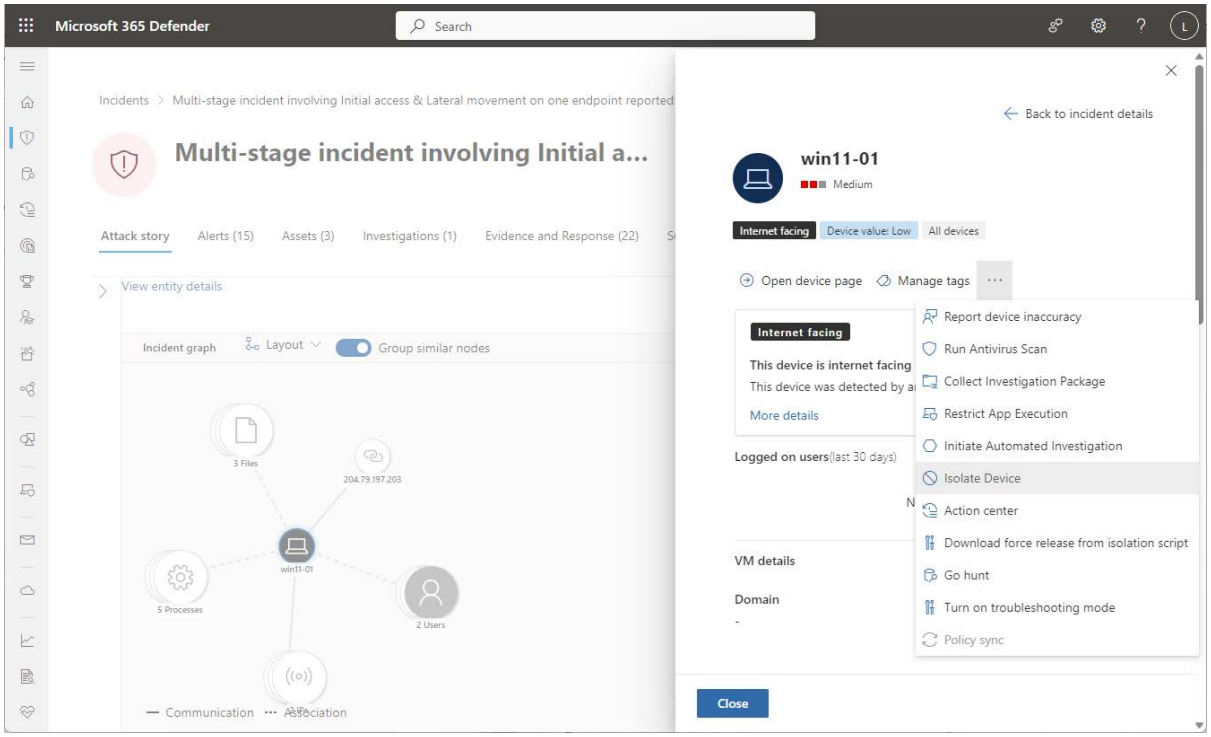

Figure 7.17 – Responding to a problematic device

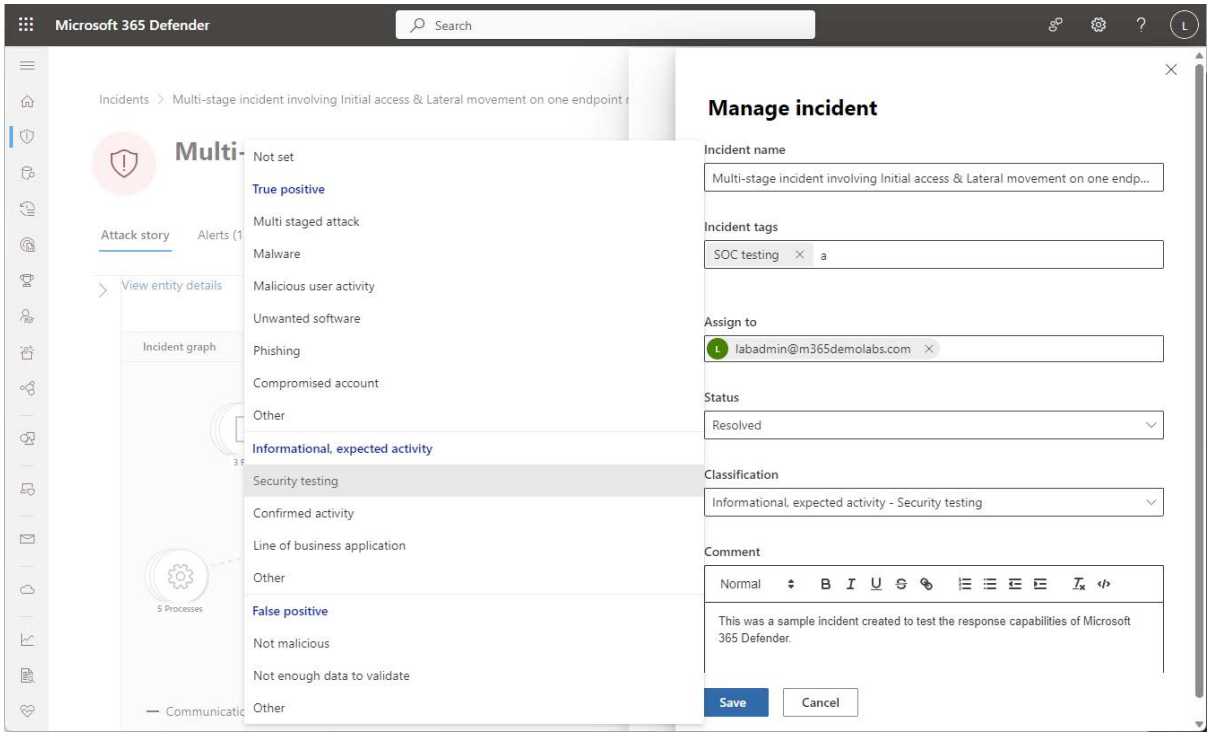

Figure 7.18 – Updating incident details

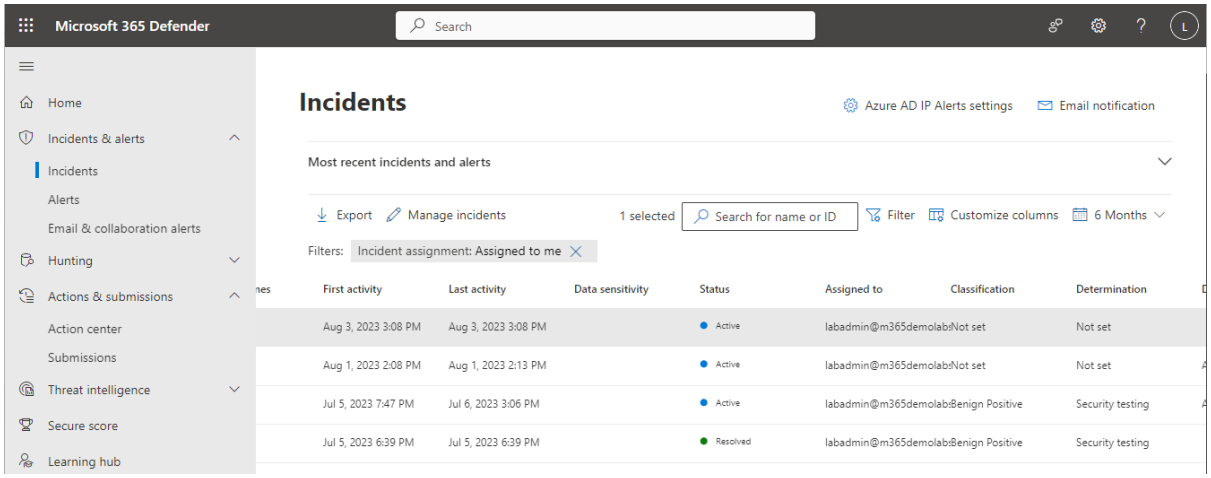

Figure 7.19 – Viewing assigned incidents

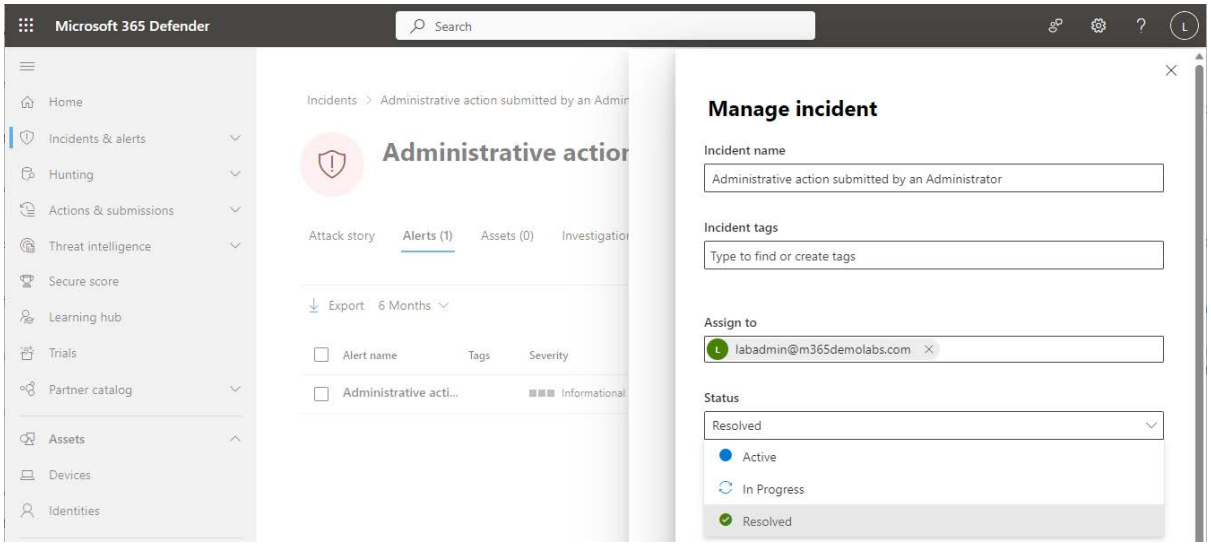

Figure 7.20 – Updating an incident status

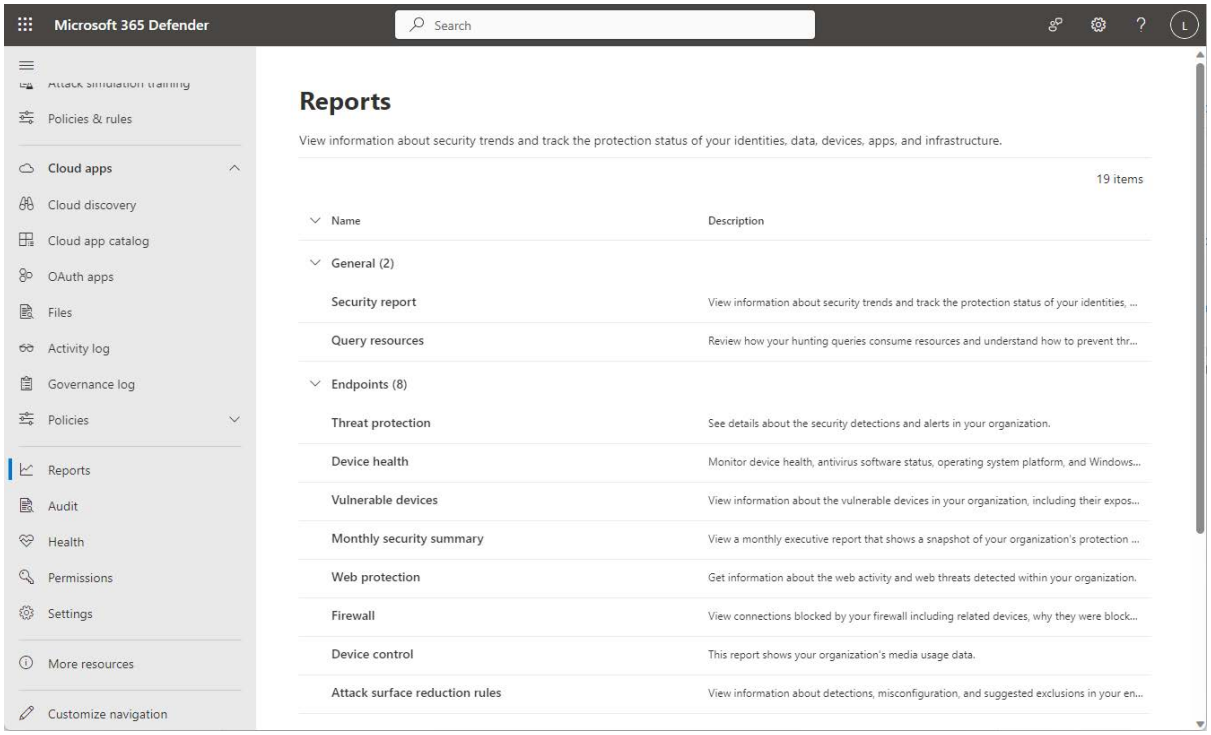

Figure 7.21 – Viewing the available Microsoft 365 reports

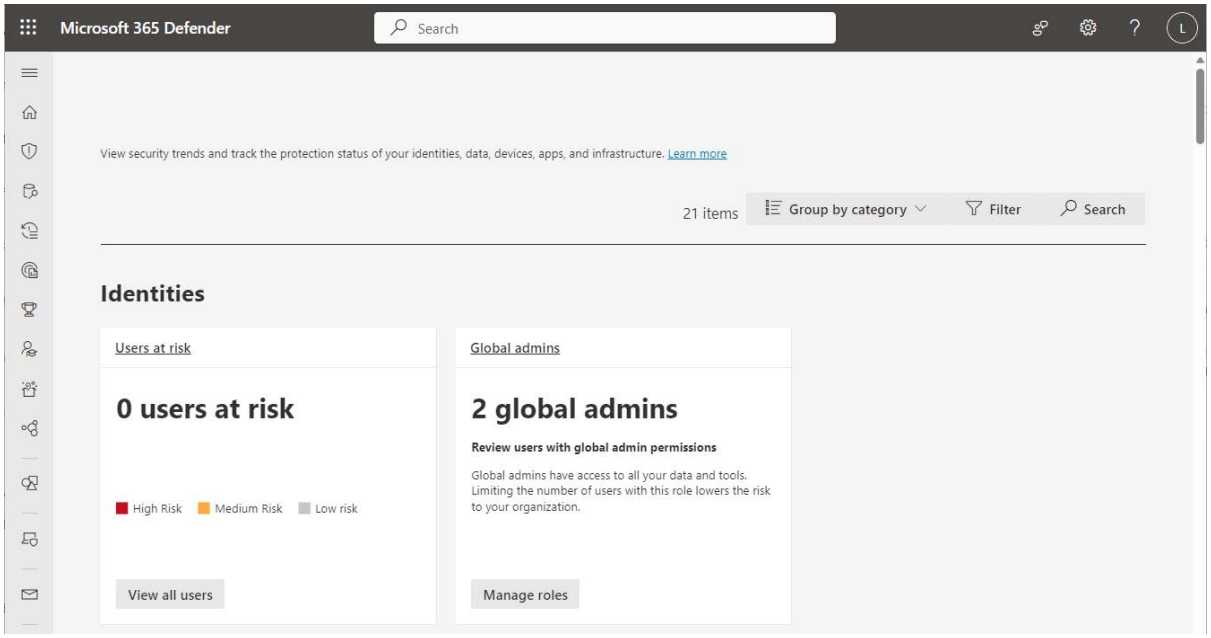

Figure 7.22 – Viewing the security report

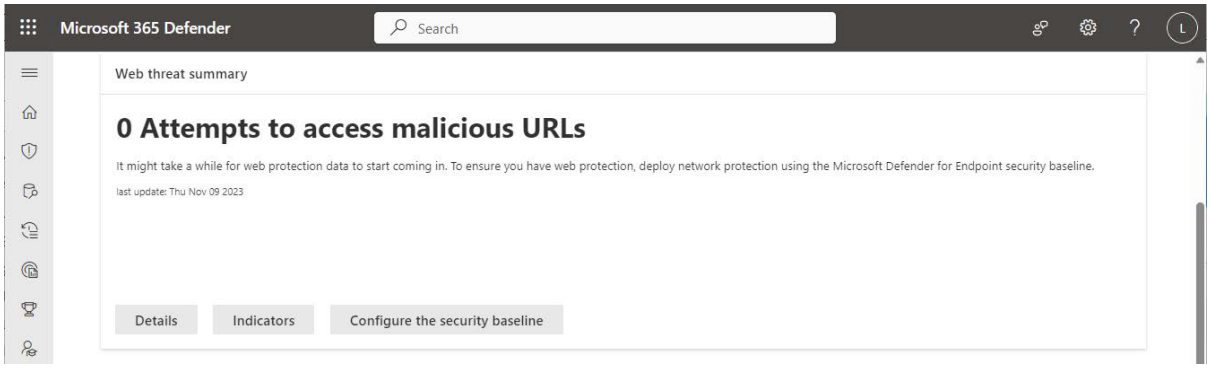

Figure 7.23 – Viewing the web protection report

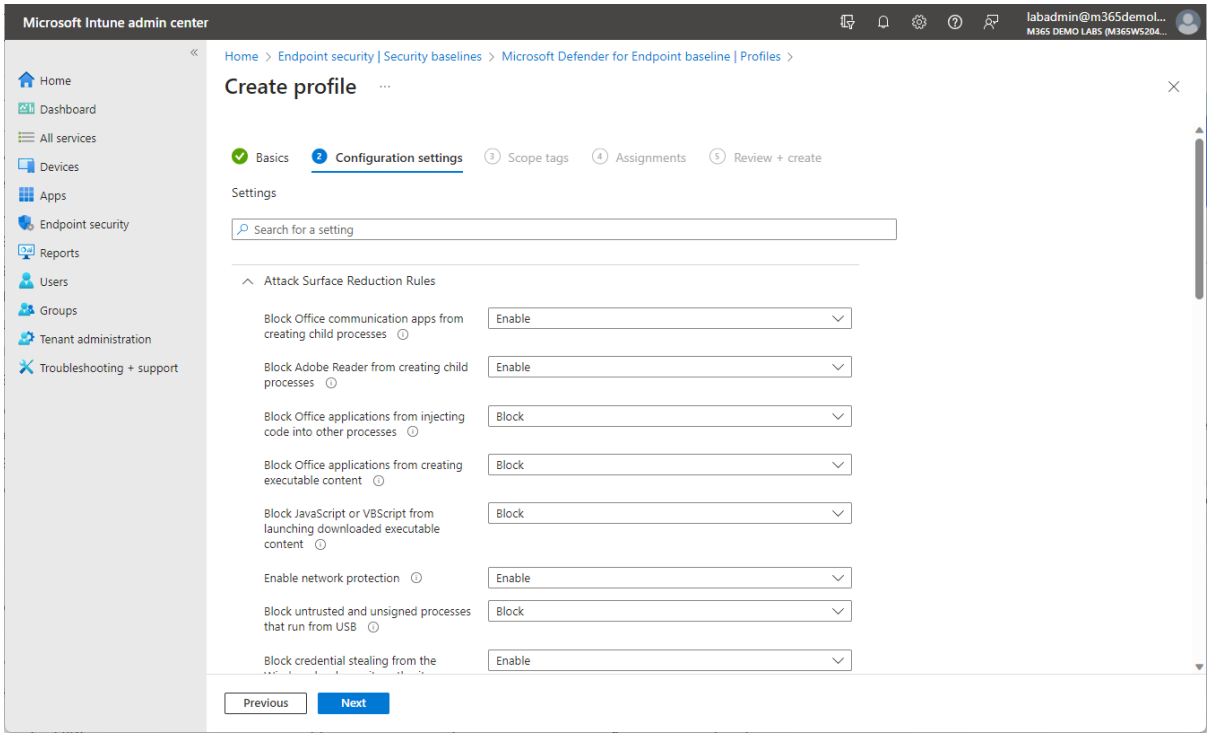

Figure 7.24 – Creating a baseline security policy

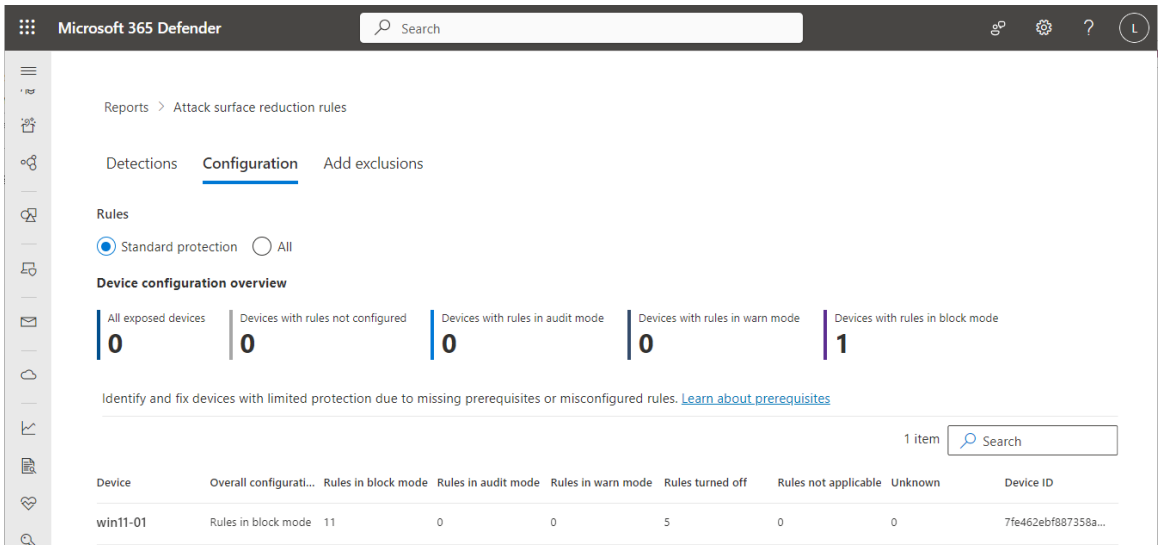

Figure 7.25 – Viewing the Attack surface reduction rules overview

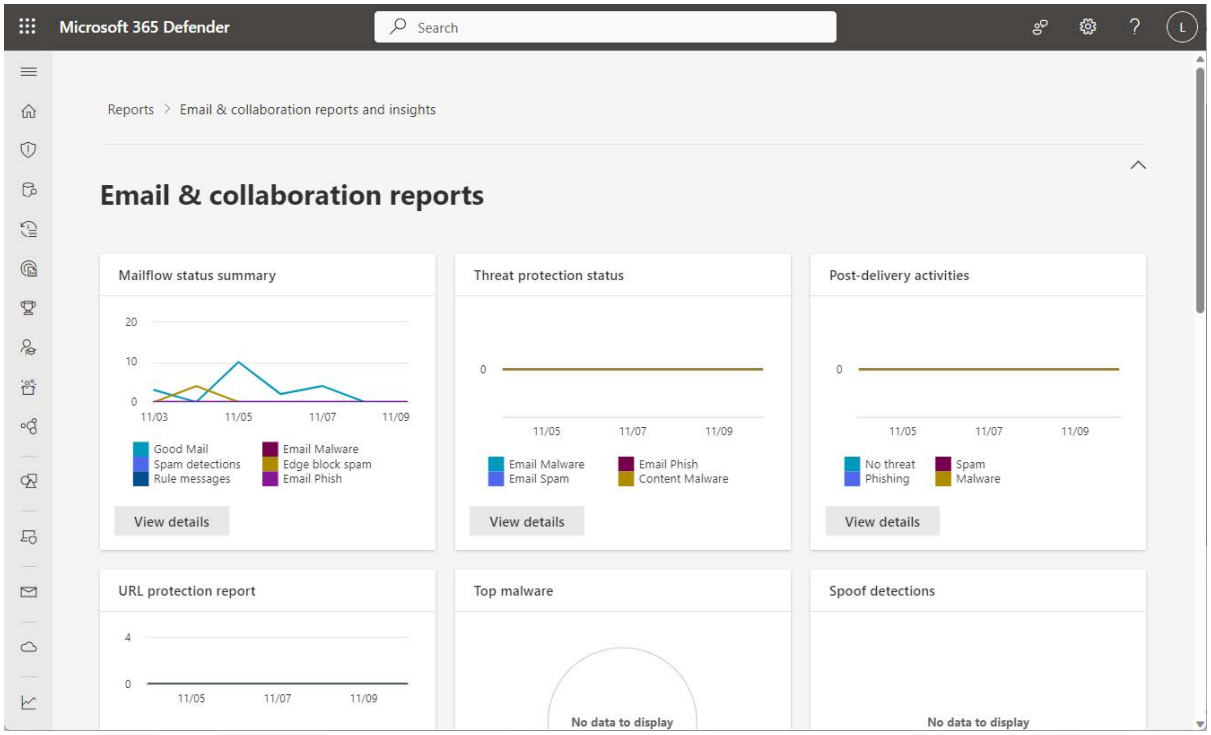

Figure 7.26 – Viewing the Email & collaboration reports dashboard

Figure 7.27 – Creating a scheduled Mailflow status report

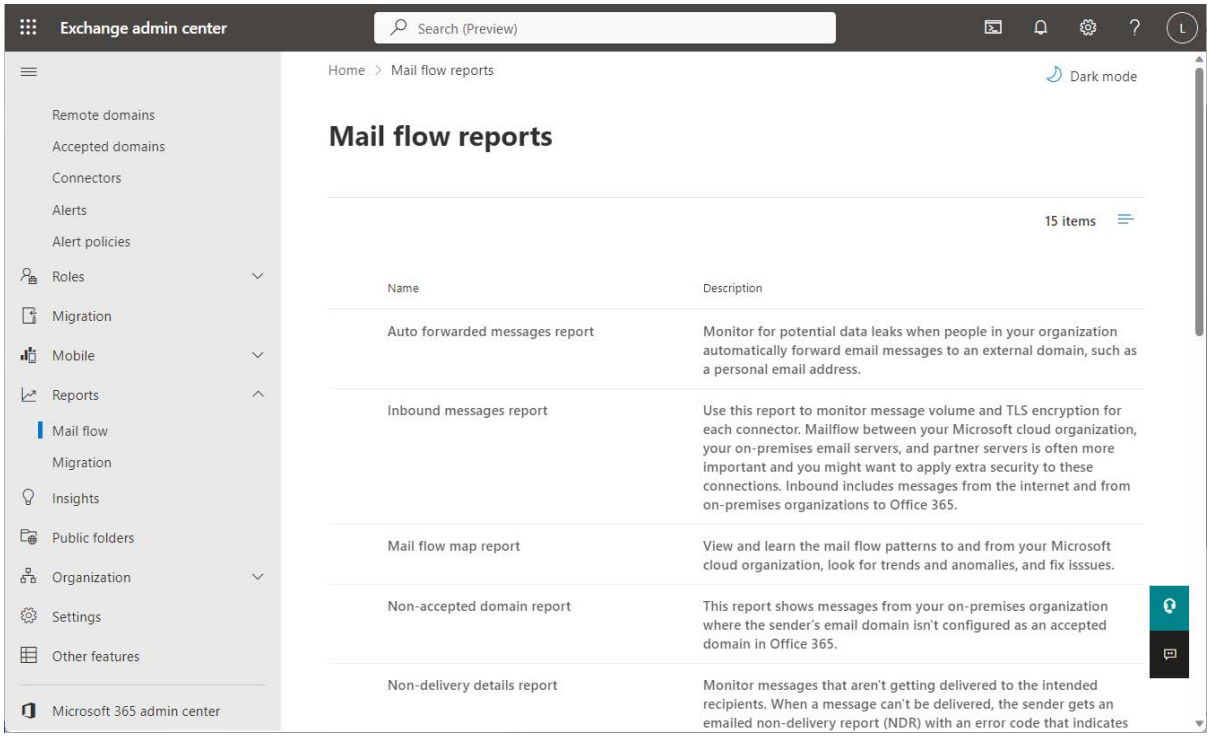

Figure 7.28 – Viewing the Mailflow reports in the Exchange admin center

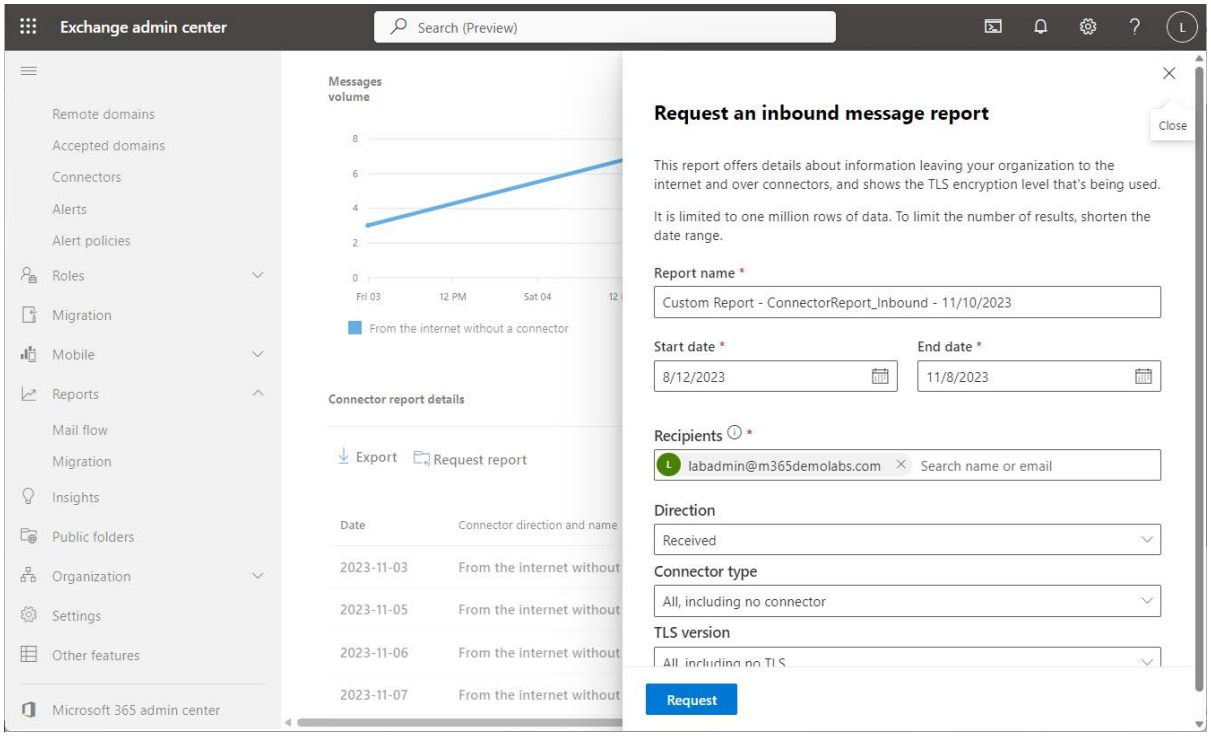

Figure 7.29 – Requesting a custom report

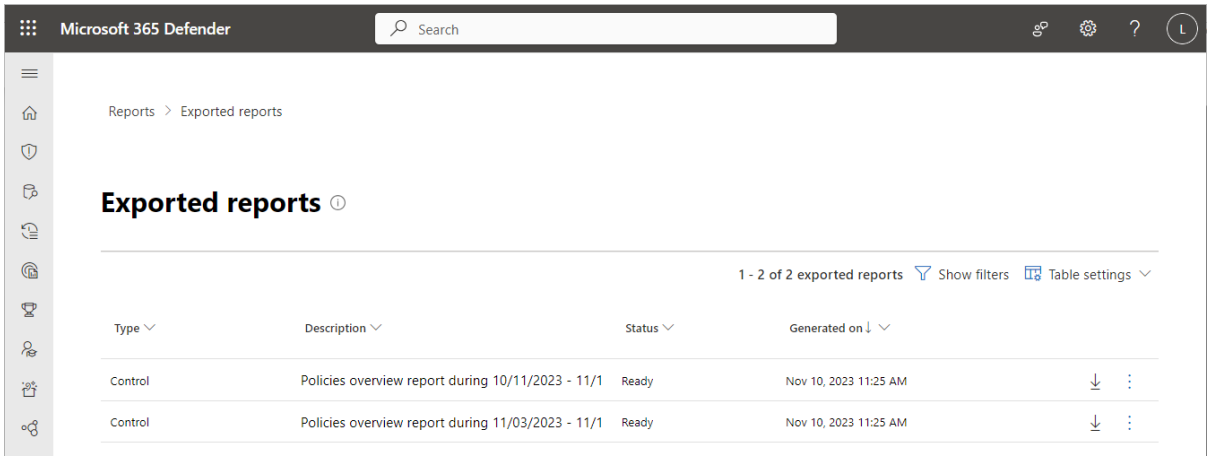

Figure 7.30 – Viewing the Cloud Apps' Exported reports page

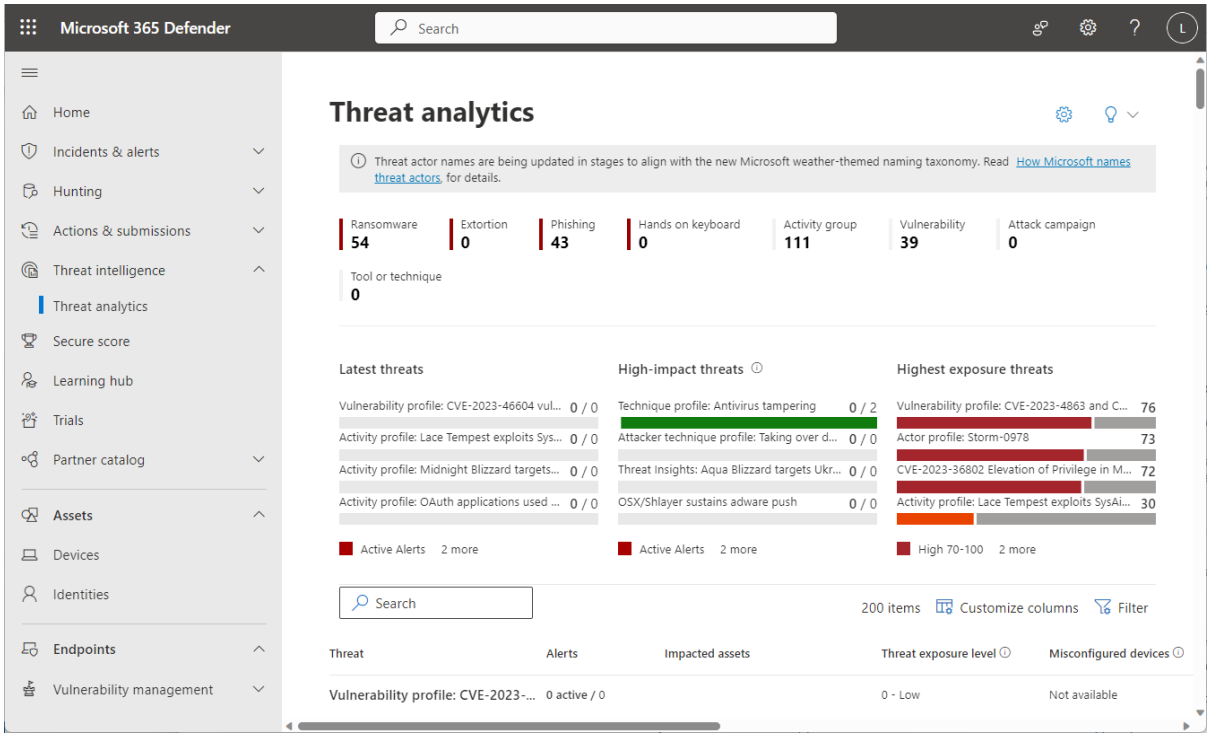

Figure 7.31 – Viewing the Threat analytics dashboard

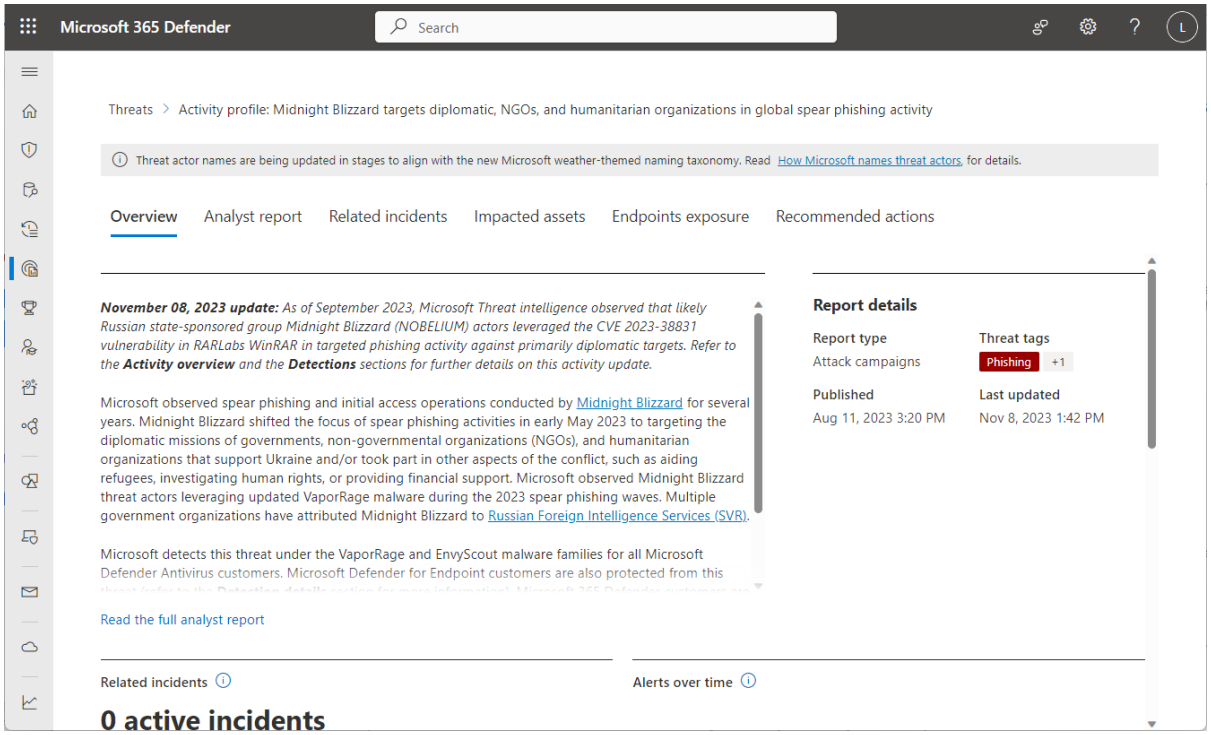

Figure 7.32 – Viewing a threat's vulnerability profile

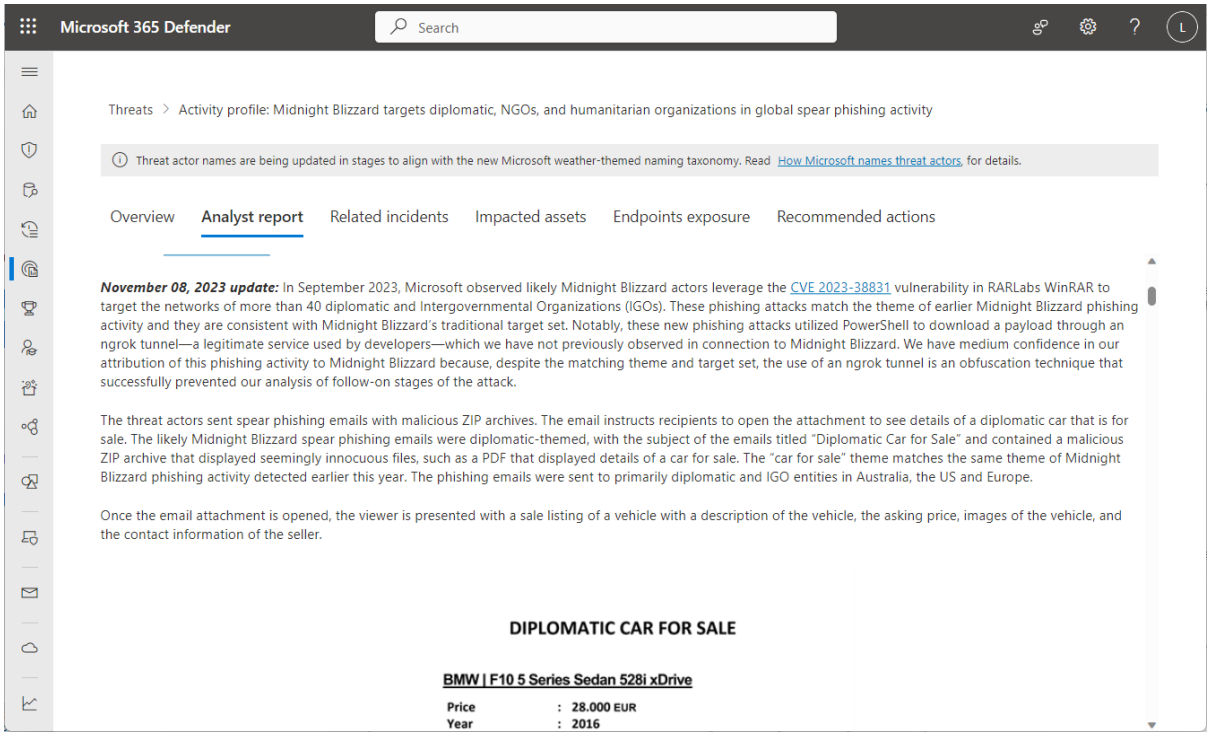

Figure 7.33 – Reviewing the Analyst report

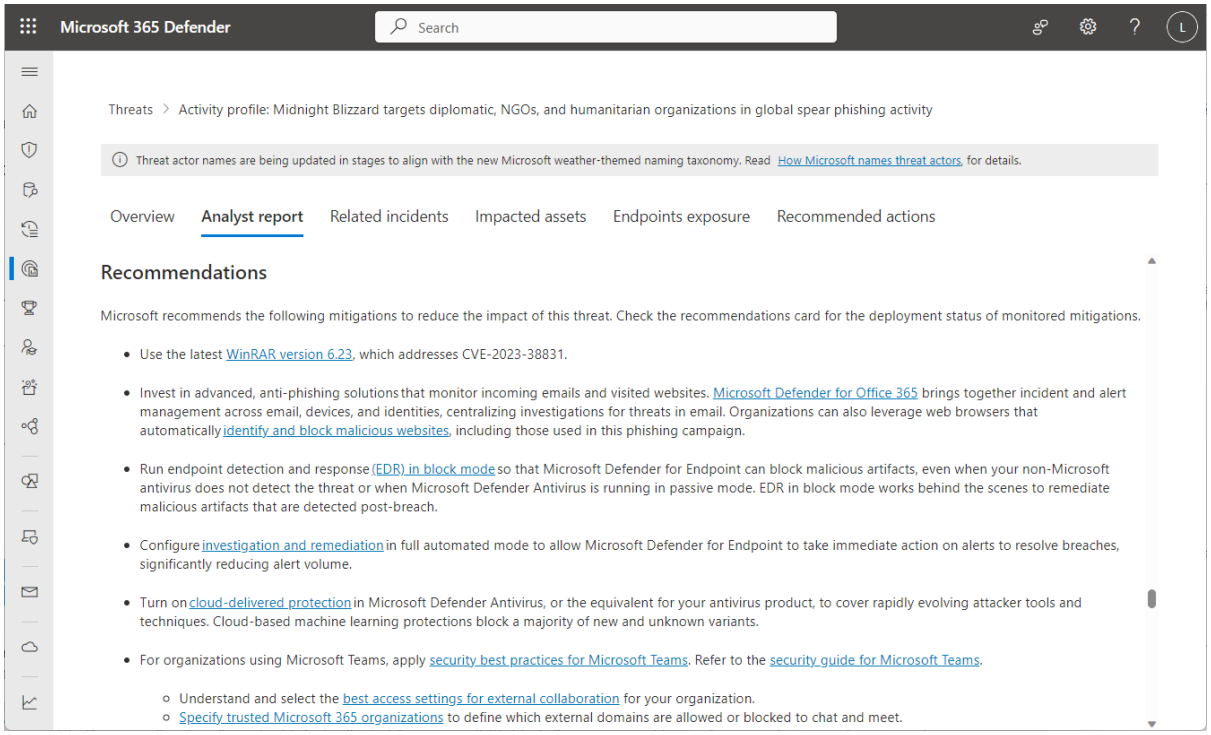

Figure 7.34 – Reviewing recommendations for non-Microsoft products in the Analyst report

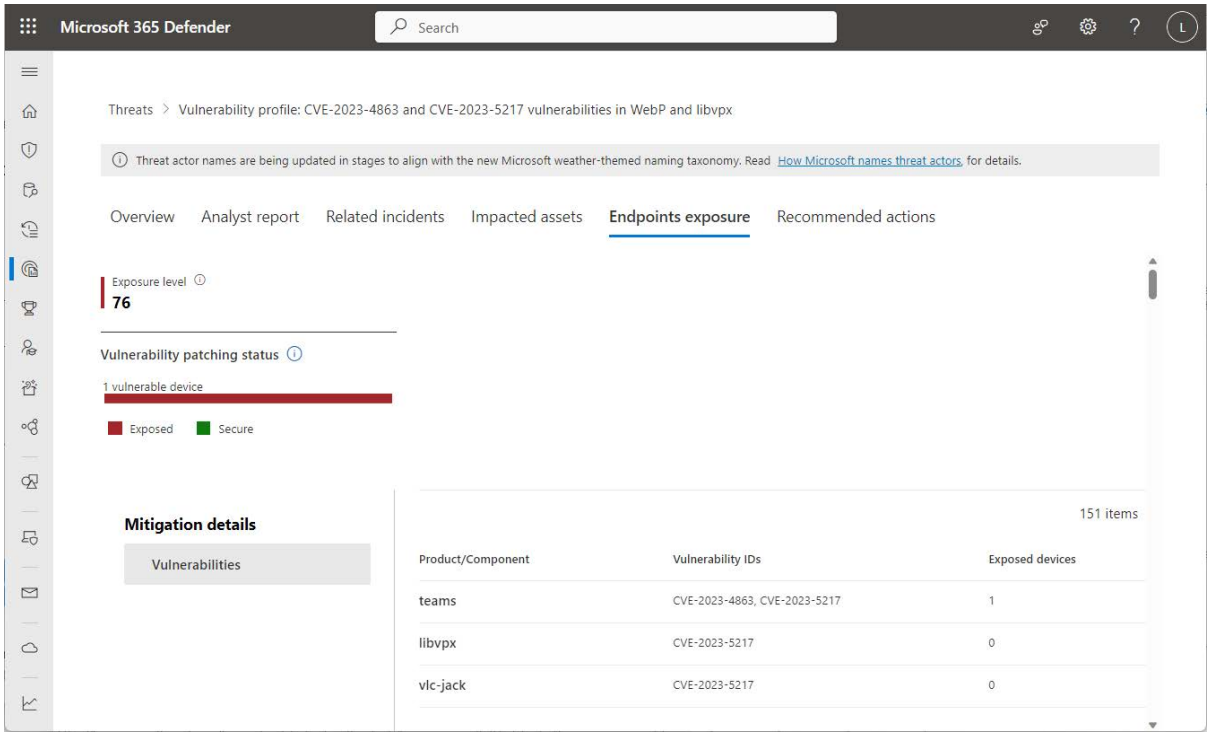

Figure 7.35 – Viewing the exposed endpoints

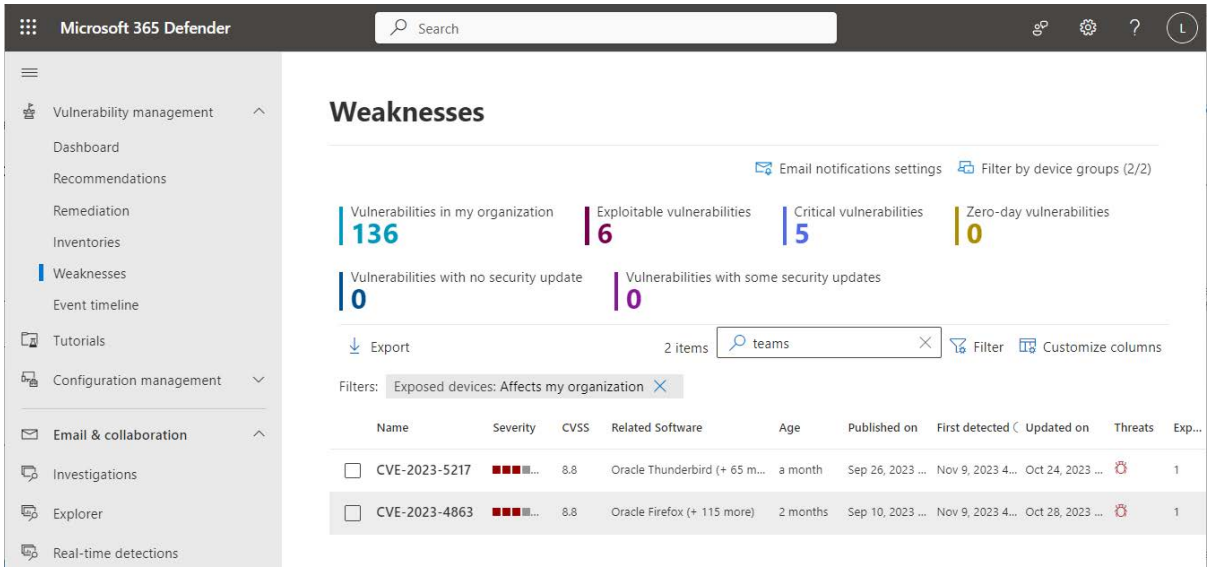

Figure 7.36 – Searching for the product related to the threat on the Endpoint exposures page

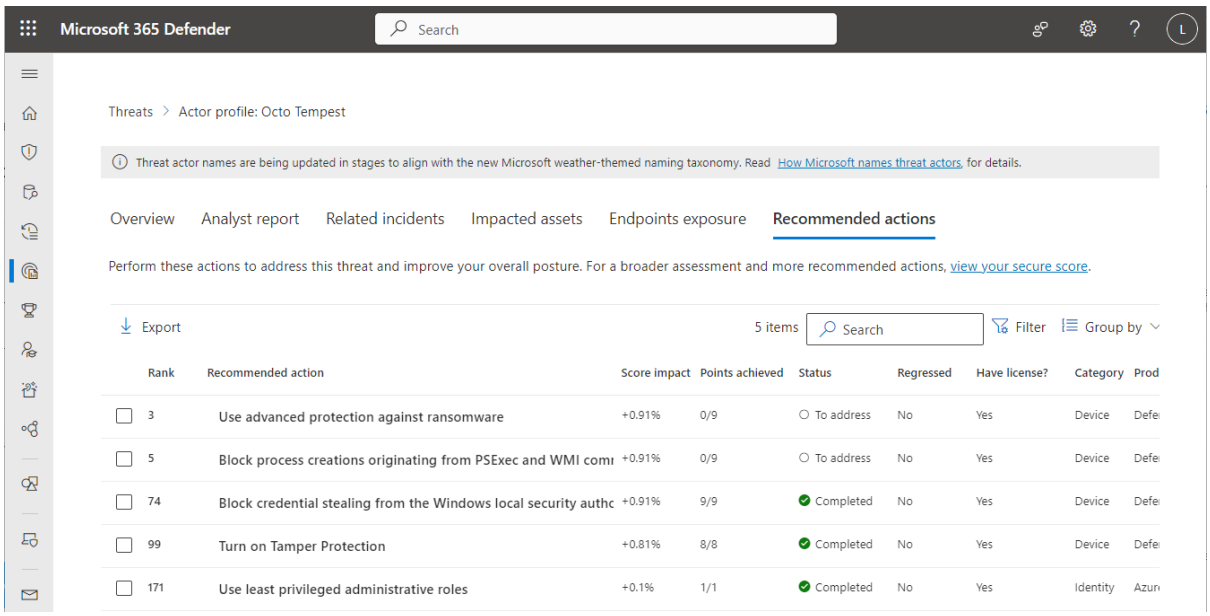

Figure 7.37 – Reviewing Recommended actions

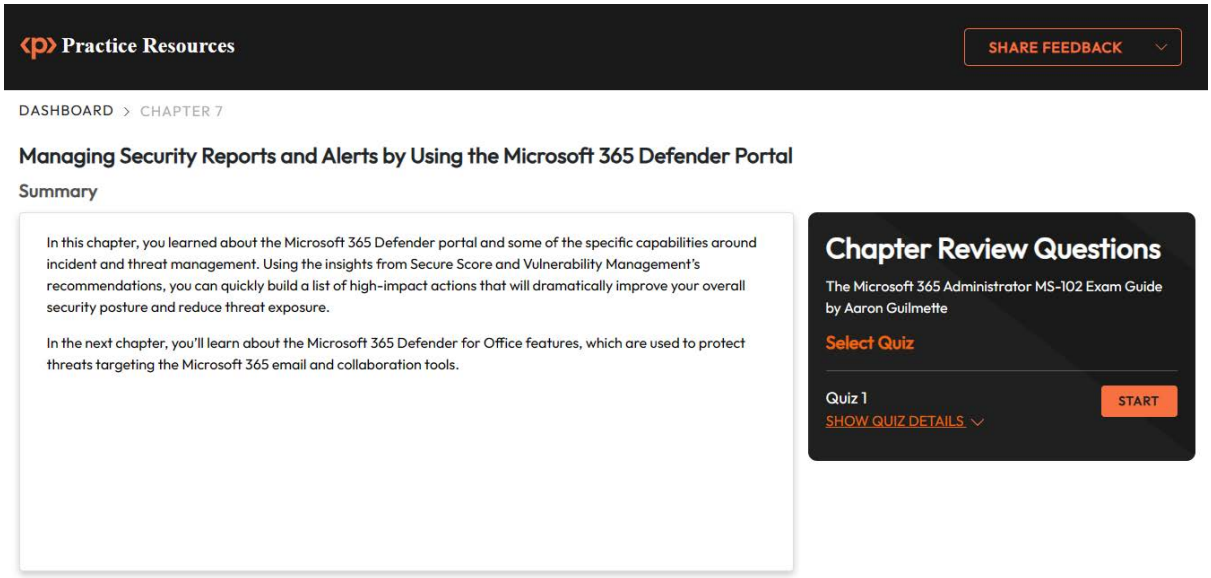

Figure 7.38 – Chapter Review Questions for Chapter 7

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

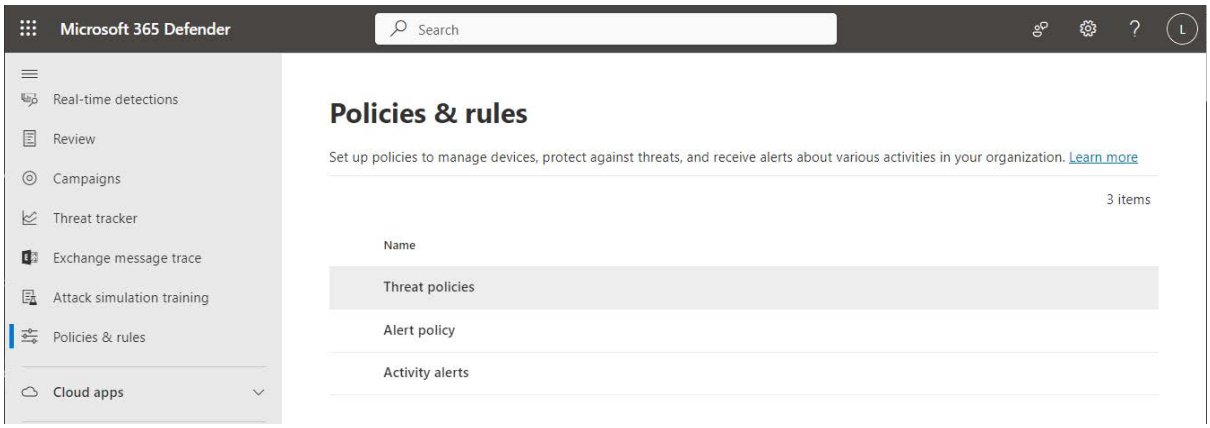

Figure 8.1 – Navigating to Threat policies

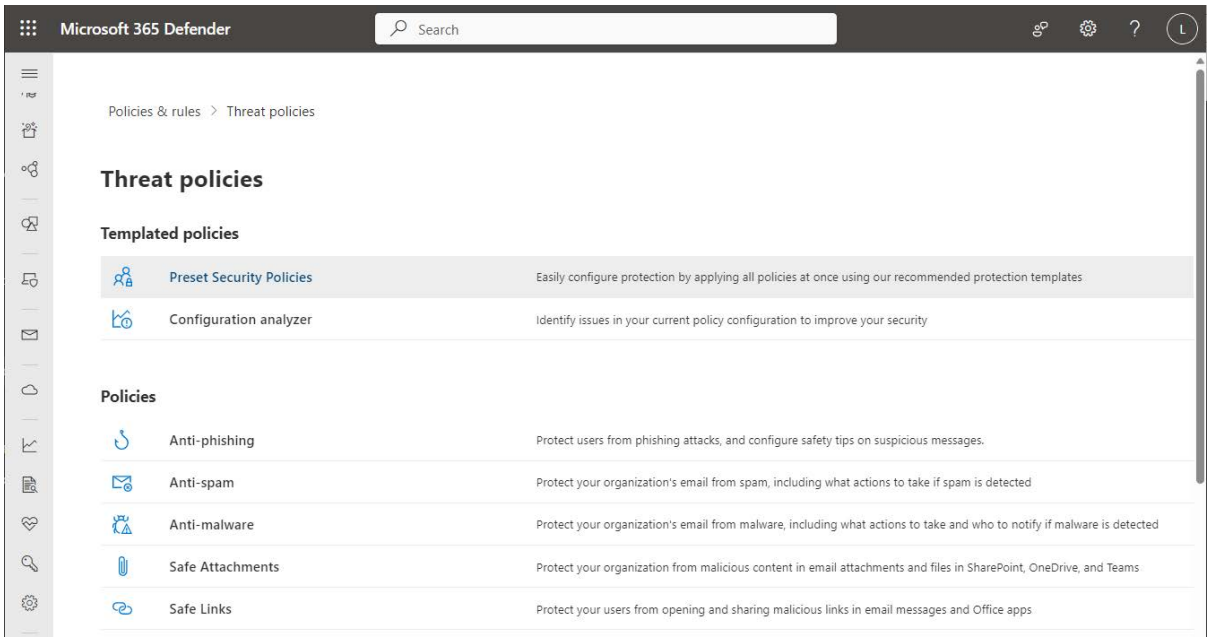

Figure 8.2 – Configuring preset security policies

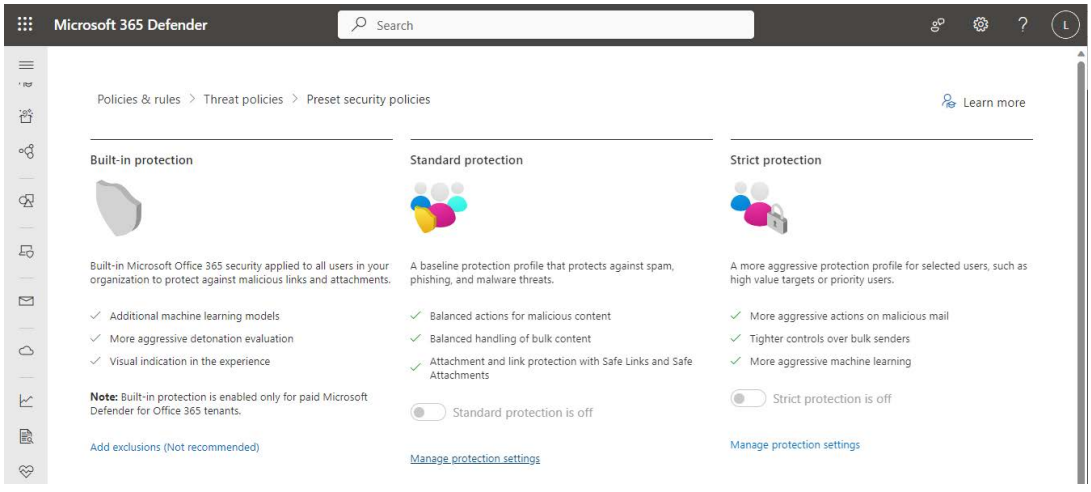

Figure 8.3 – Configuring Standard protection settings

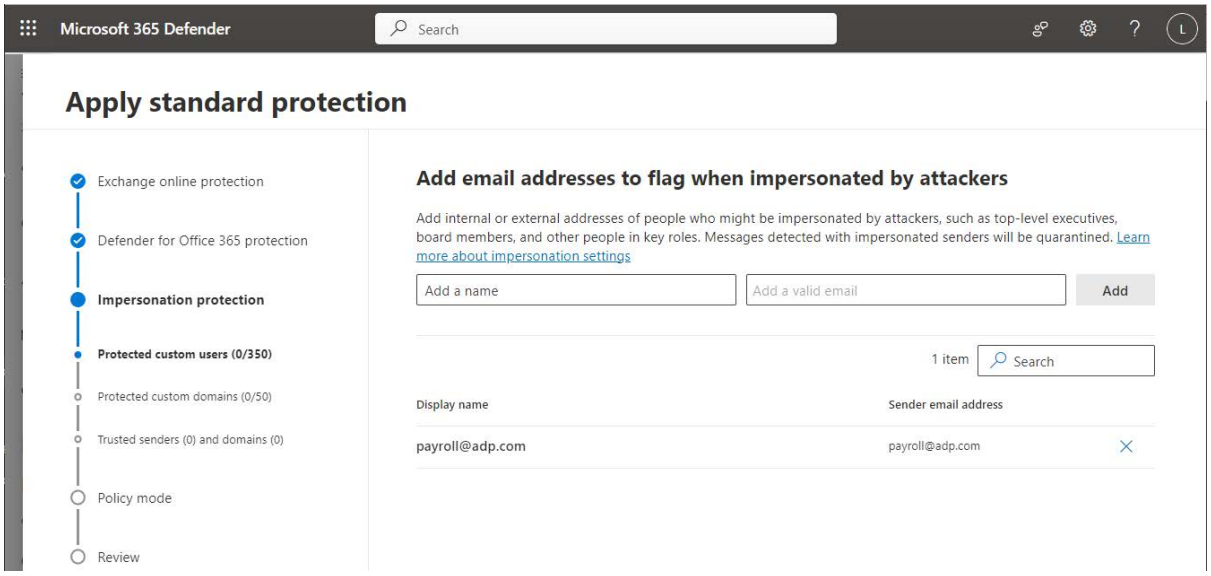

Figure 8.4 – Configuring impersonation settings

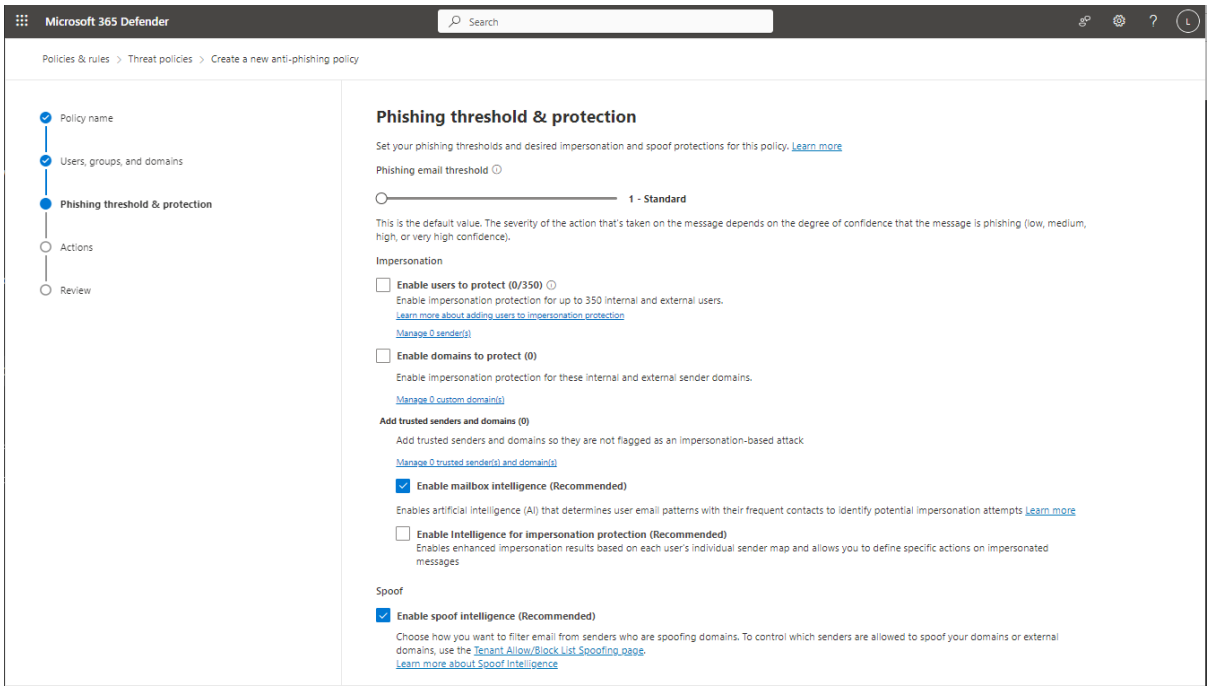

Figure 8.5 – Phishing threshold & protection page

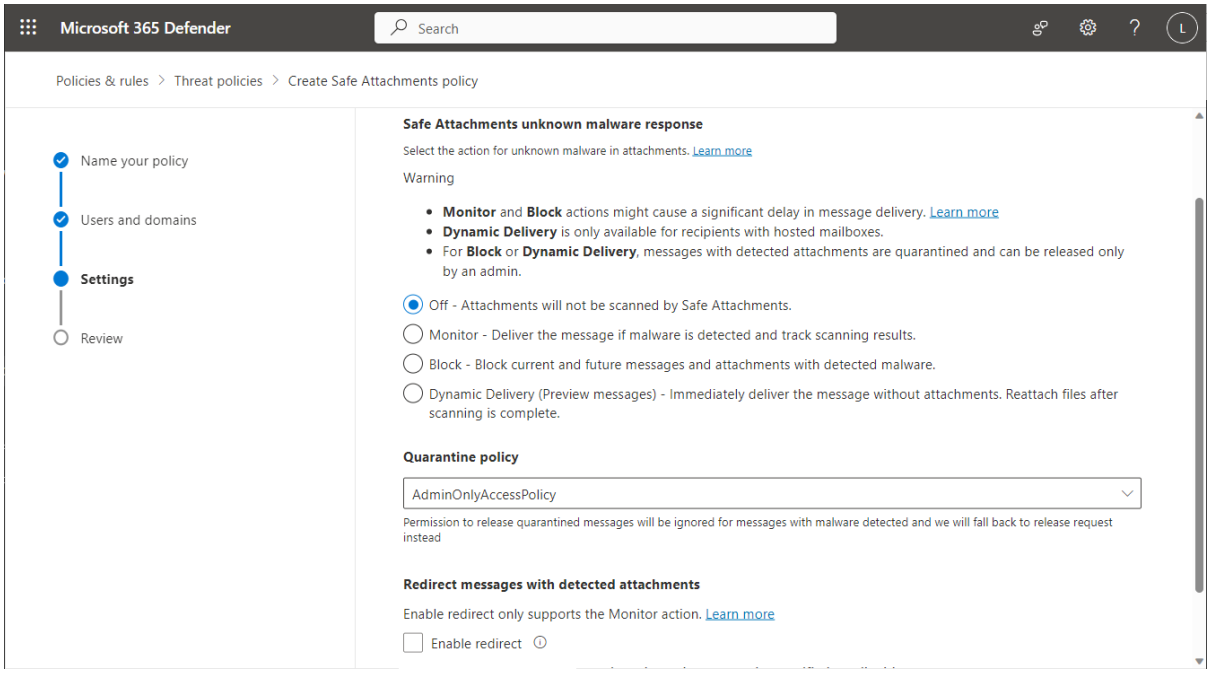

Figure 8.6 – Choosing Safe Attachments options

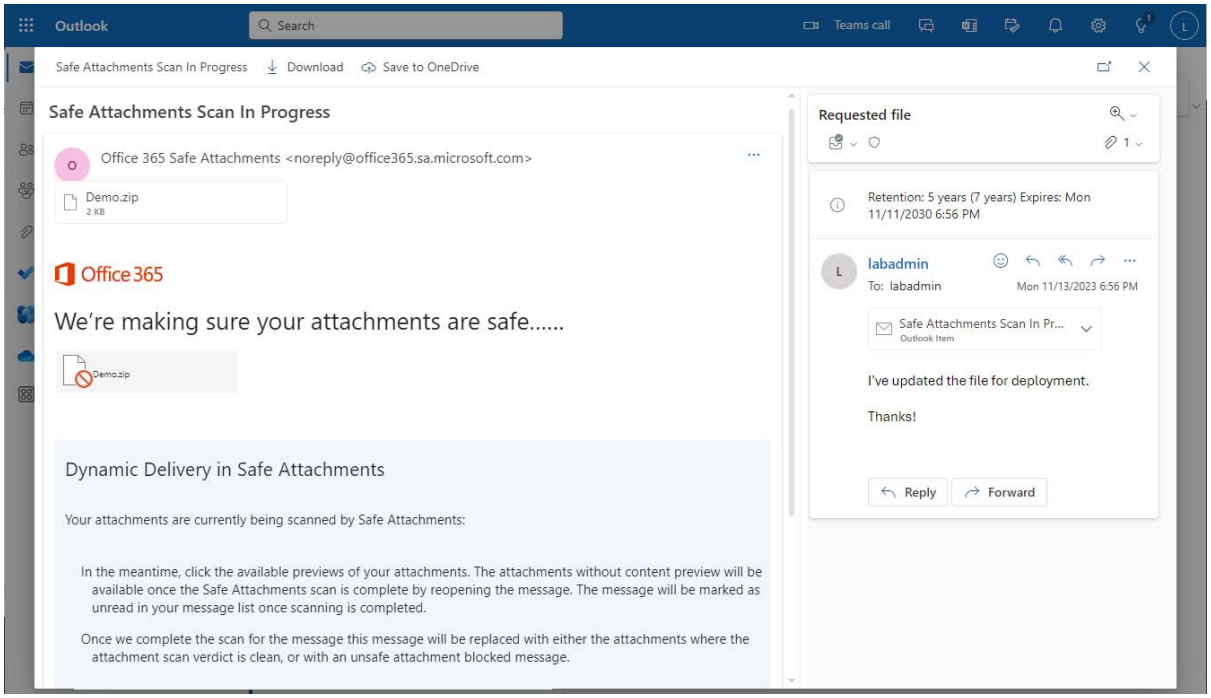

Figure 8.7 – Viewing a Safe Attachments message

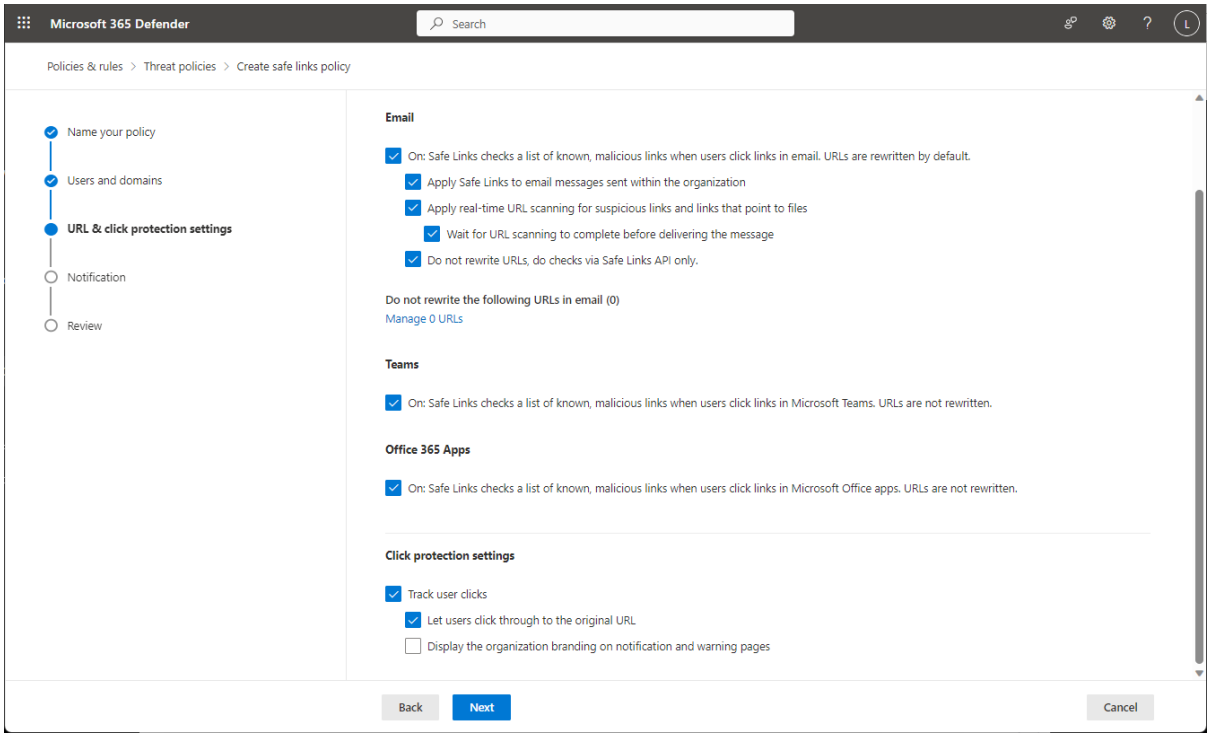

Figure 8.8 – Configuring a Safe Links policy

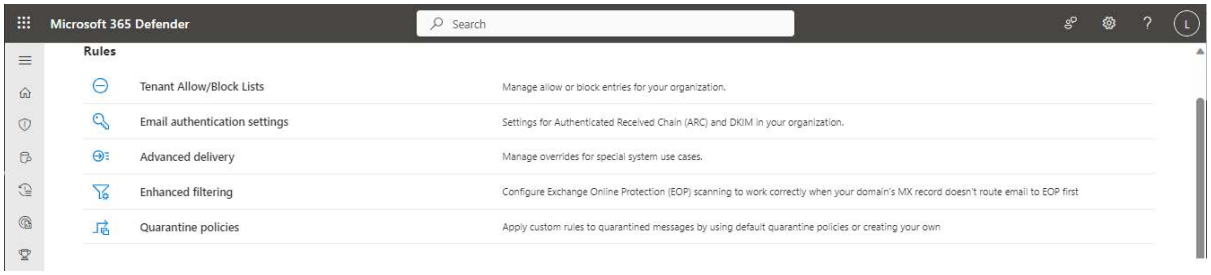

Figure 8.9 – Exchange Online Protection standard features

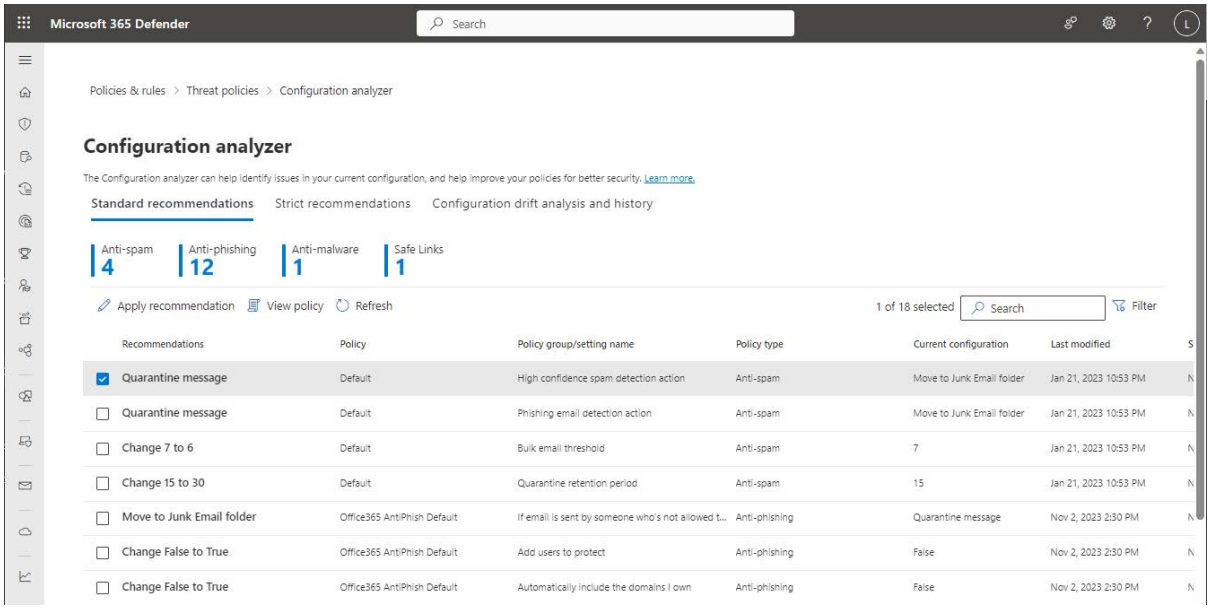

Figure 8.10 – Viewing the Configuration analyzer's recommendations

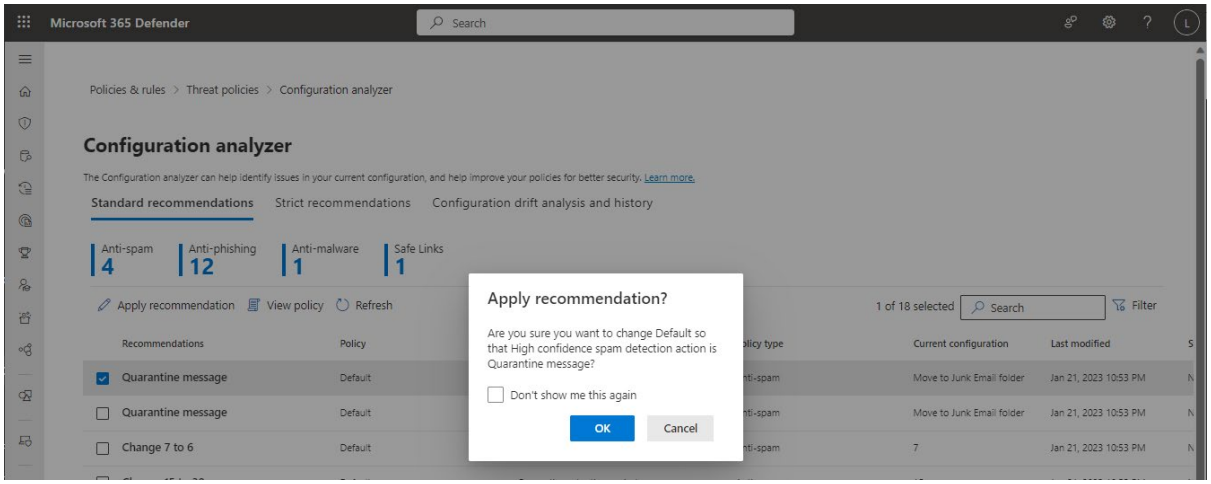

Figure 8.11 – Applying a Microsoft 365 Defender recommendation

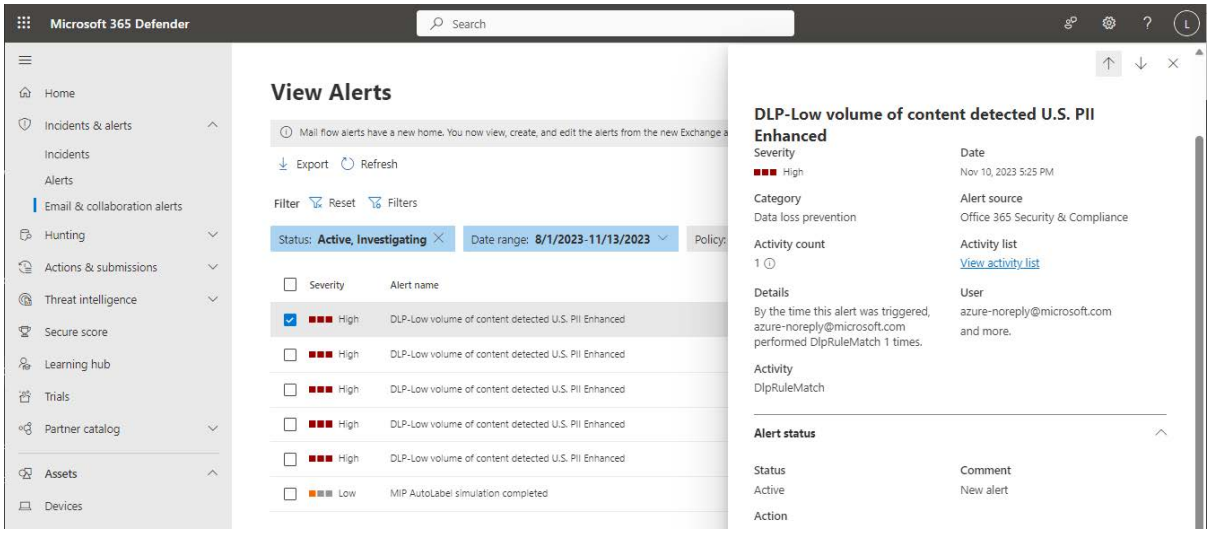

Figure 8.12 – Viewing Email & collaboration alerts

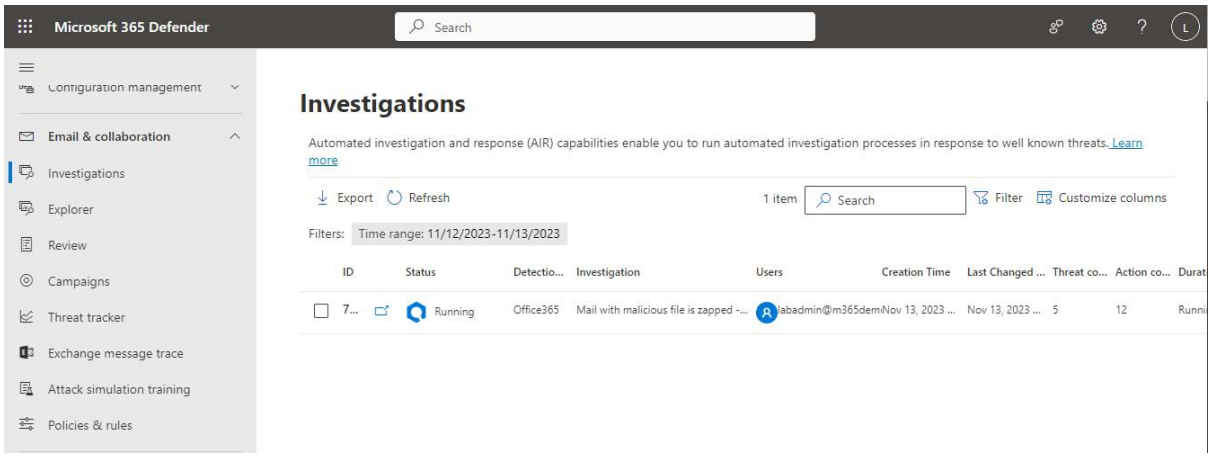

Figure 8.13 – Viewing the Investigations page

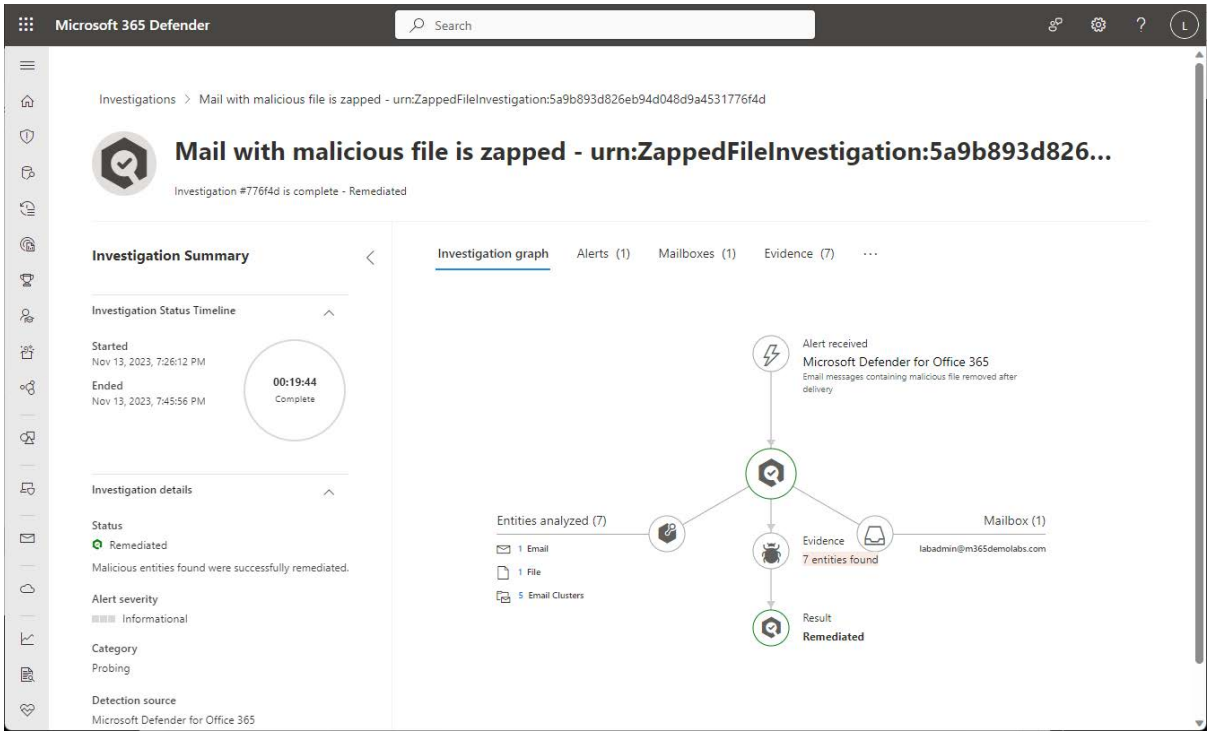

Figure 8.14 – Viewing the Investigation graph

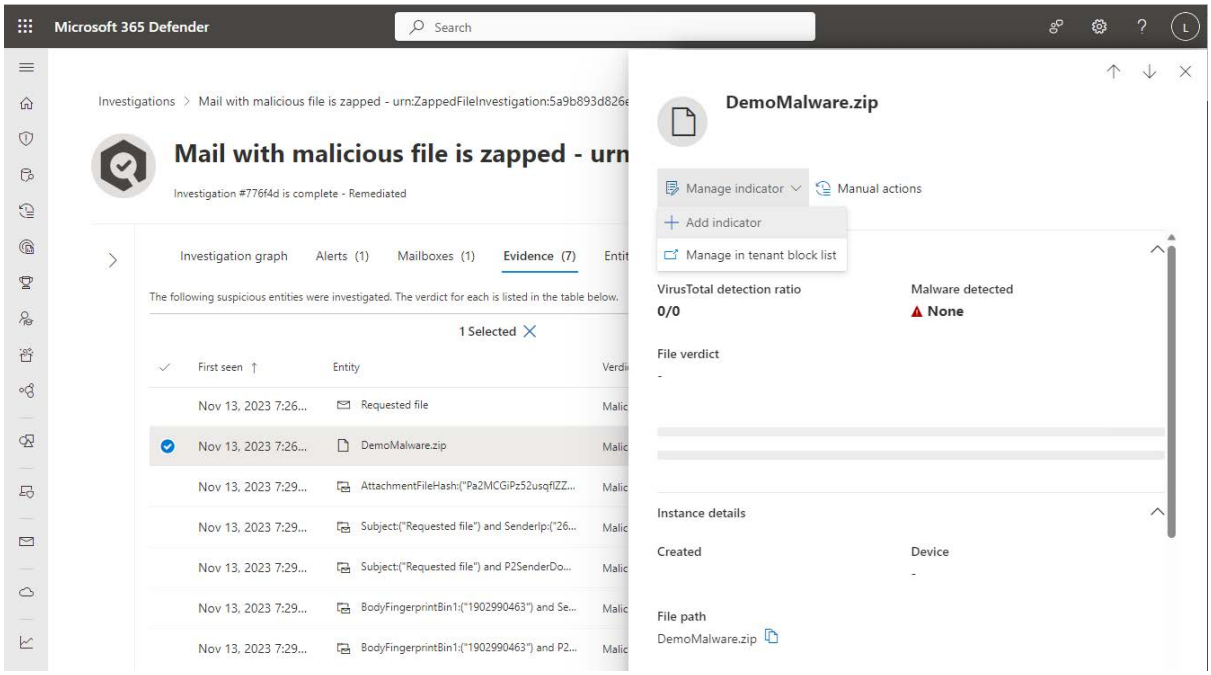

Figure 8.15 – Reviewing actions for evidence in an investigation

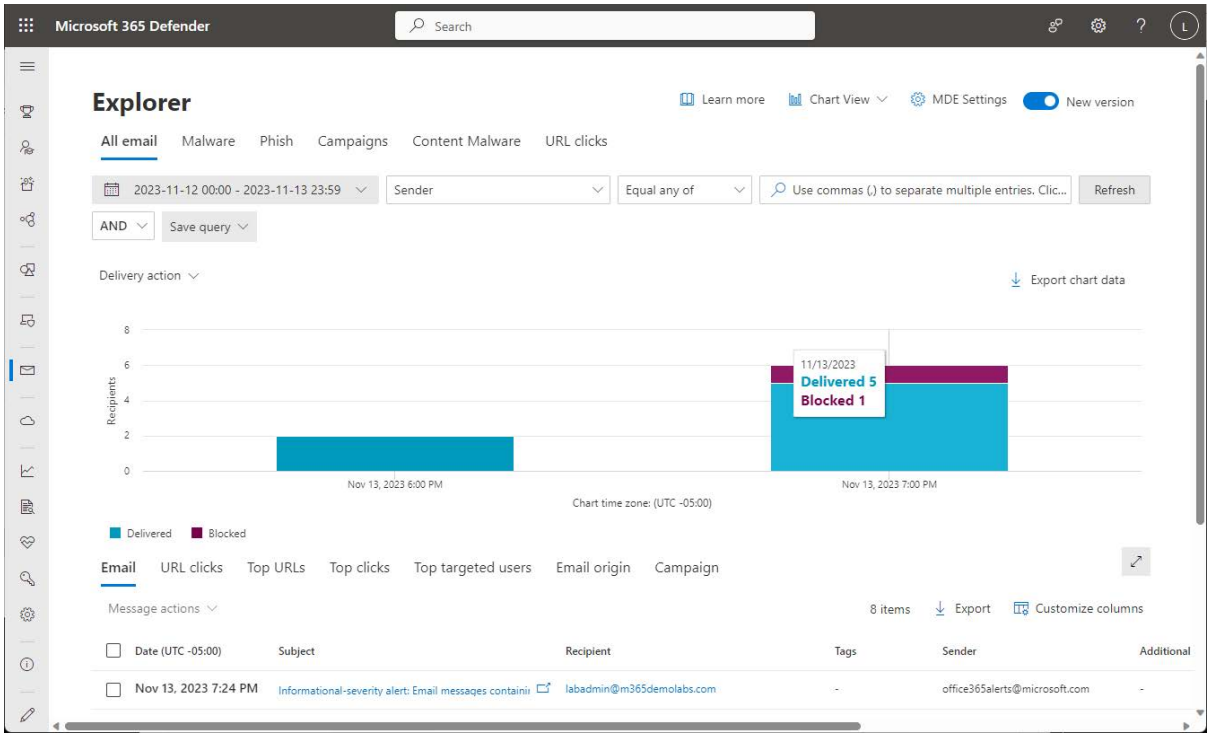

Figure 8.16 – Viewing the Explorer dashboard

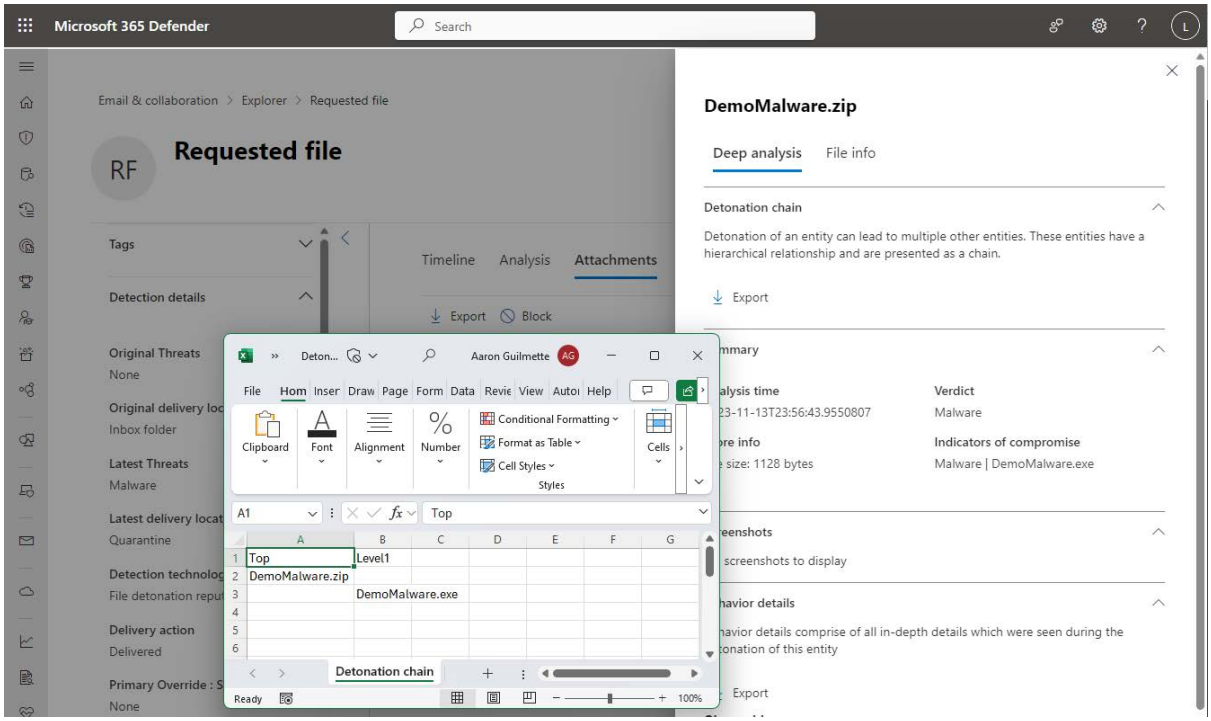

Figure 8.17 – Viewing the details of an attachment

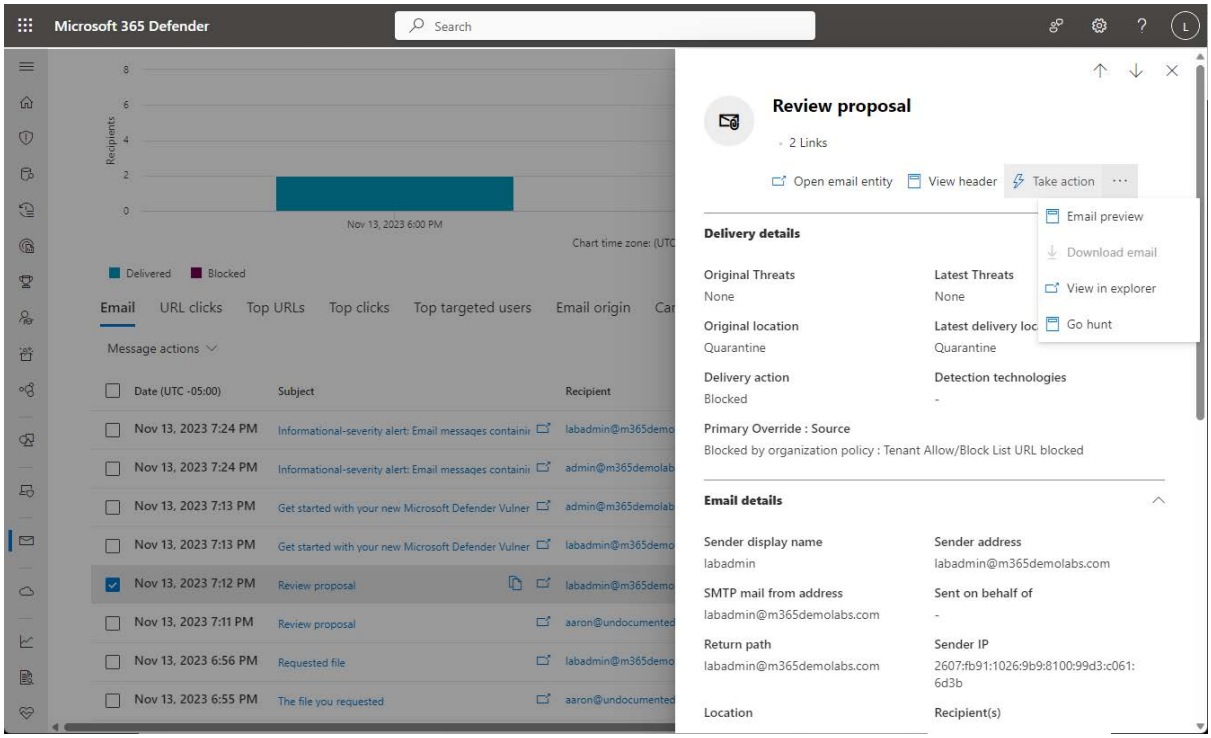

Figure 8.18 – Viewing the actions for a message

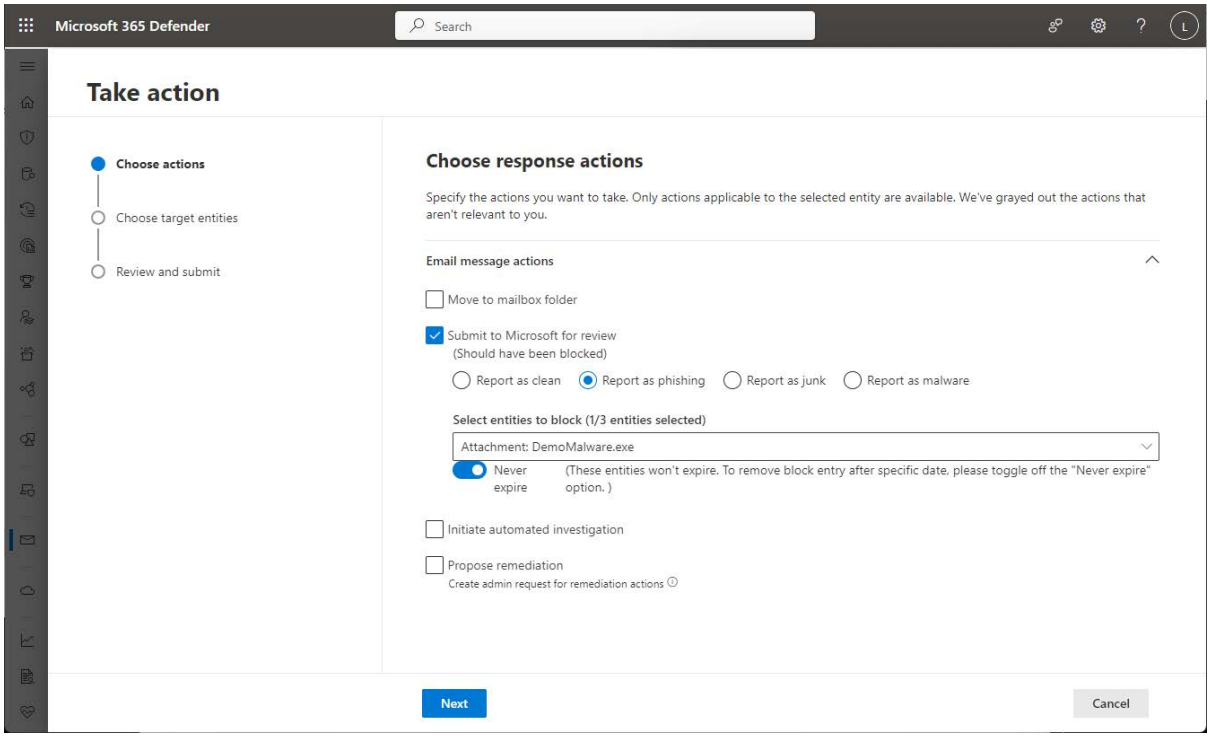

Figure 8.19 – Taking action on a message

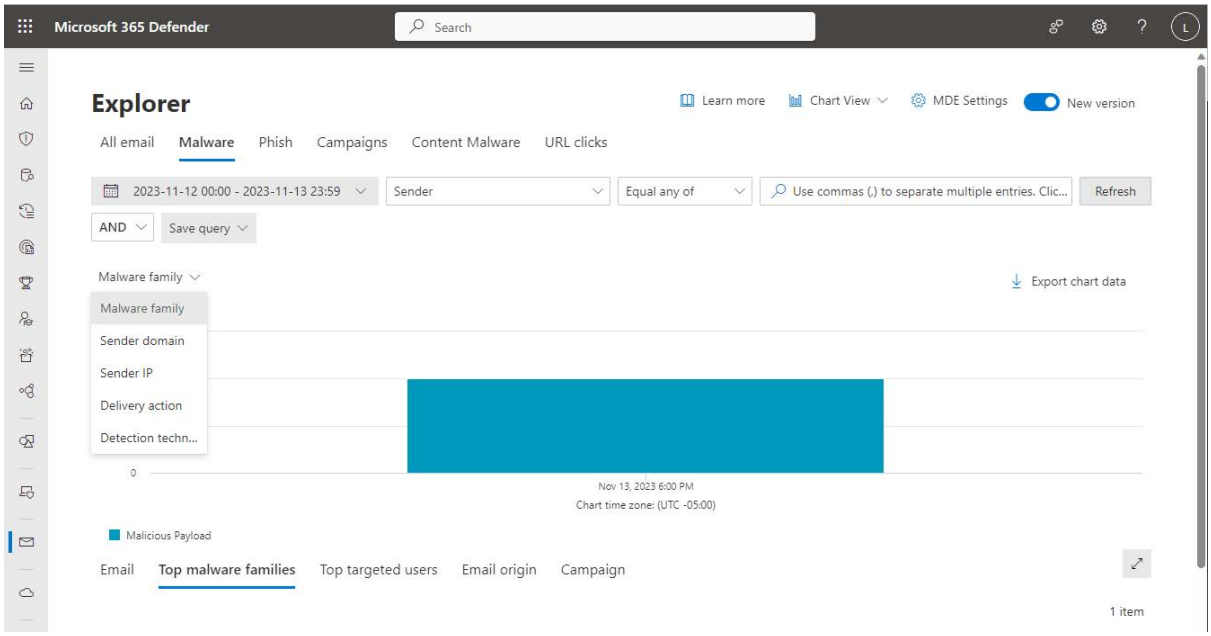

Figure 8.20 – Reviewing the malware page in Explorer

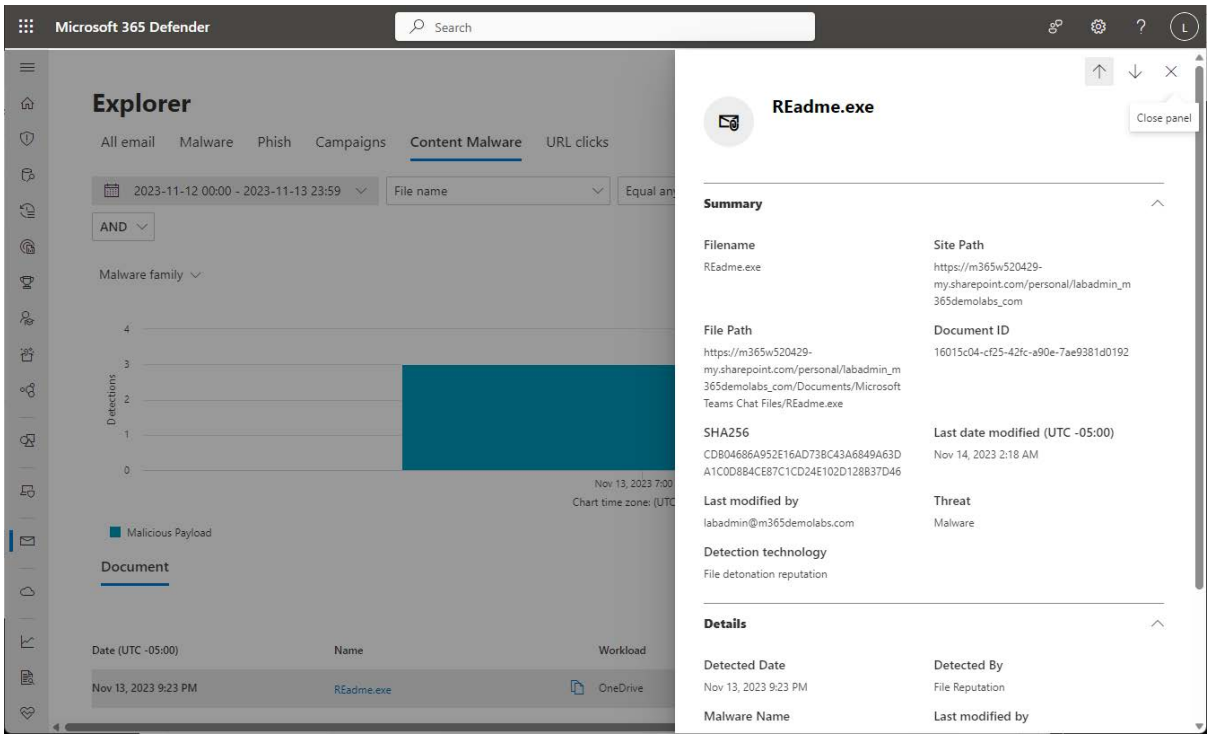

Figure 8.21 – Reviewing a malicious file detection on the Content Malware page

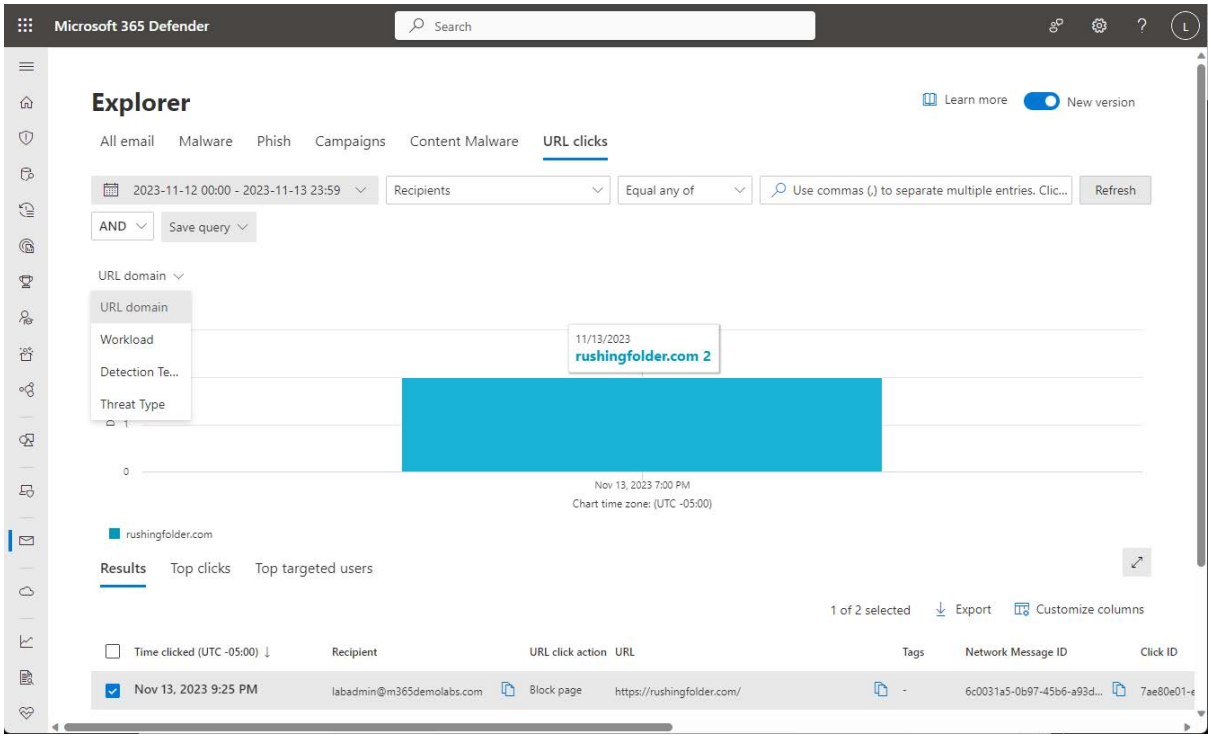

Figure 8.22 – Reviewing the URL clicks page

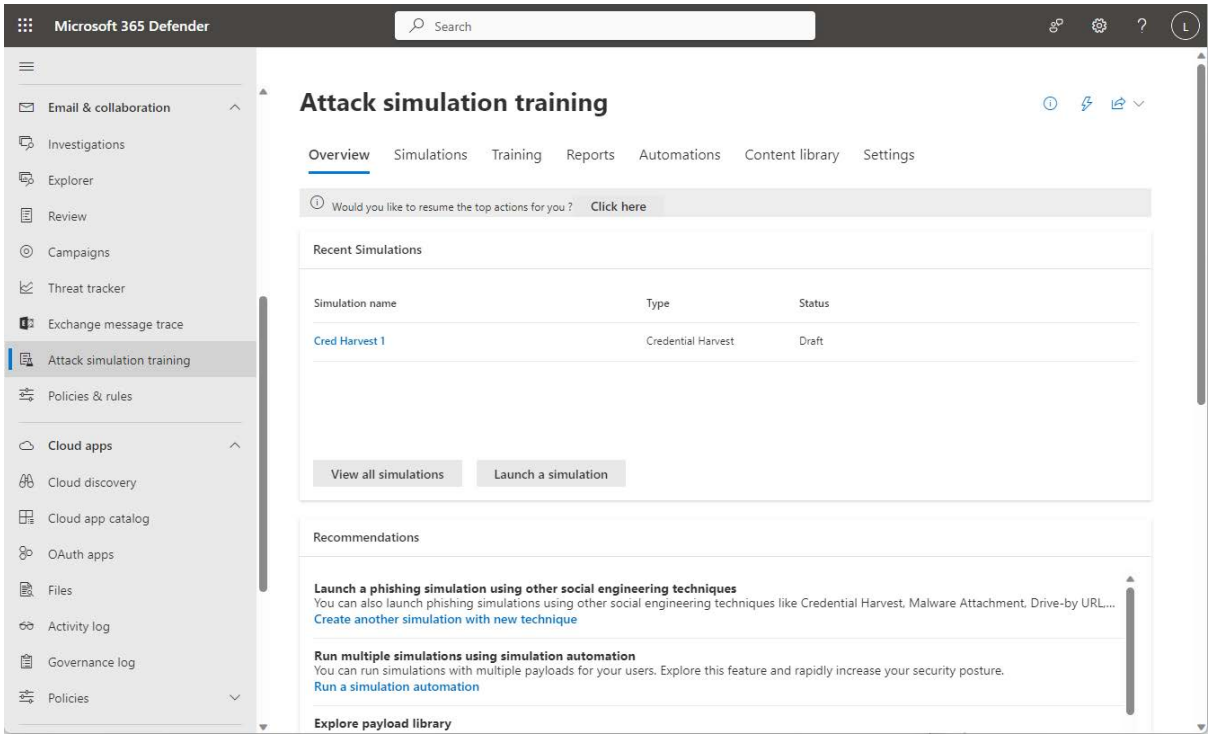

Figure 8.23 – Attack simulation training overview

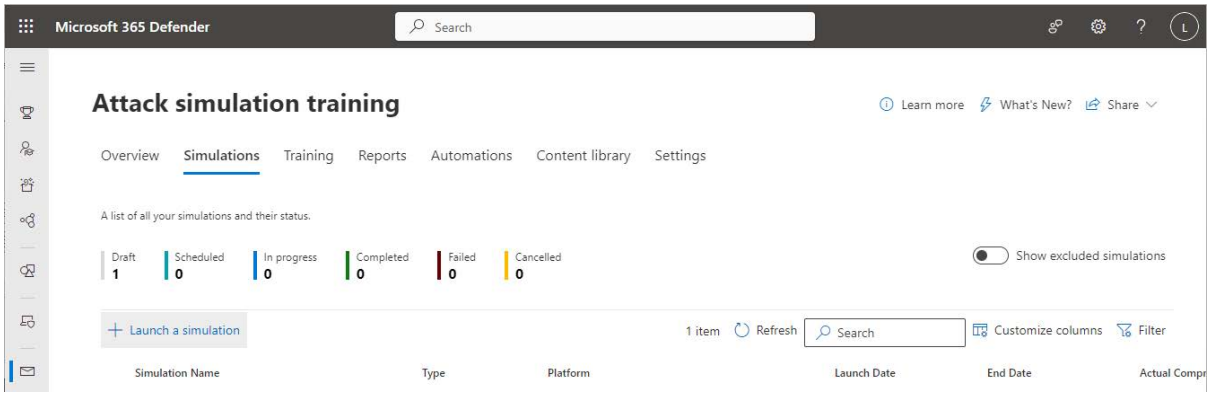

Figure 8.24 – Launching a phishing campaign

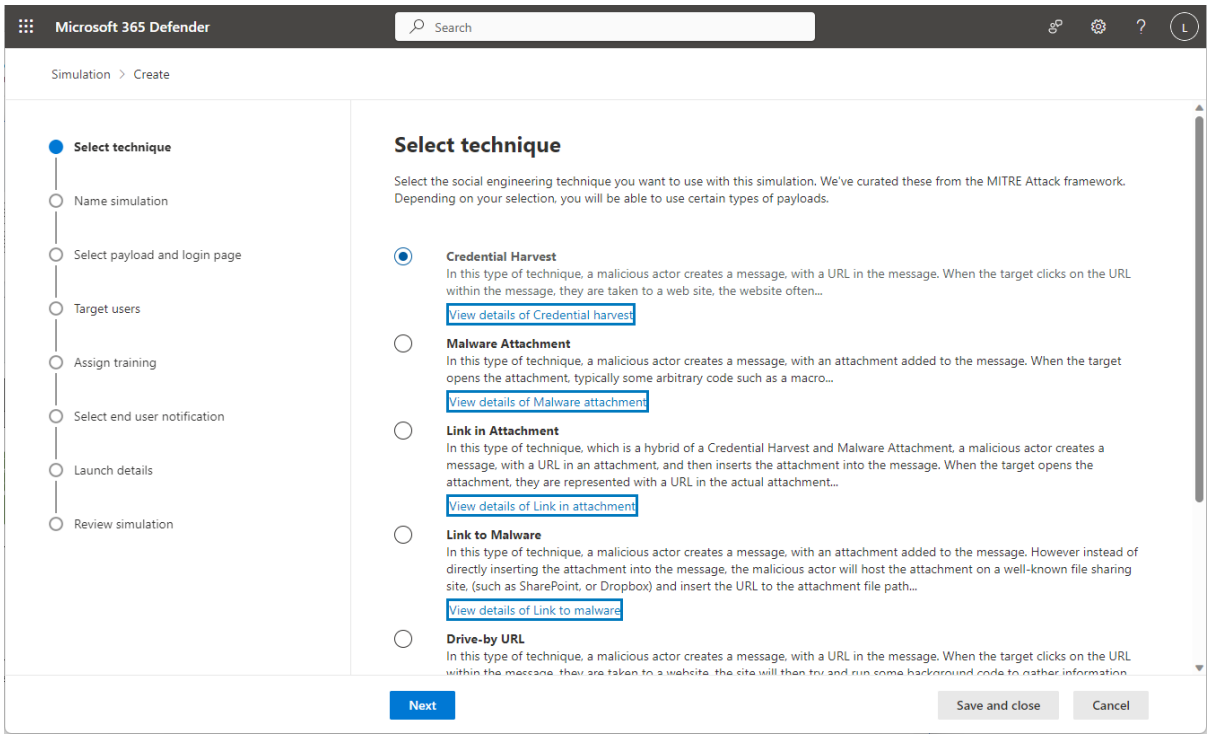

Figure 8.25 – Selecting a technique for the campaign

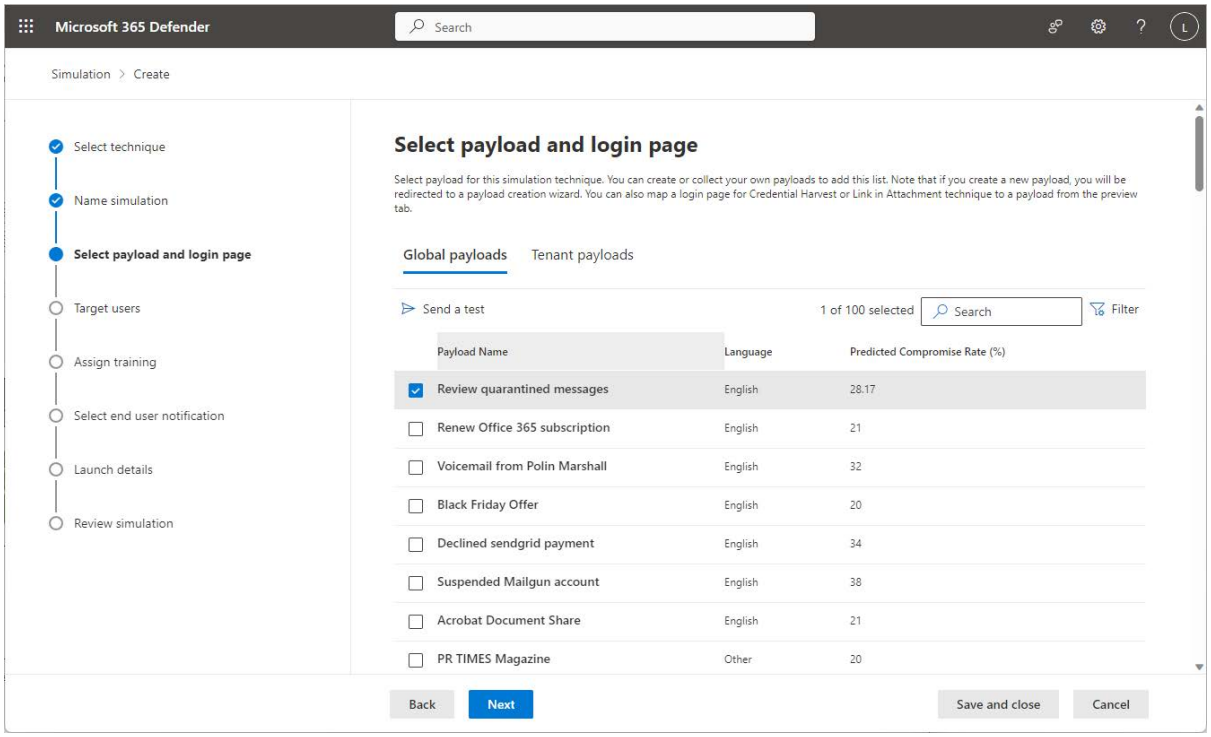

Figure 8.26 – Selecting a payload

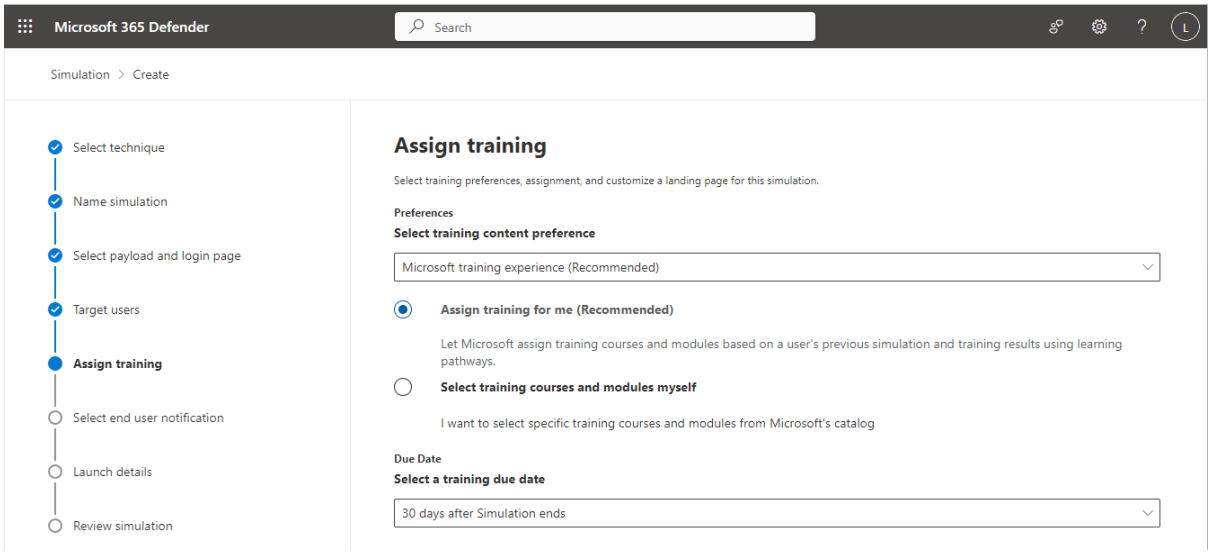

Figure 8.27 – Selecting training options

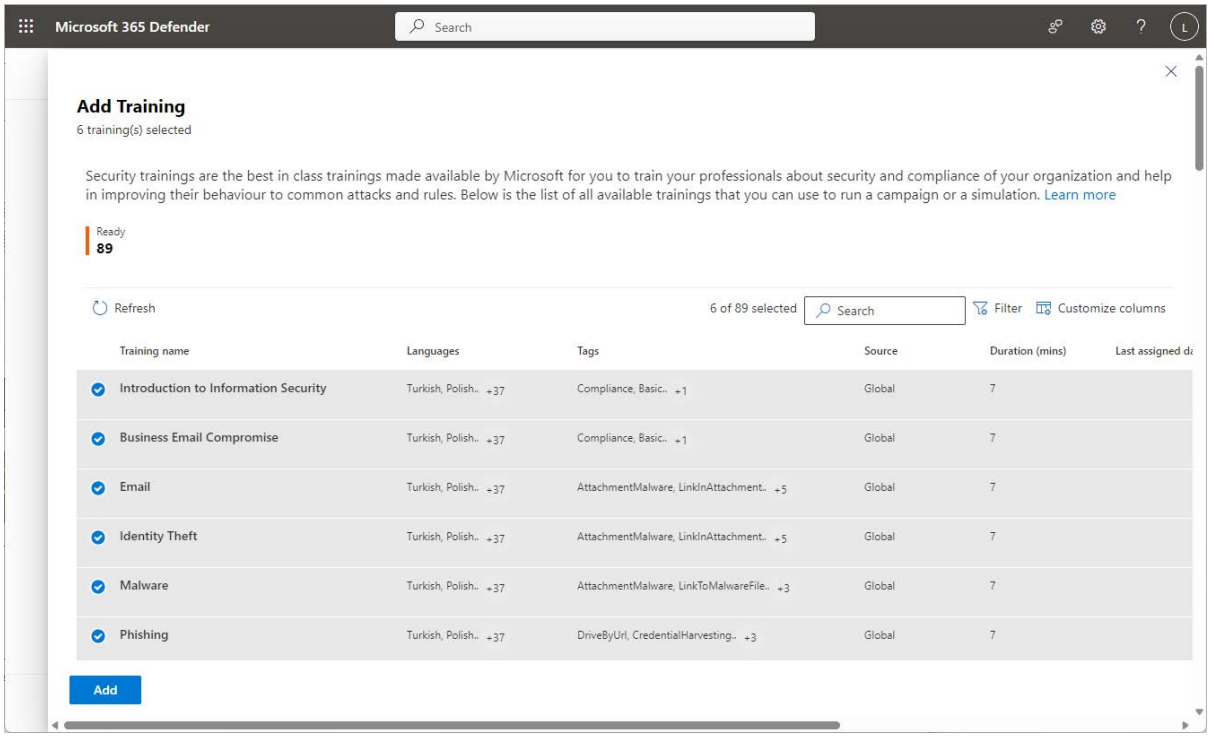

Figure 8.28 – Adding training modules from the built-in catalog

Figure 8.29 – Adding custom training options

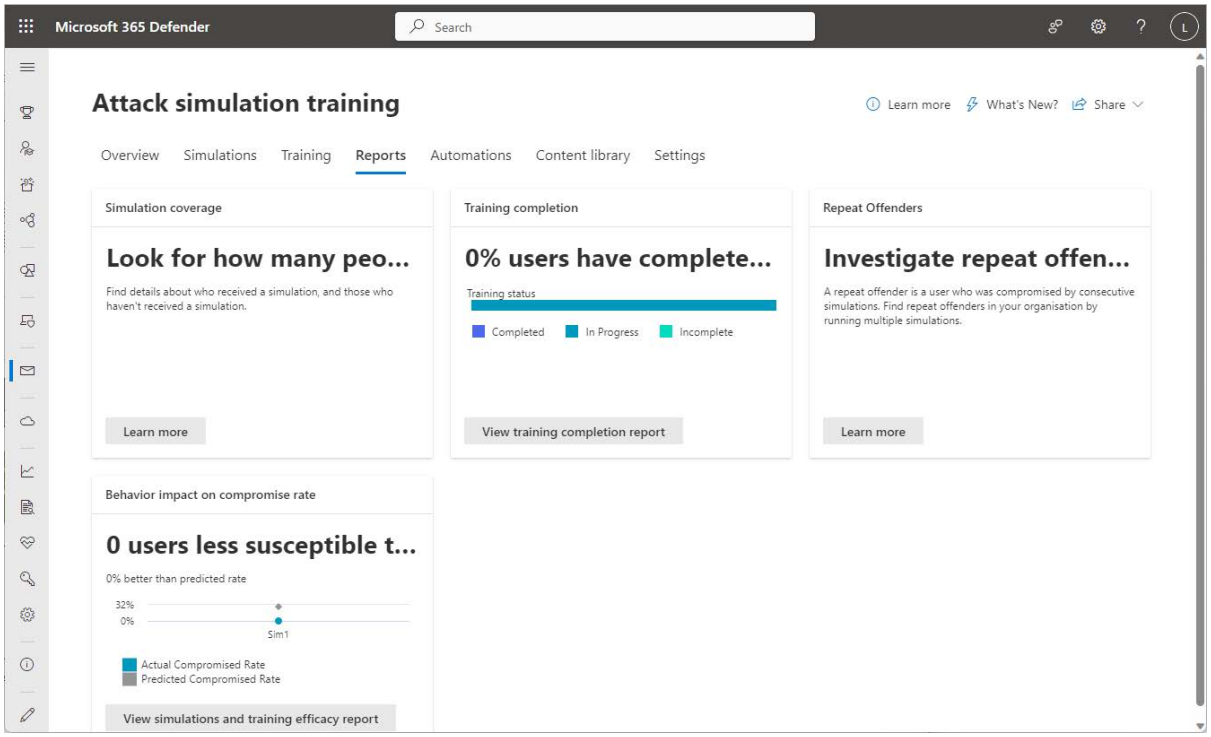

Figure 8.30 – Reviewing training reports

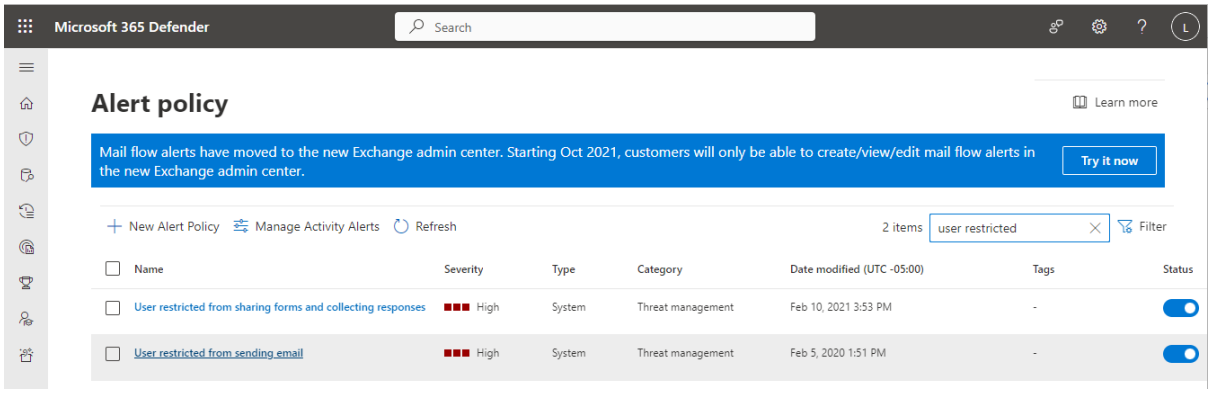

Figure 8.31 – Locating the alert policy

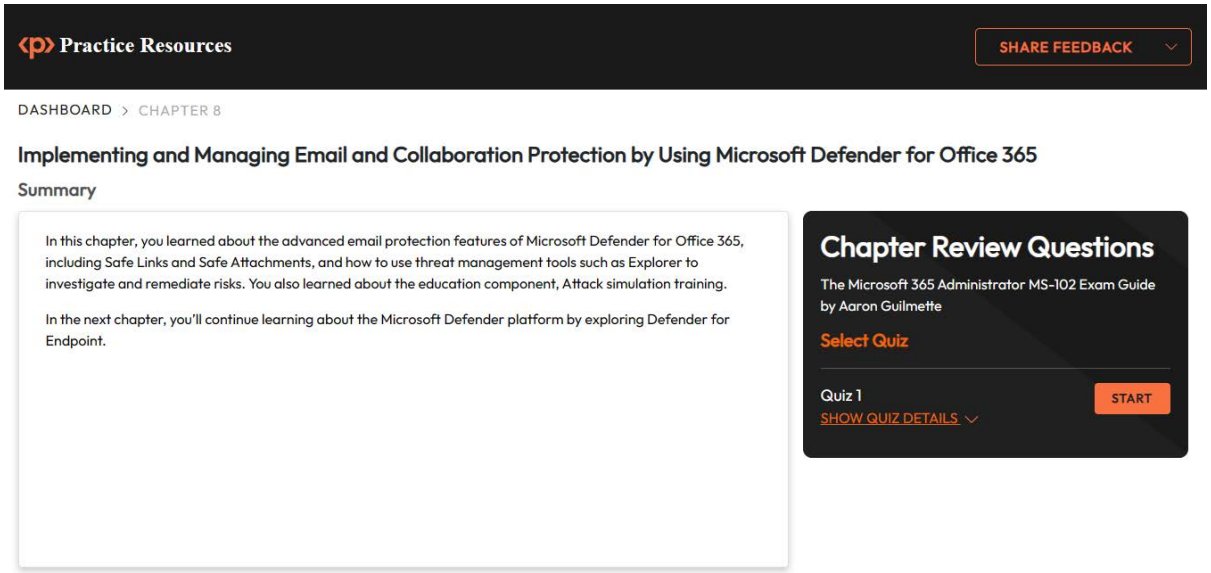

Figure 8.32 – Chapter Review Questions for Chapter 8

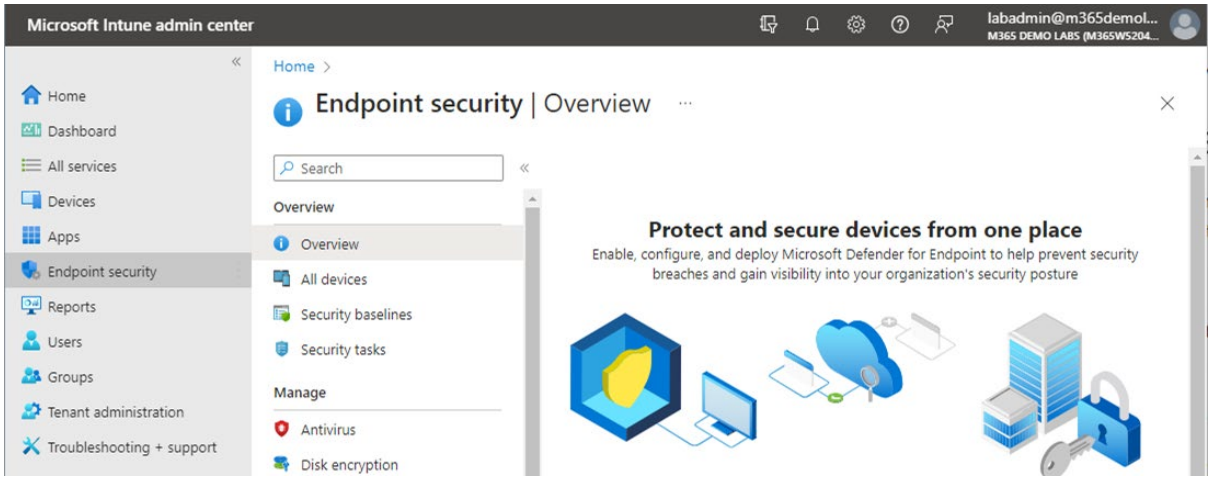

Figure 9.1 – Intune admin center

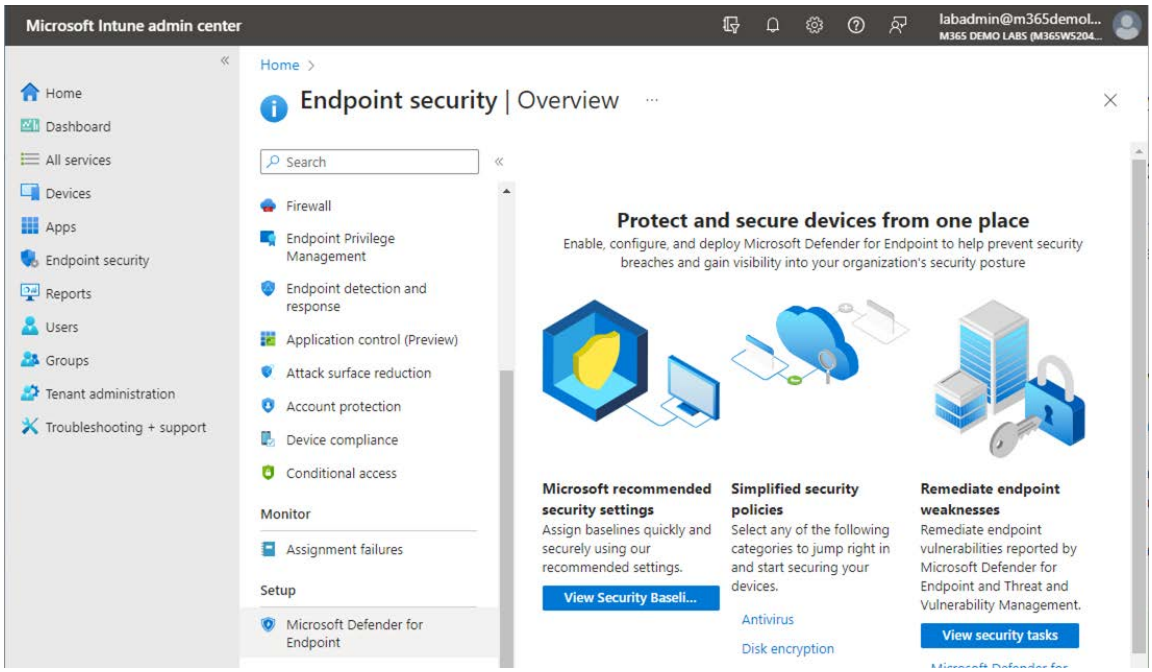

Figure 9.2 – Setting up MDE

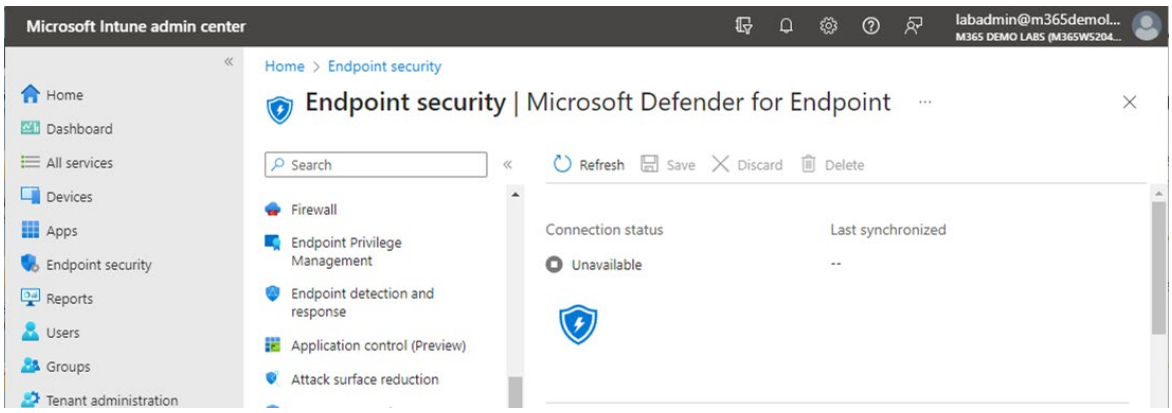

Figure 9.3 – Viewing Intune and Defender connection status

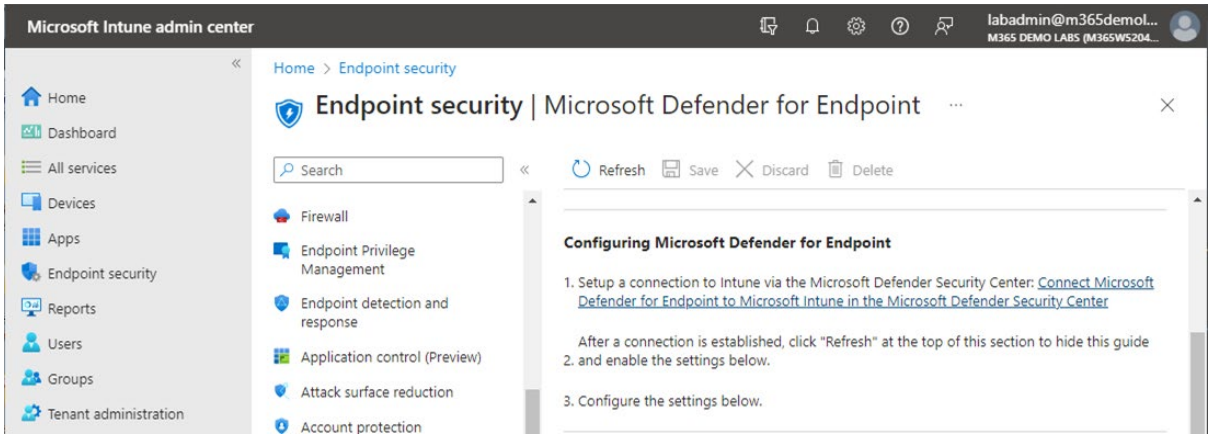

Figure 9.4 – Connecting to the Microsoft 365 Defender Security Center

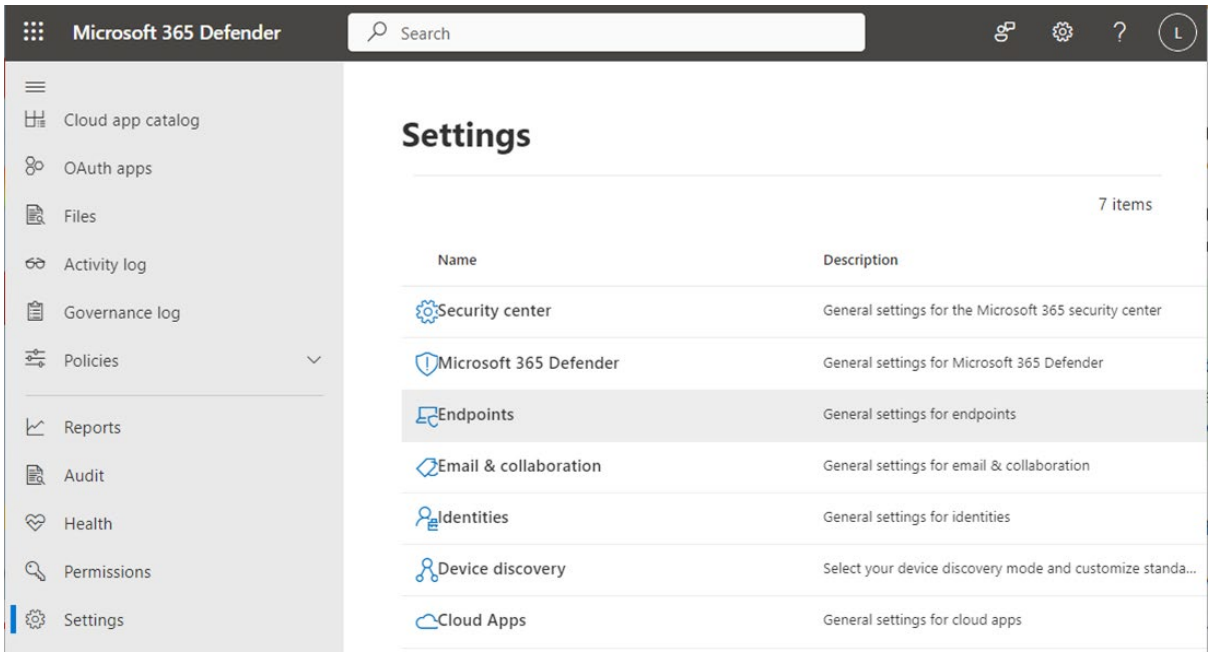

Figure 9.5 – Microsoft 365 Defender portal Settings page

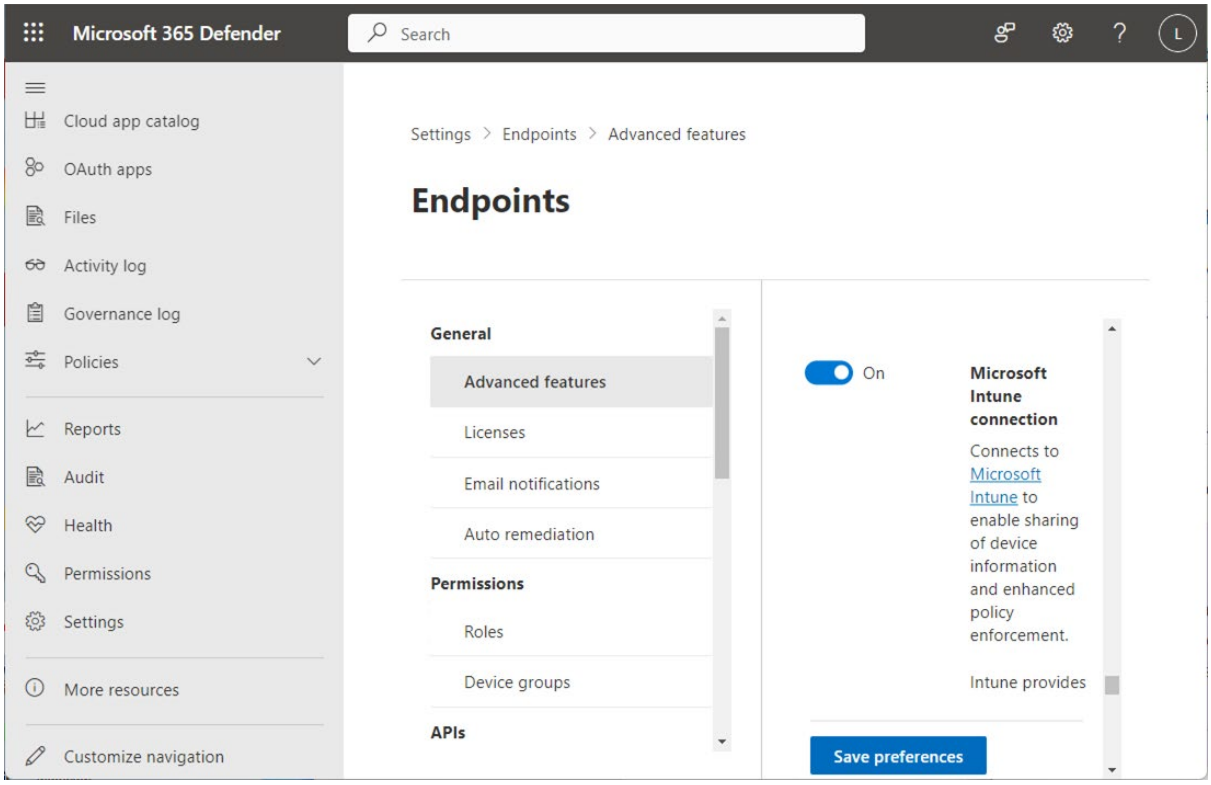

Figure 9.6 – Enabling Microsoft Intune connection

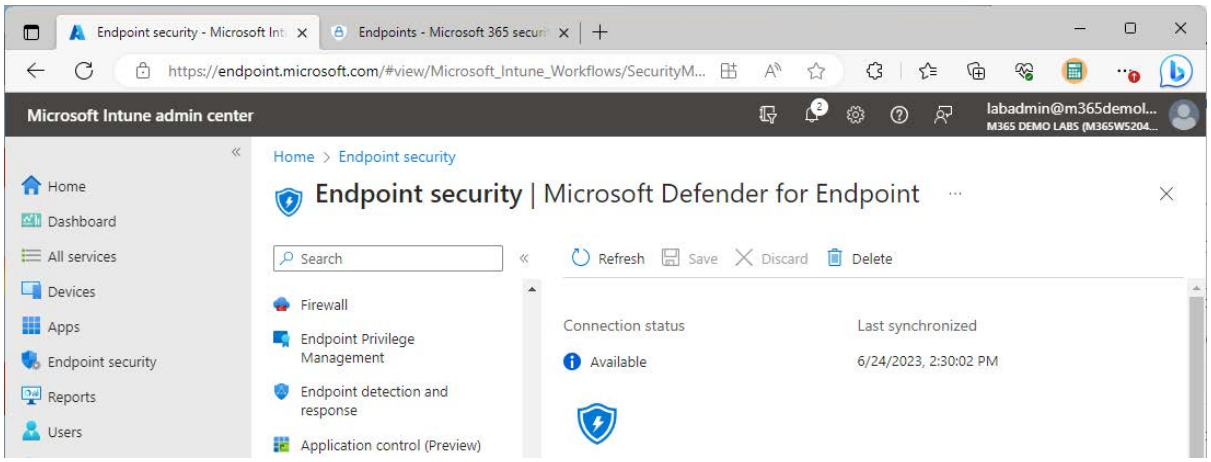

Figure 9.7 – Intune admin center after connection has been established

Figure 9.8 – Compliance policy evaluation section

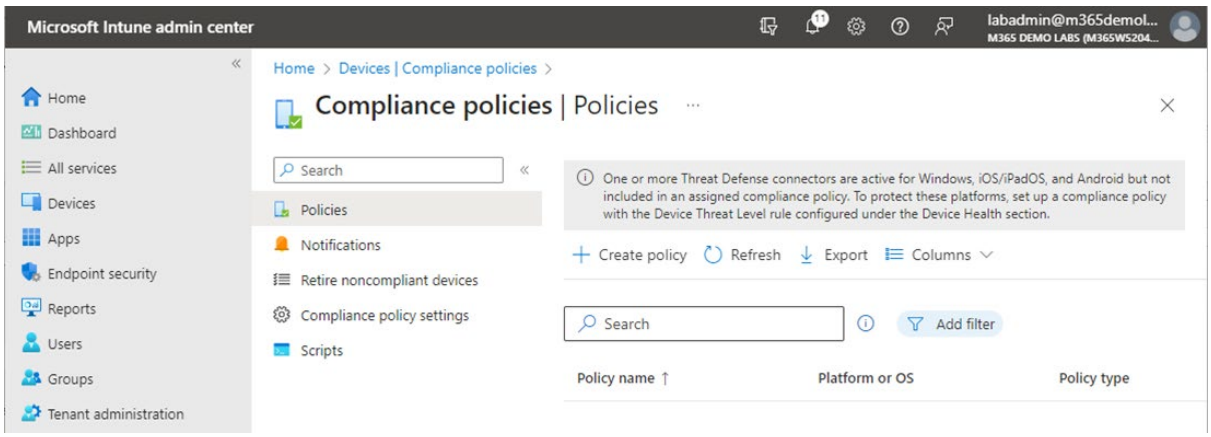

Figure 9.9 – Device Compliance policy page

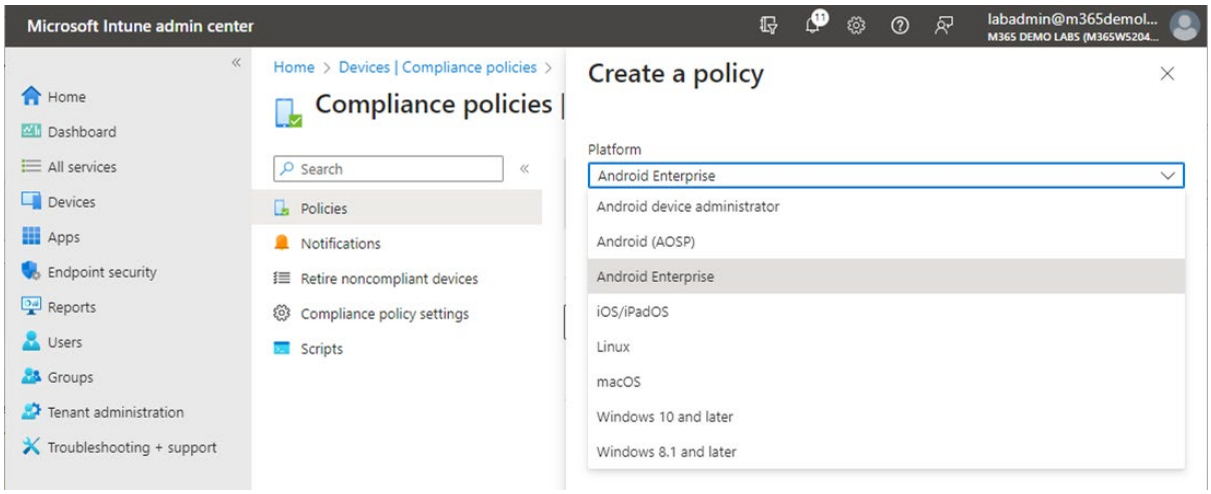

Figure 9.10 – Creating a device compliance policy

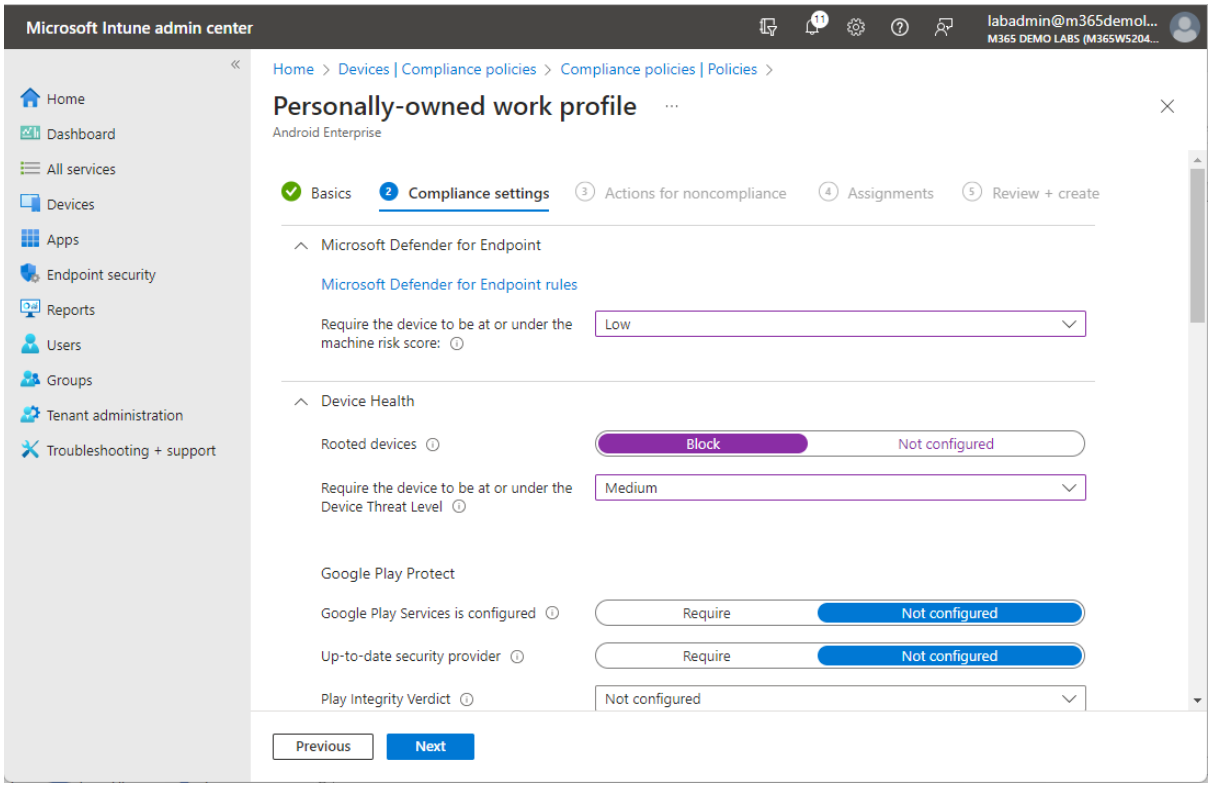

Figure 9.11 – Configuring Compliance settings

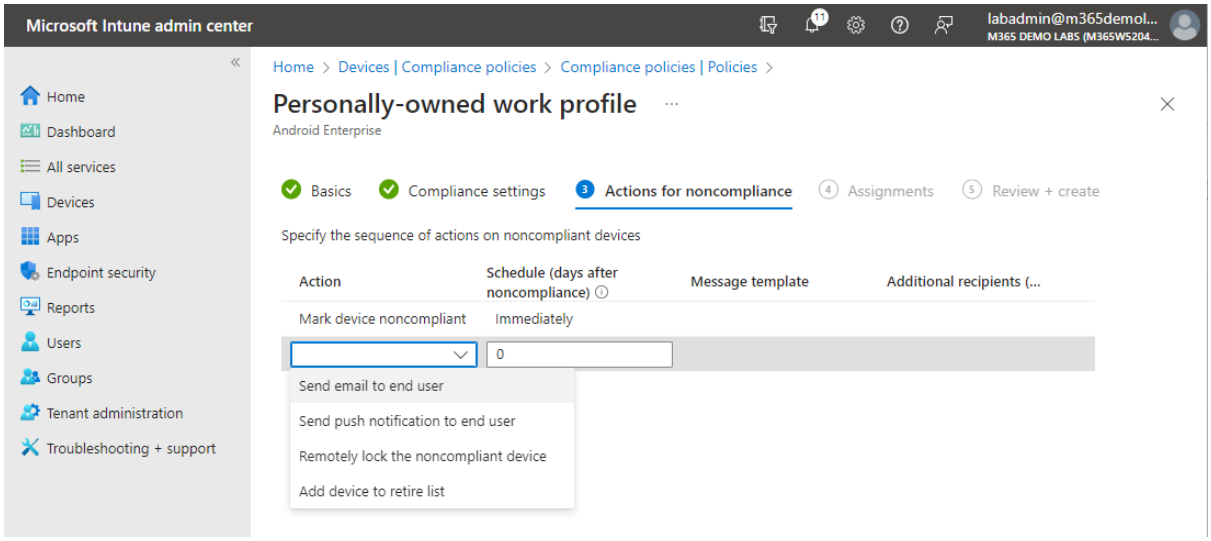

Figure 9.12 – Configuring Actions for noncompliance

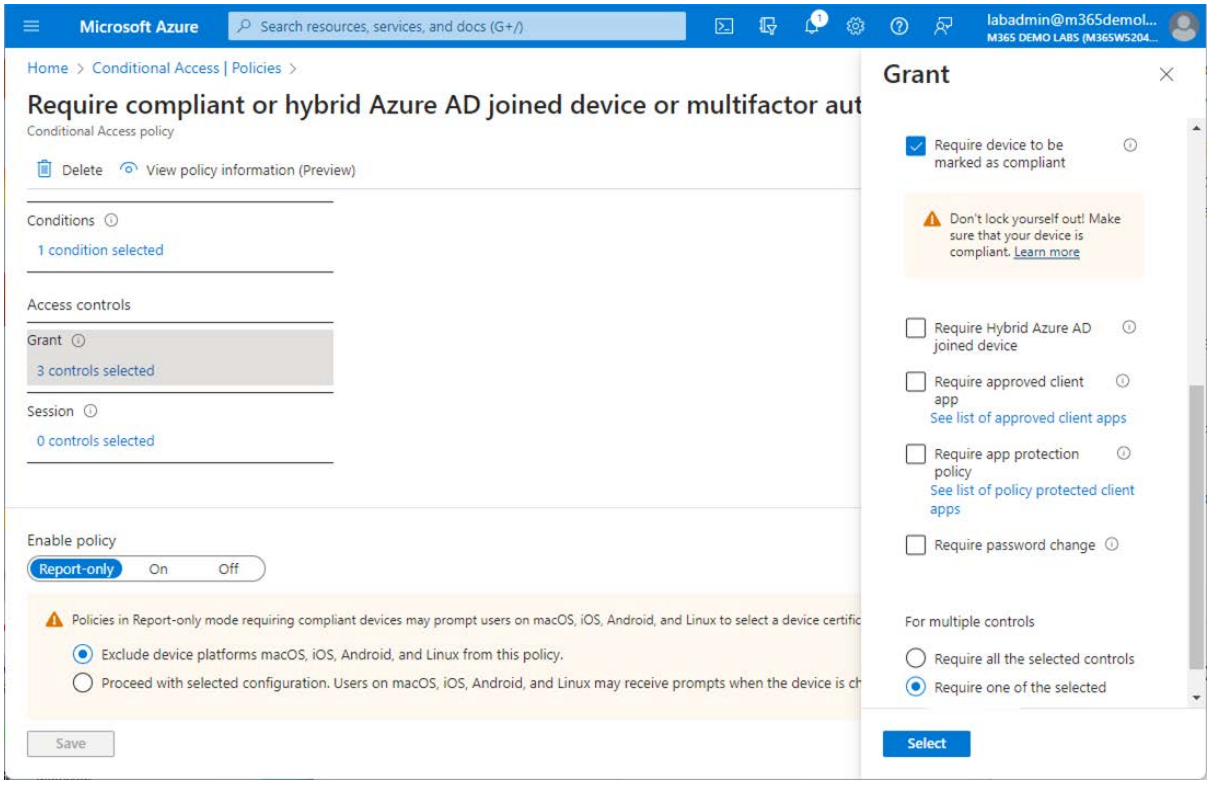

Figure 9.13 – Enabling device compliance as a requirement for Conditional Access policy

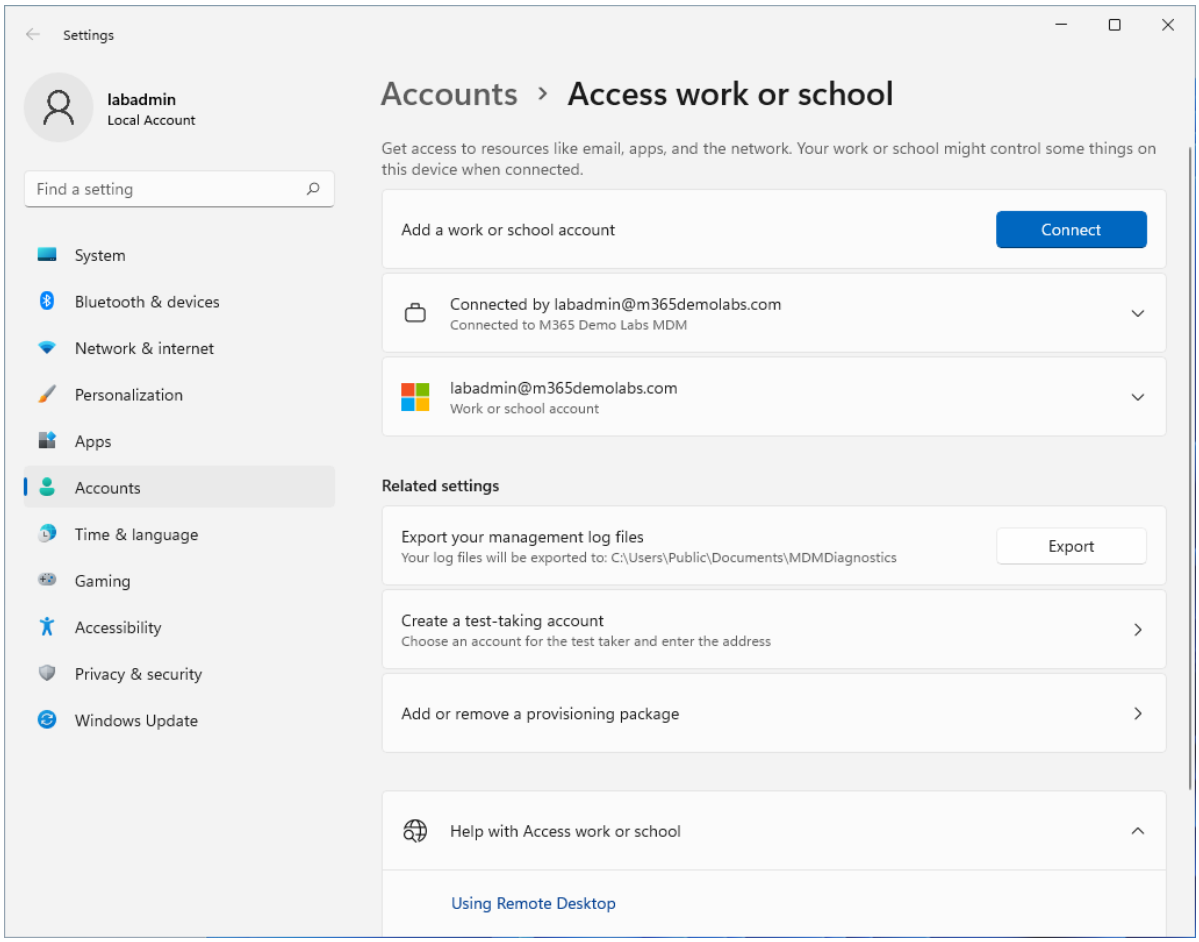

Figure 9.14 – Access work or school screen

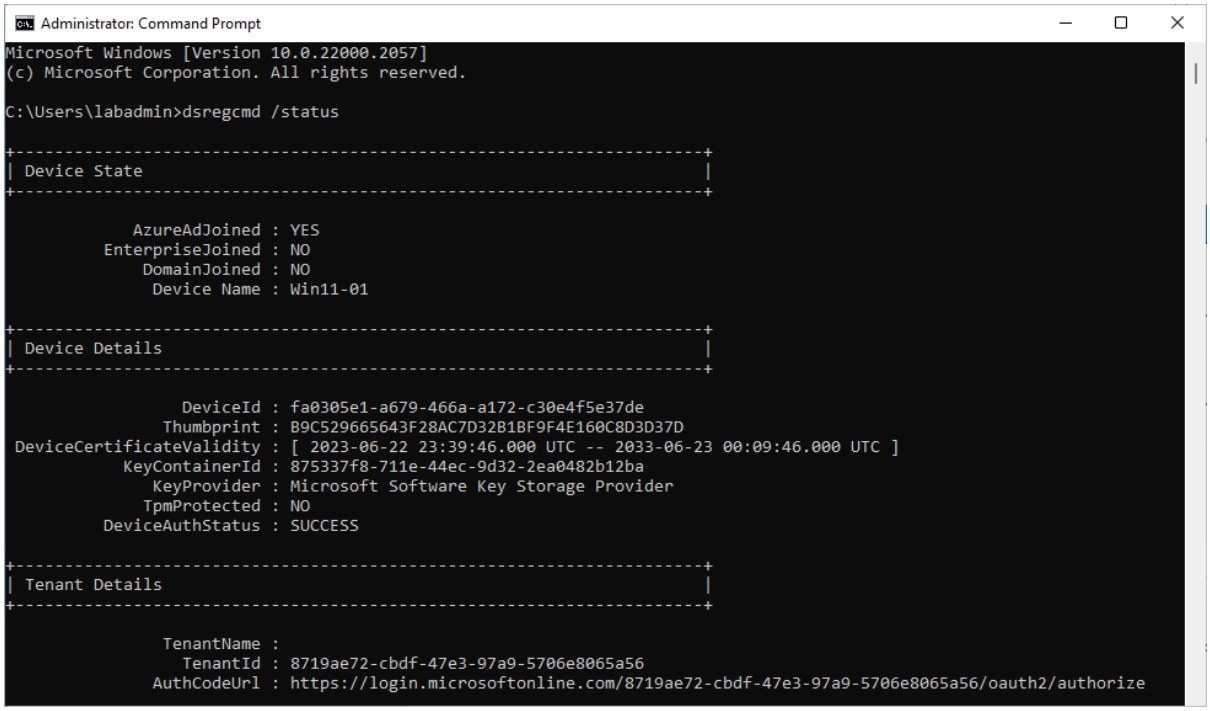

Figure 9.15 – Viewing device join status

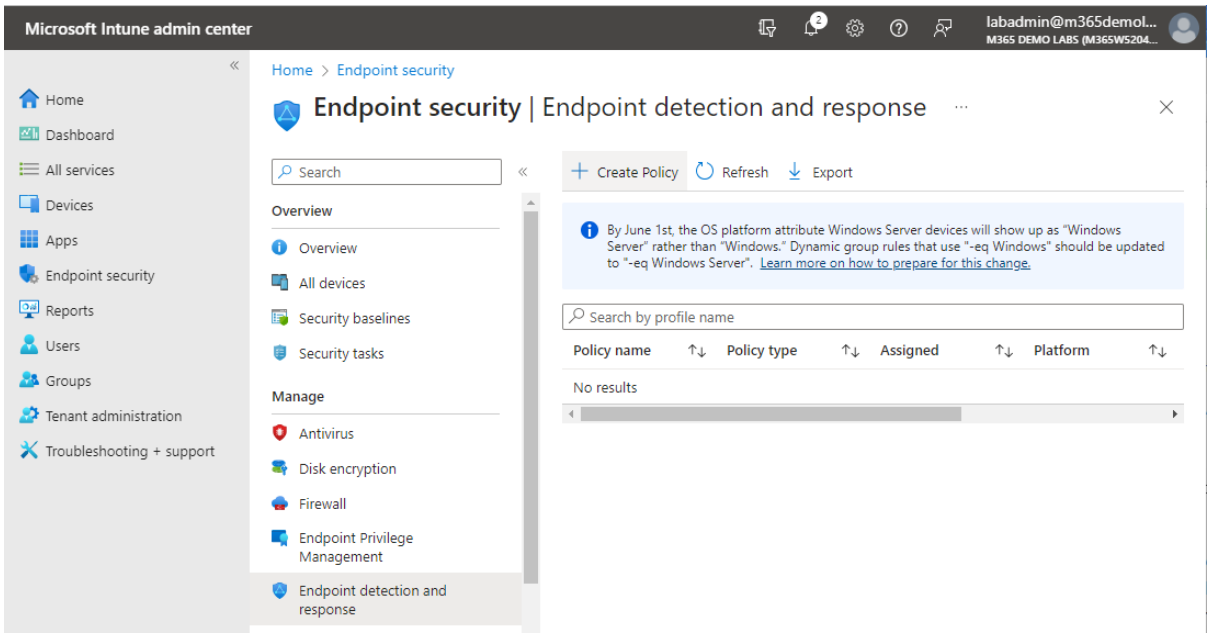

Figure 9.16 – Creating an EDR policy

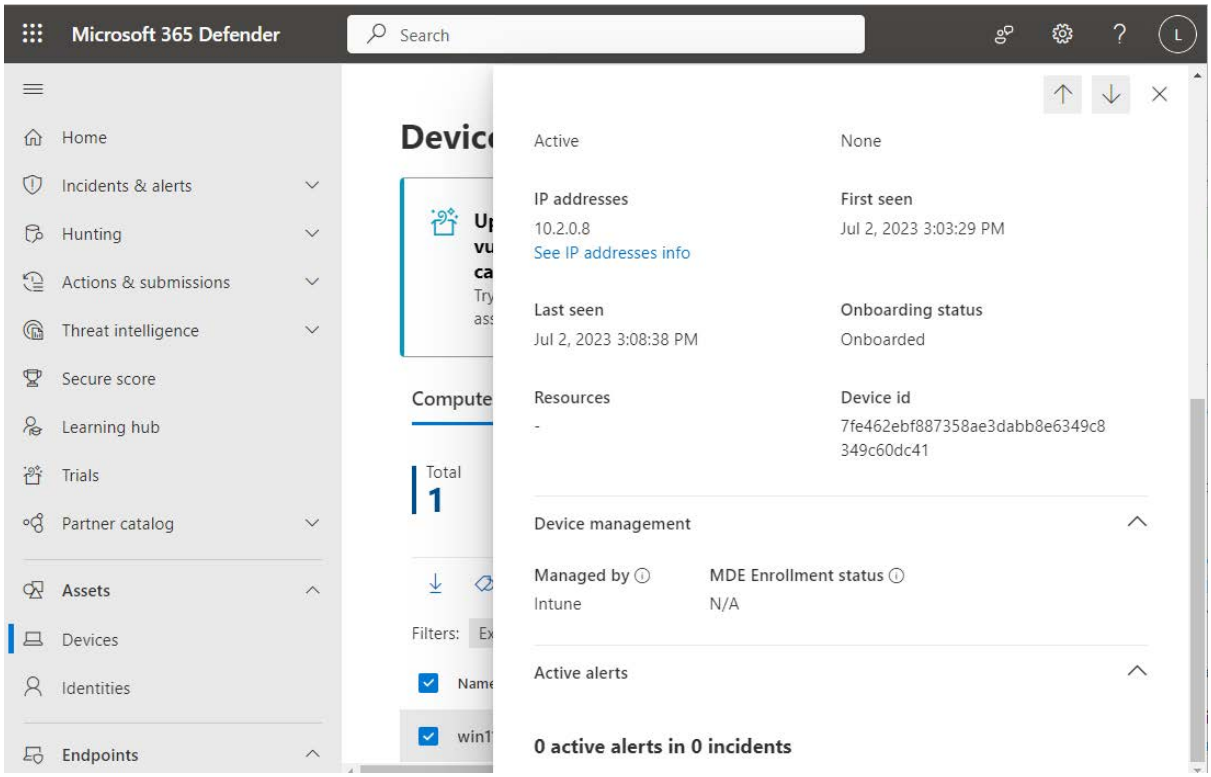

Figure 9.17 – Microsoft 365 Defender admin center device onboarding status

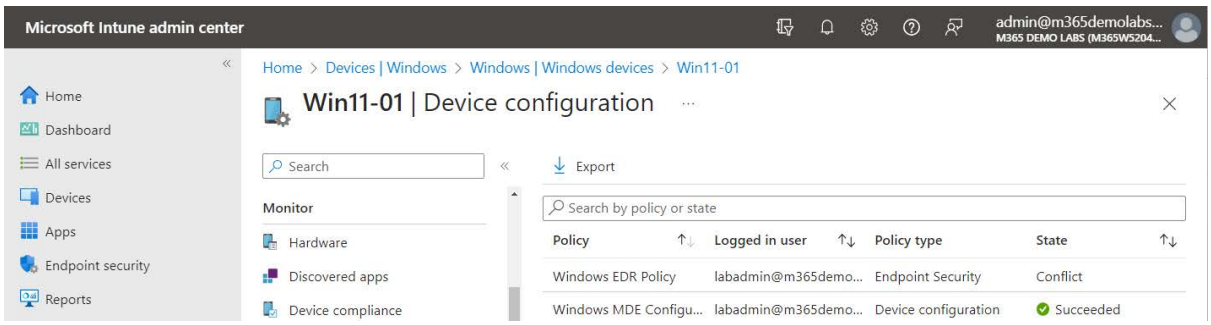

Figure 9.18 – Defender for Endpoint policy conflict

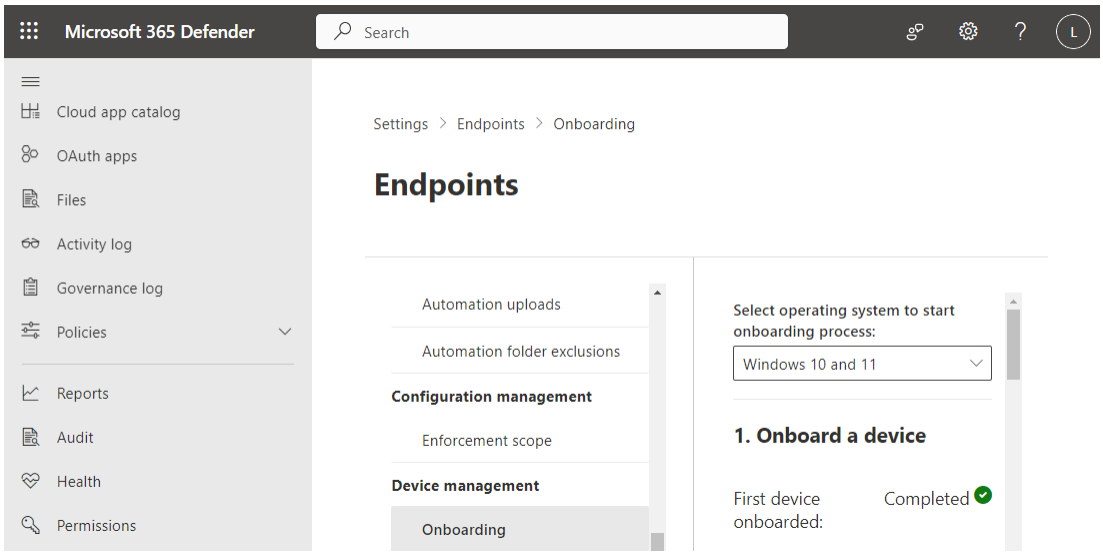

Figure 9.19 – Reviewing endpoint onboarding status

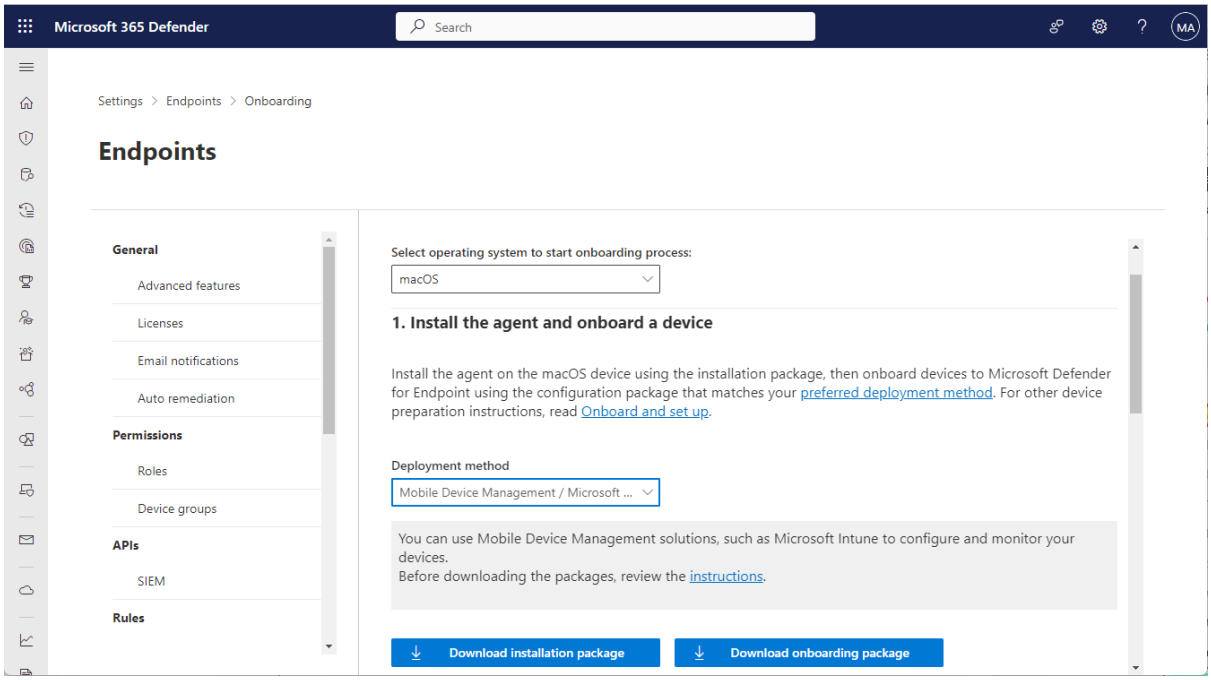

Figure 9.20 – Downloading the onboarding package for macOS

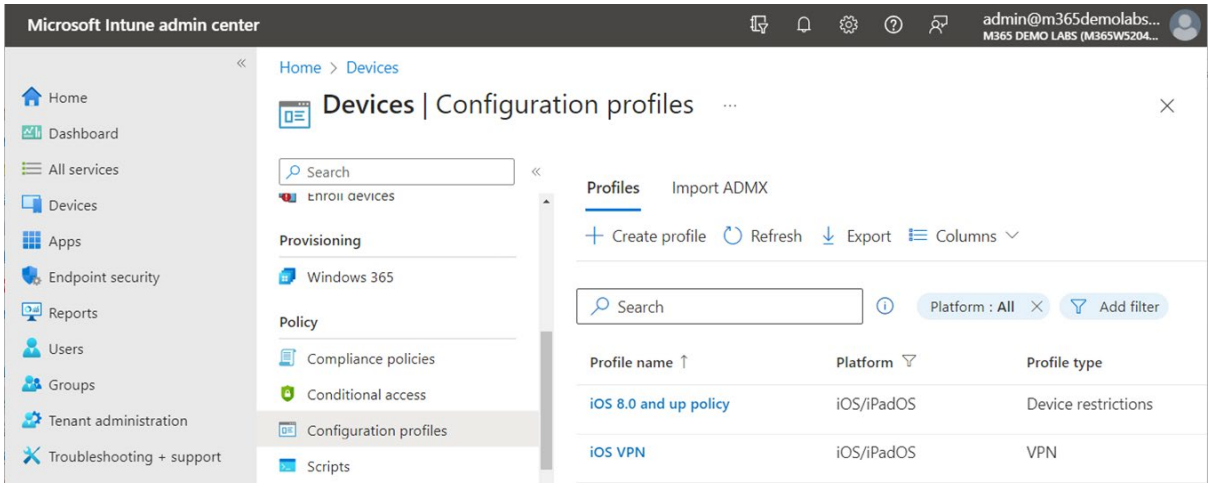

Figure 9.21 – Setting up a new configuration profile

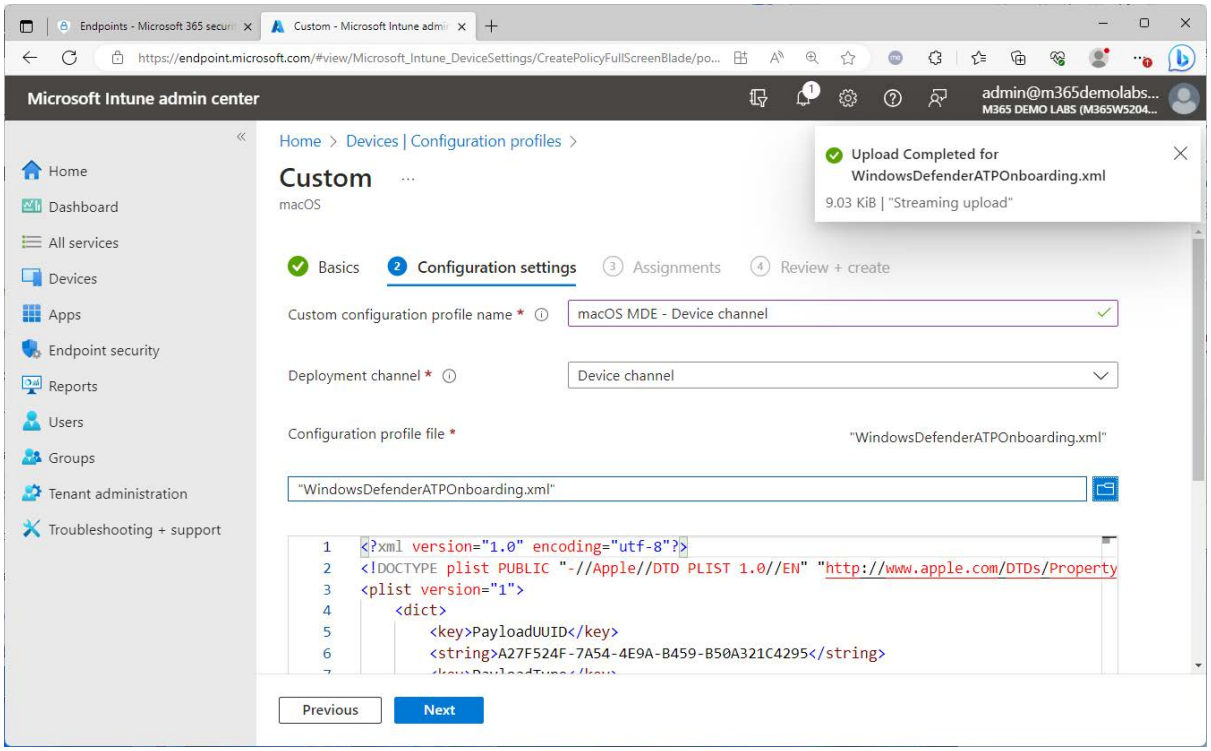

Figure 9.22 – Configuration settings tab

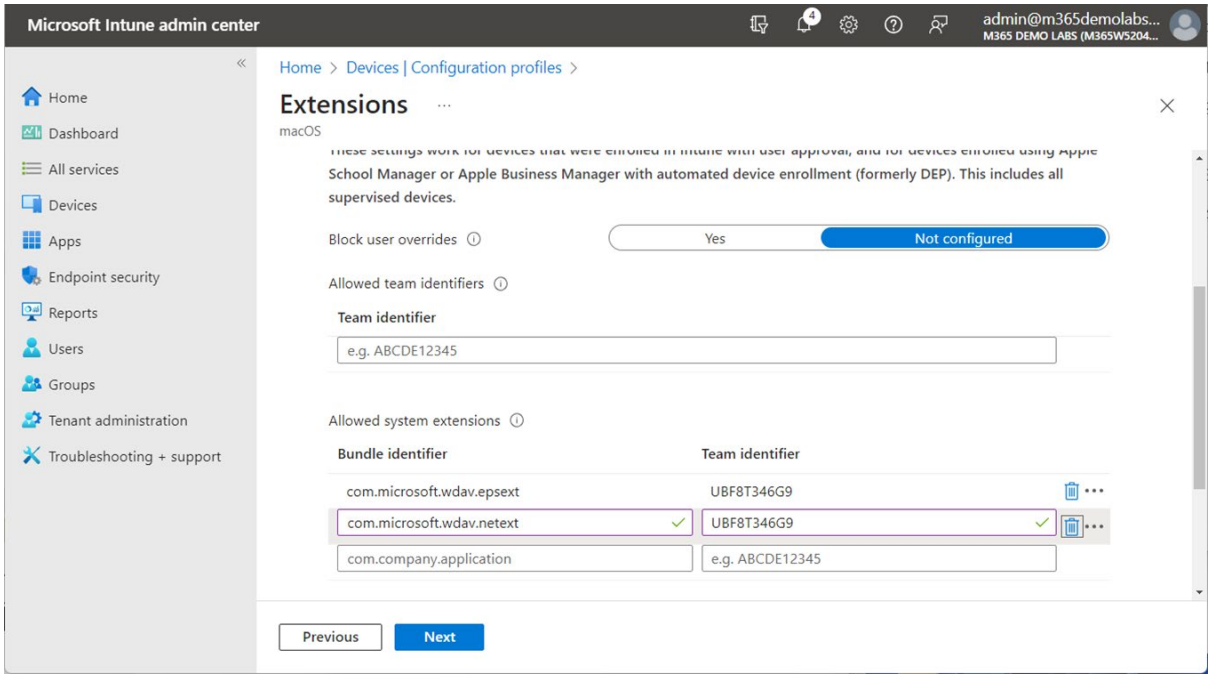

Figure 9.23 – Extension configuration settings

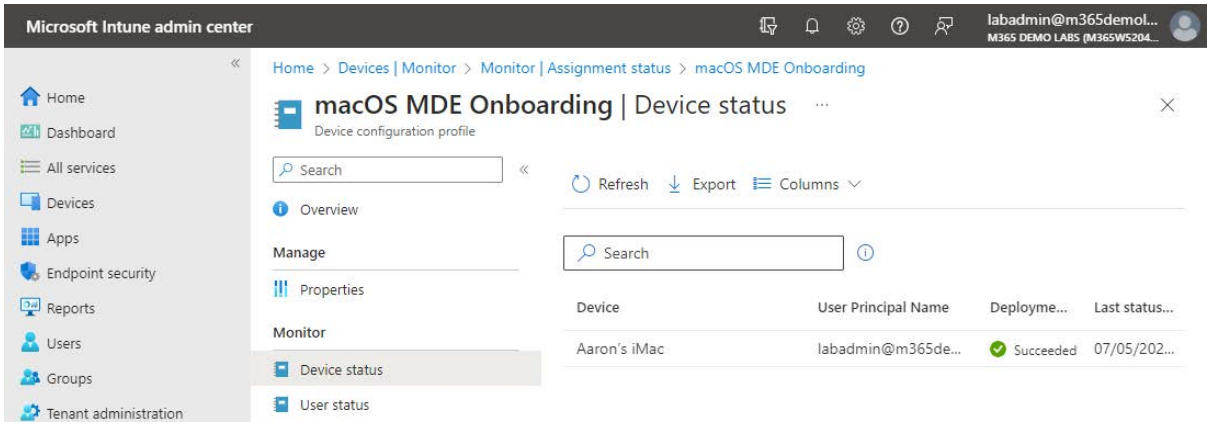

Figure 9.24 – macOS enrolled in Intune

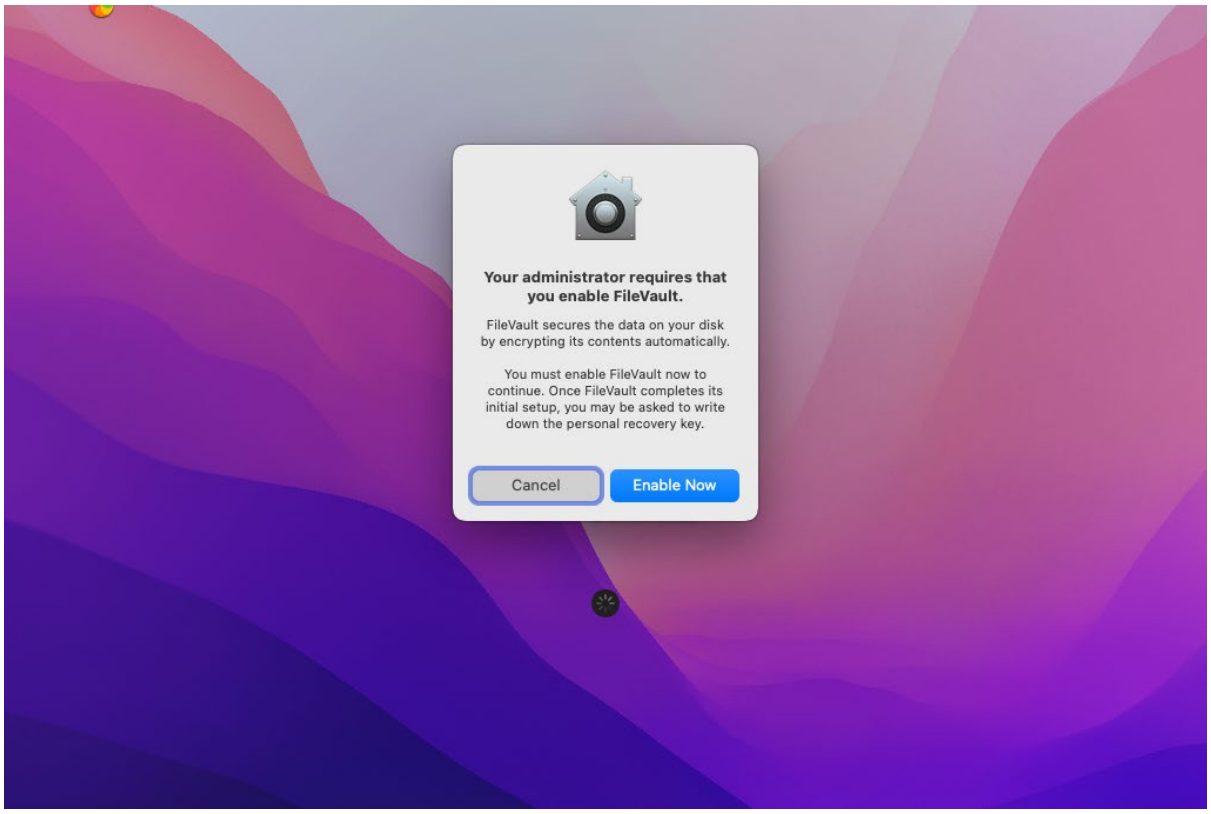

Figure 9.25 – macOS with FileVault encryption policy enabled

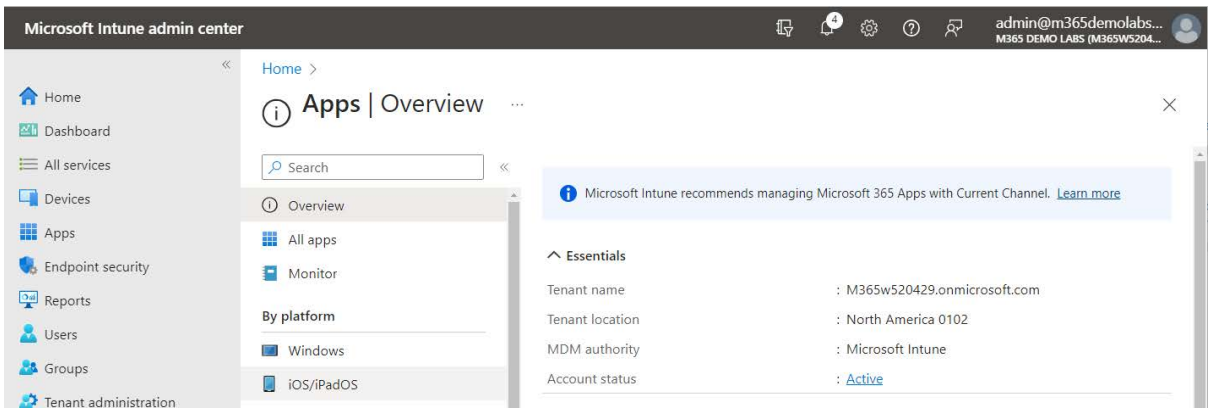

Figure 9.26 – Configuring an iOS app

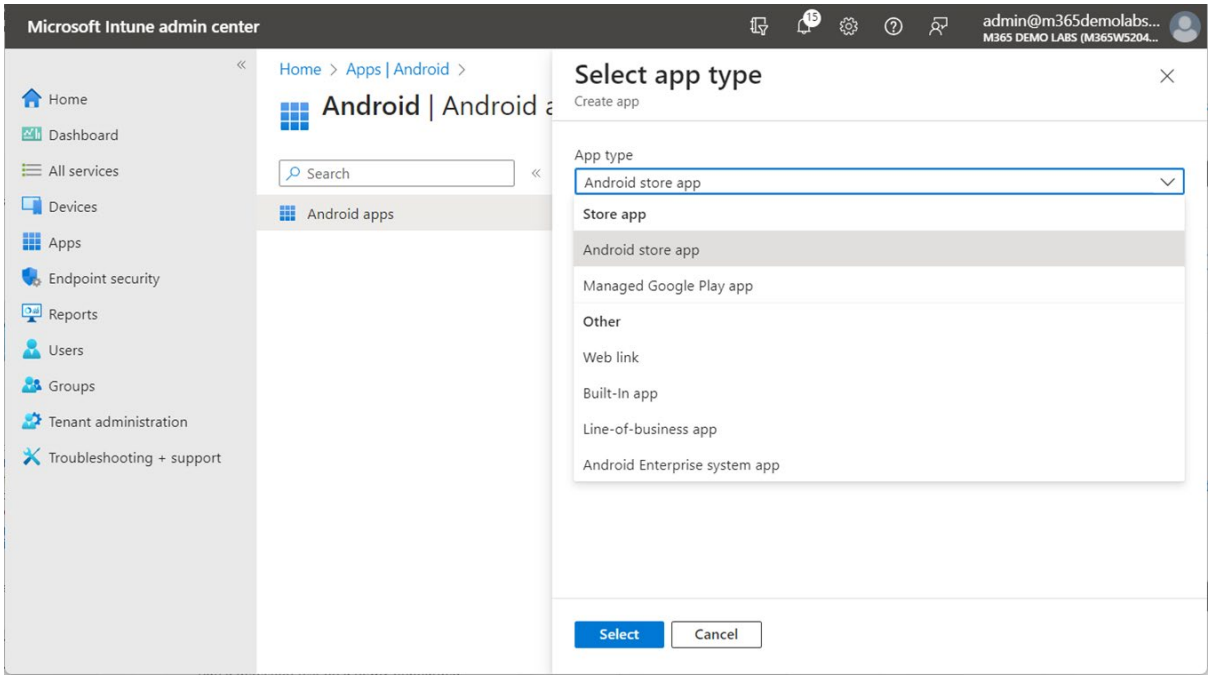

Figure 9.27 – Selecting the Android store app type

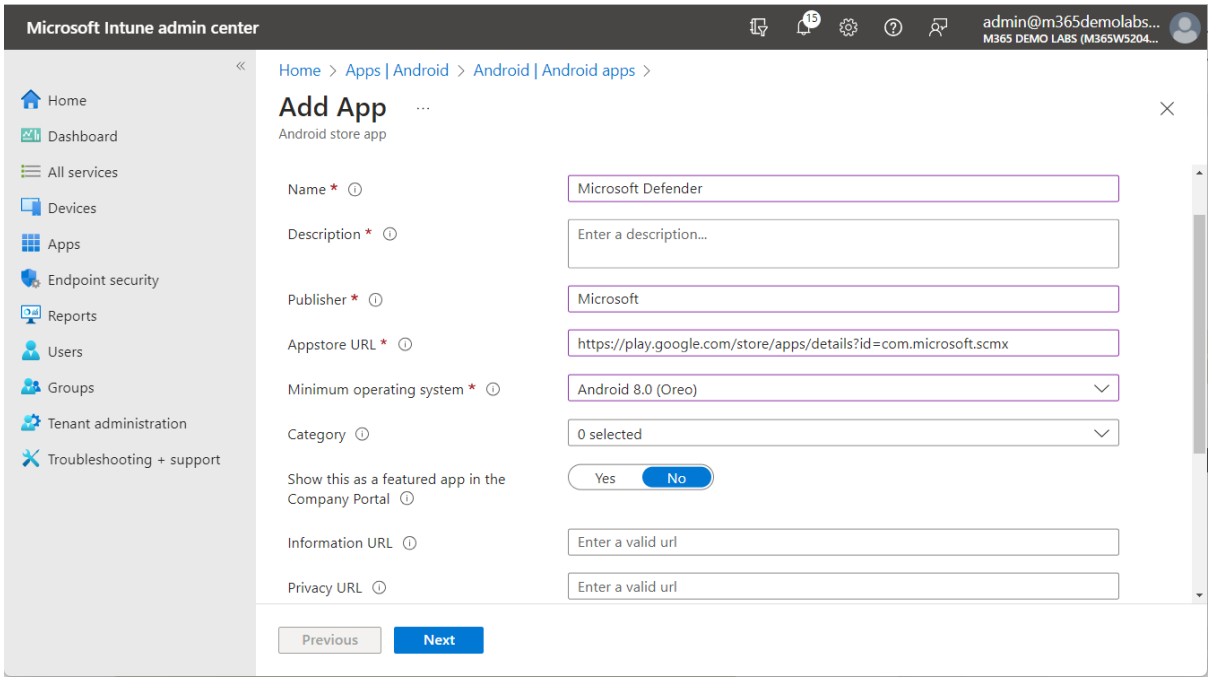

Figure 9.27 – Selecting the Android store app type

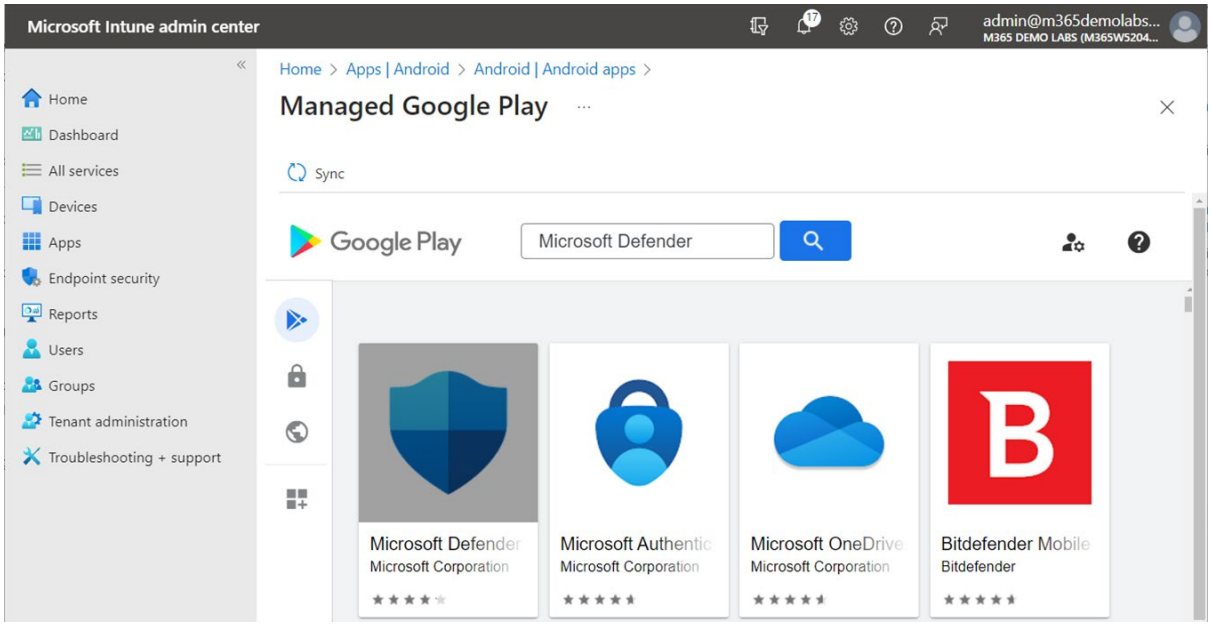

Figure 9.29 – Locating the Microsoft Defender app

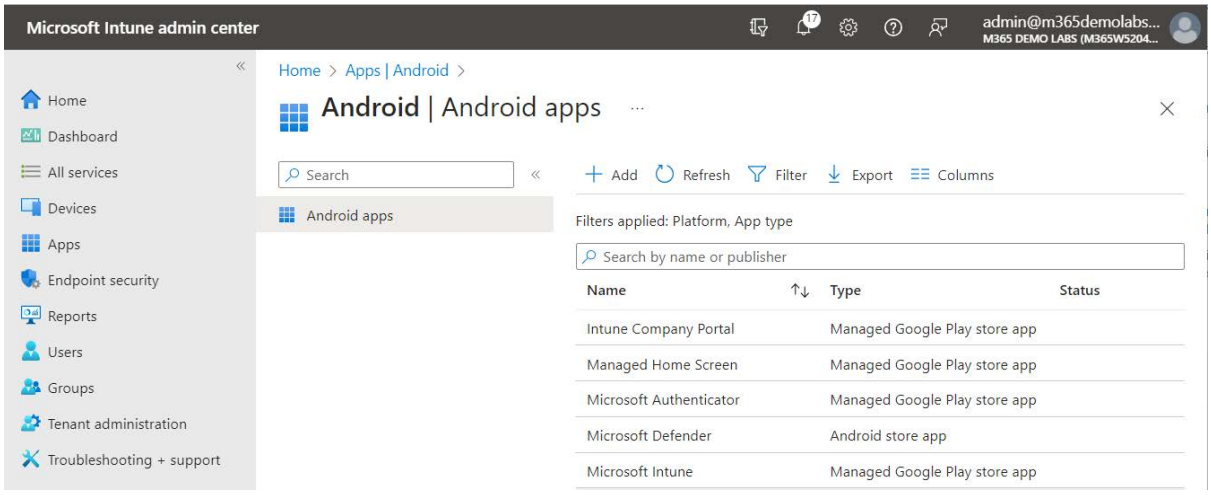

Figure 9.30 – Managed Google Play Store apps

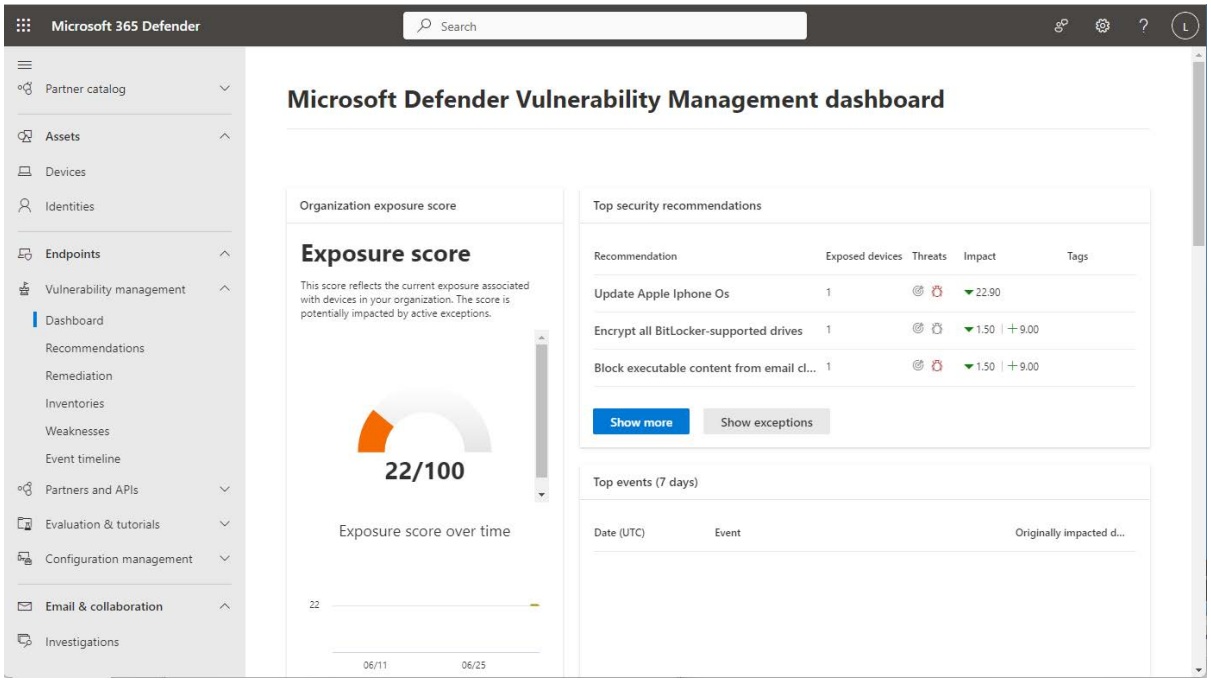

Figure 9.31 – Vulnerability Management dashboard

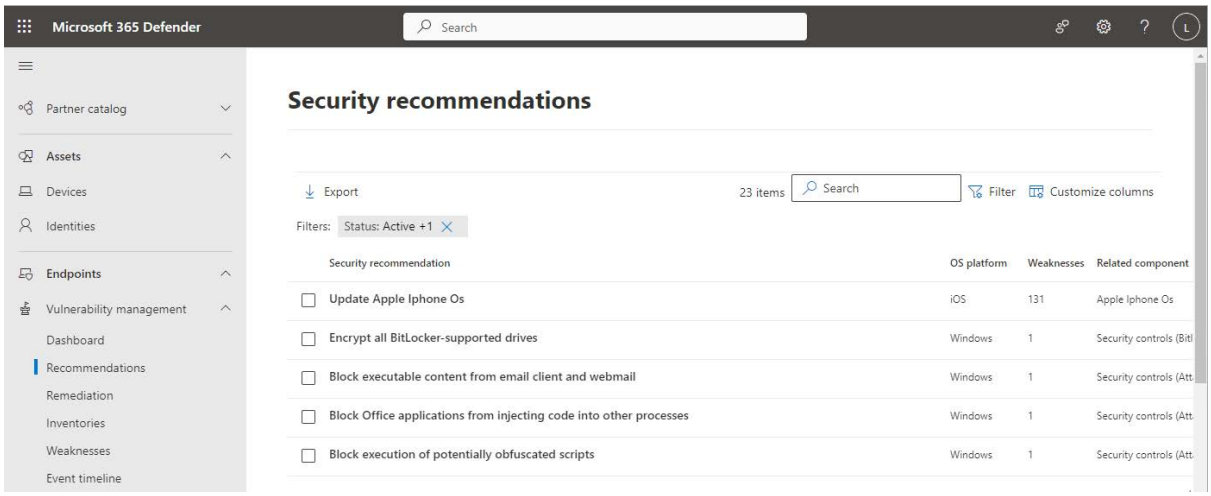

Figure 9.32 – Recommendations page

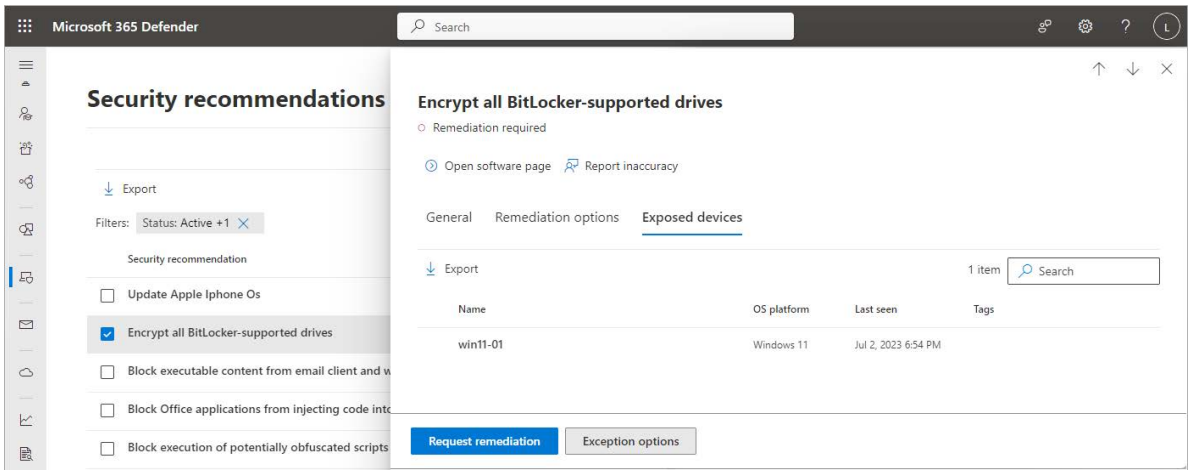

Figure 9.33 – Request remediation

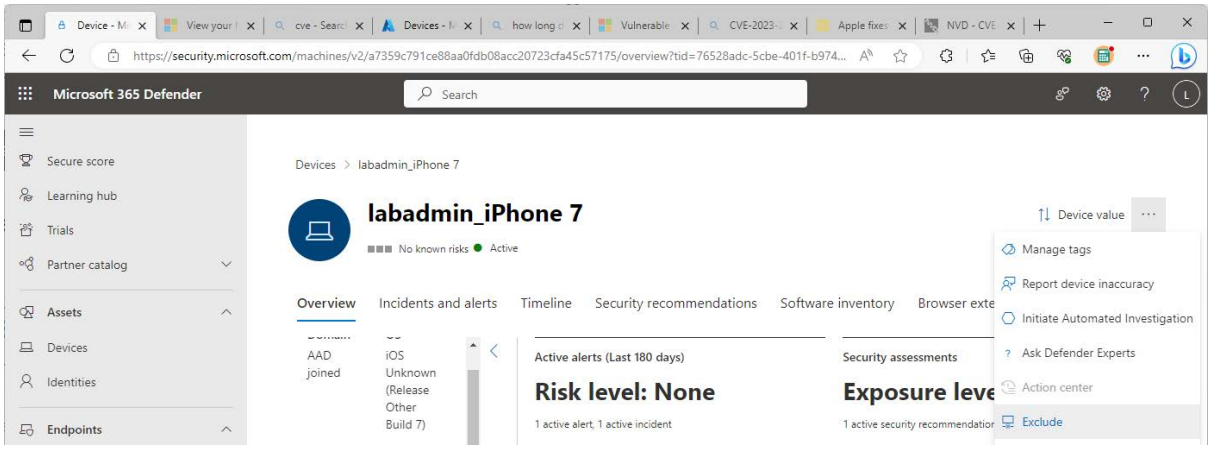

Figure 9.34 – Excluding a device from Threat Management

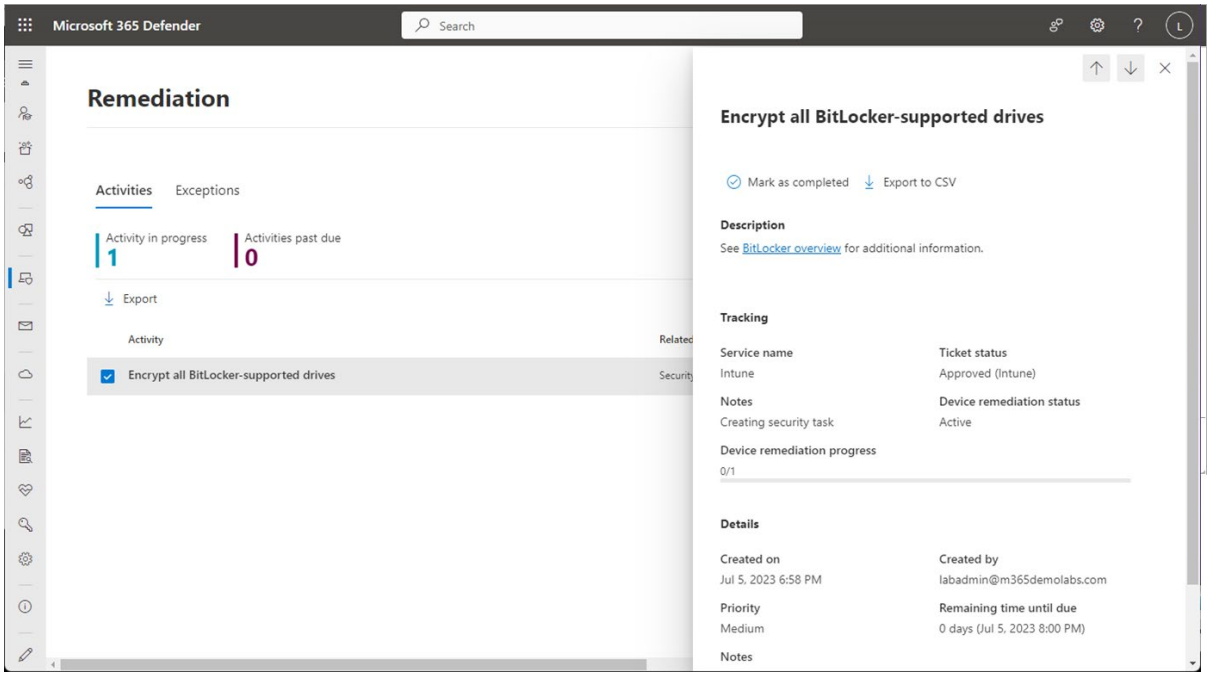

Figure 9.35 – Remediation page

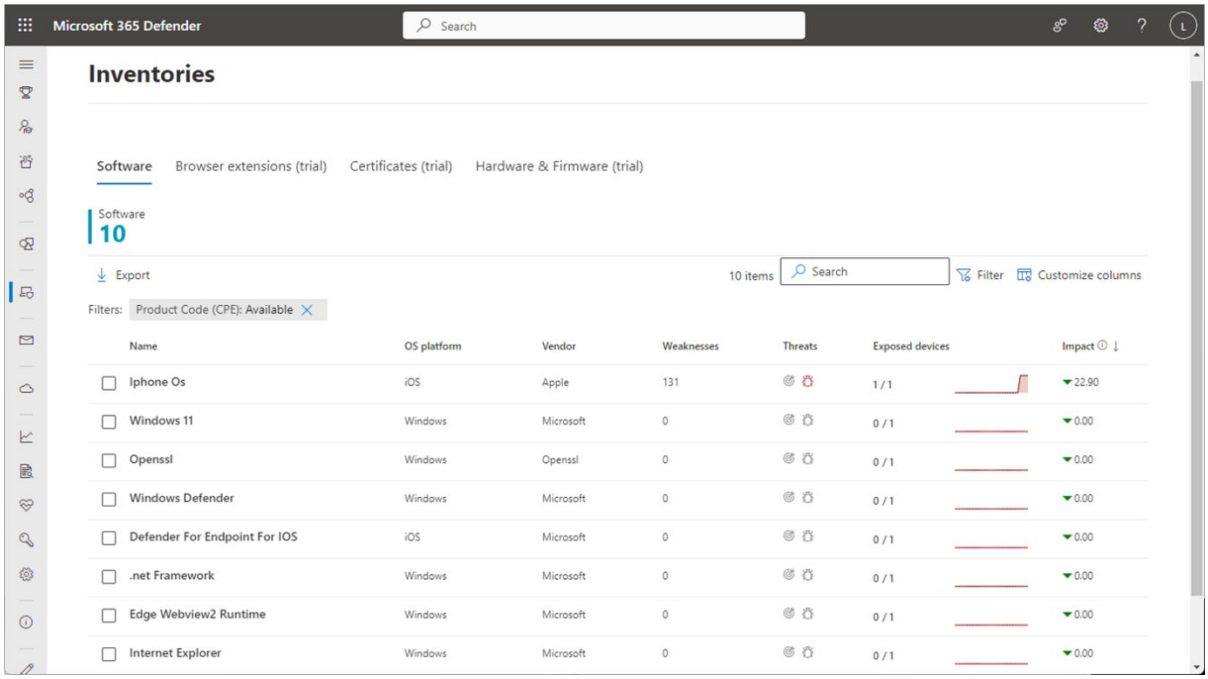

Figure 9.36 – Inventories page

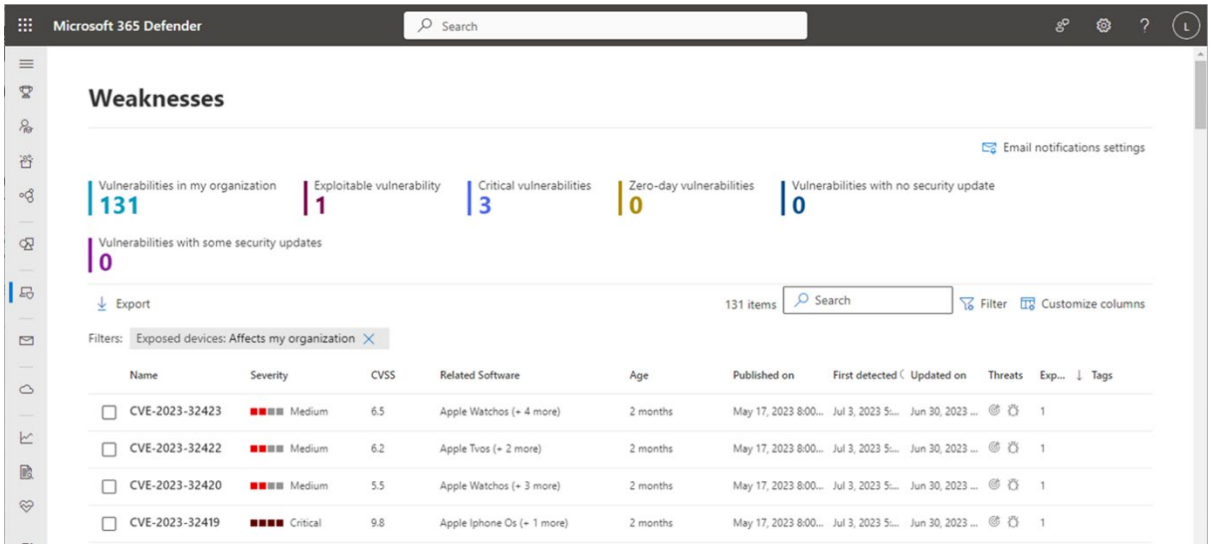

Figure 9.37 – Weaknesses page

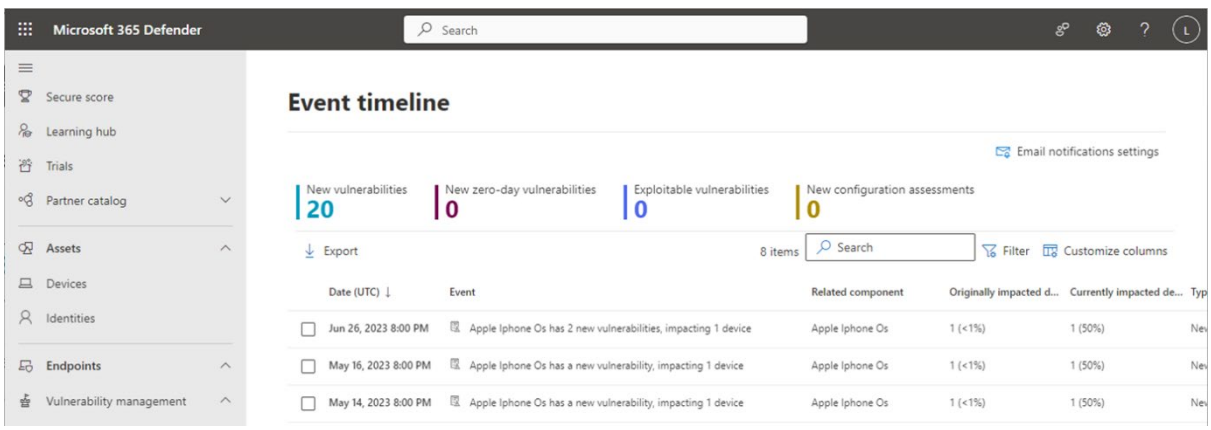

Figure 9.38 – Event timeline page

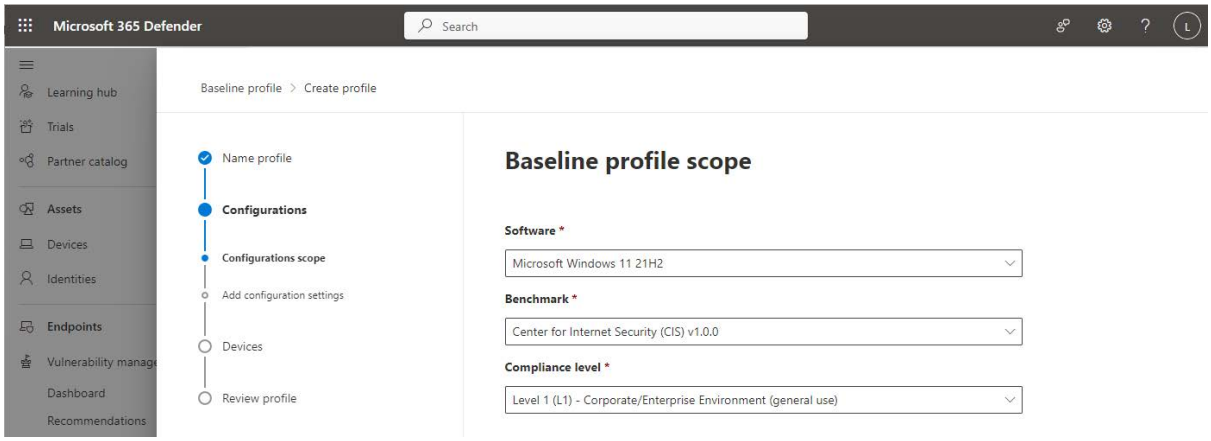

Figure 9.39 – Configuring Baseline profile scope

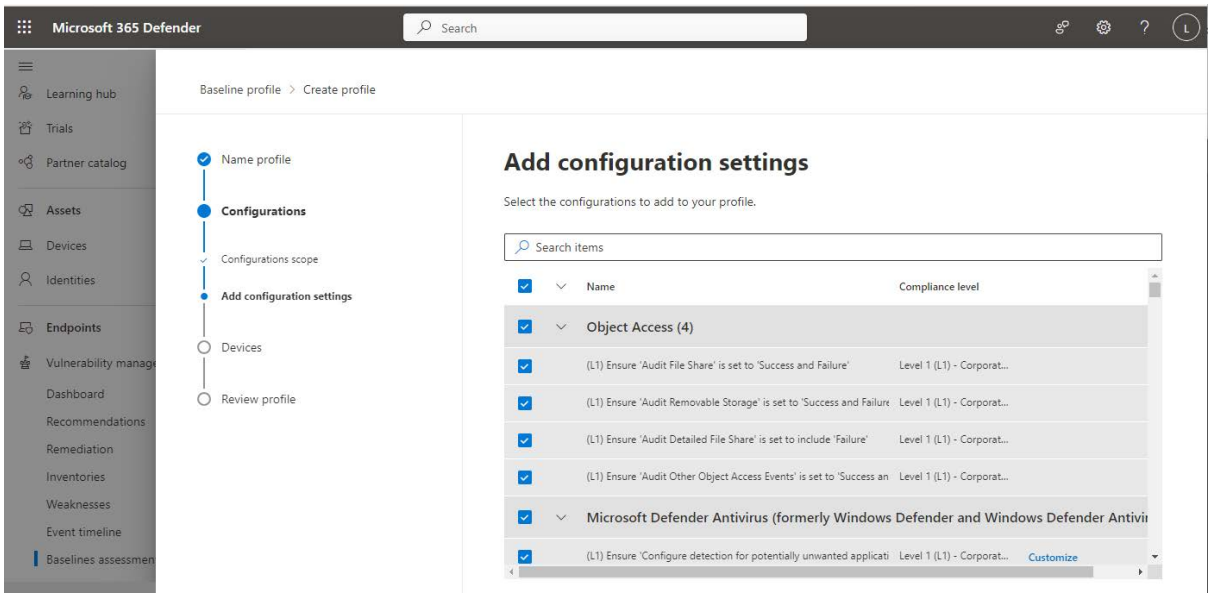

Figure 9.40 – Profile configuration settings

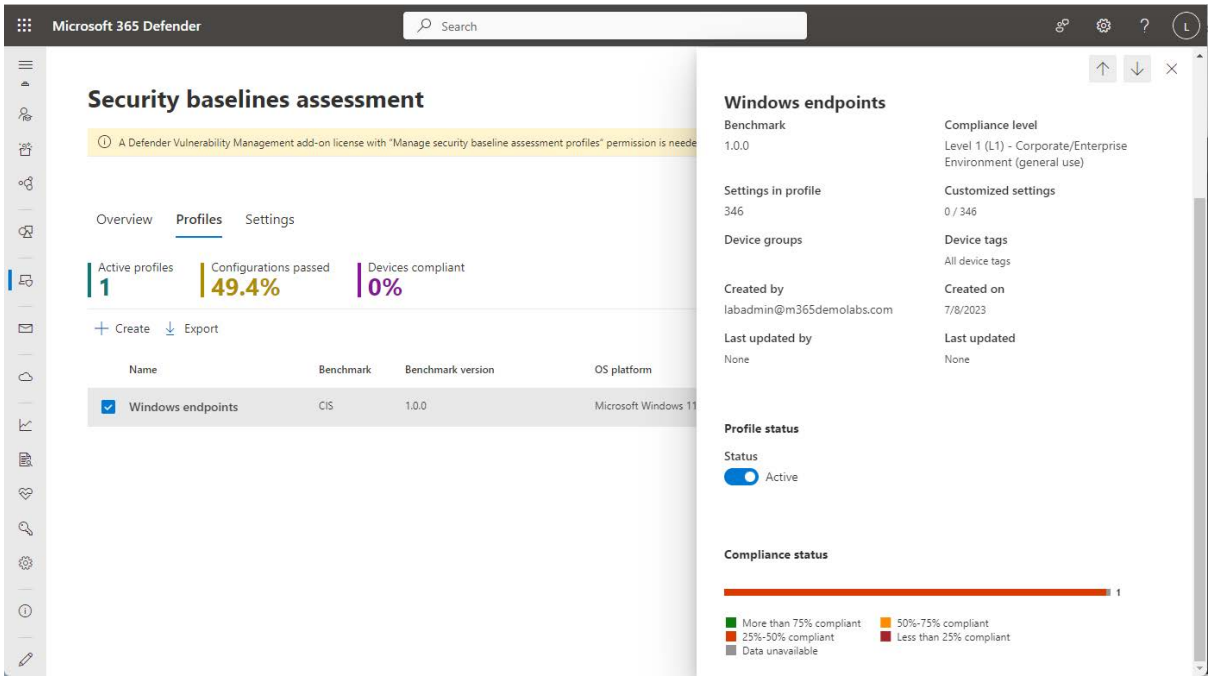

Figure 9.41 – Profile assessment

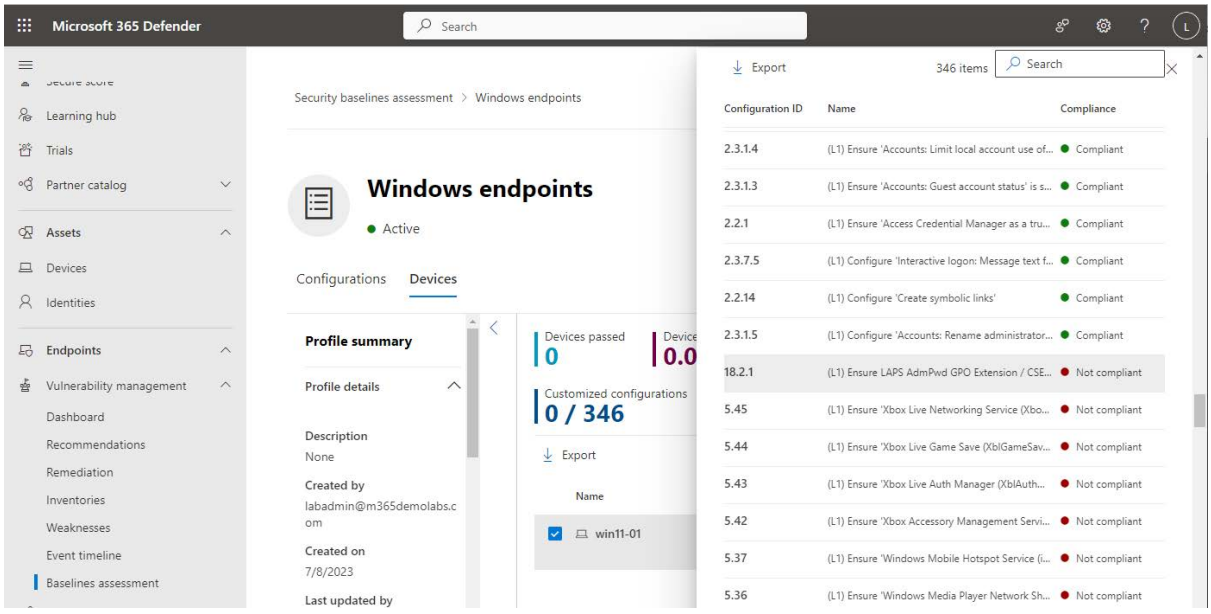

Figure 9.42 – Viewing an individual device's compliance against a baseline profile

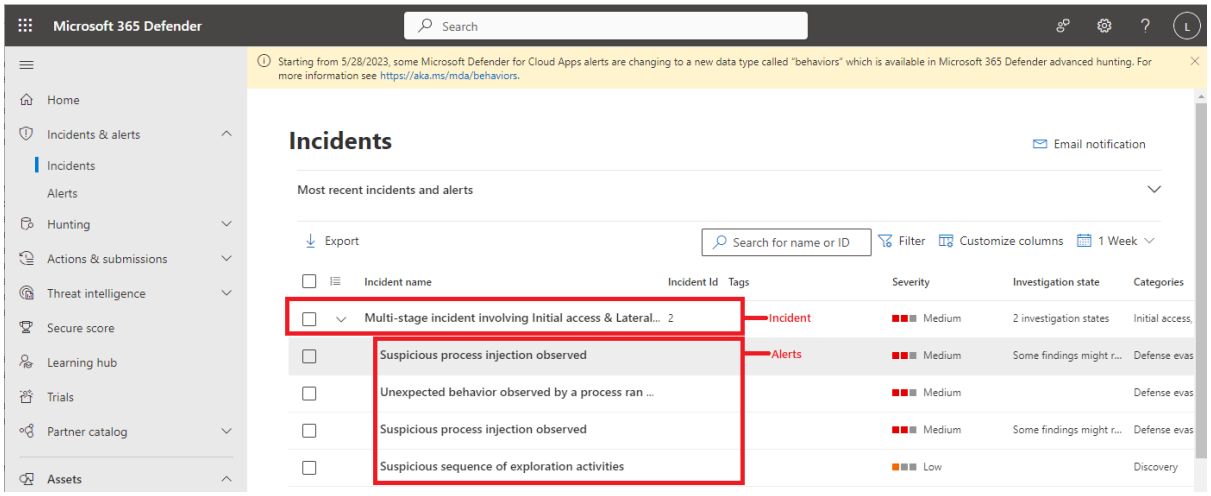

Figure 9.43 – Microsoft 365 Defender incidents and alerts

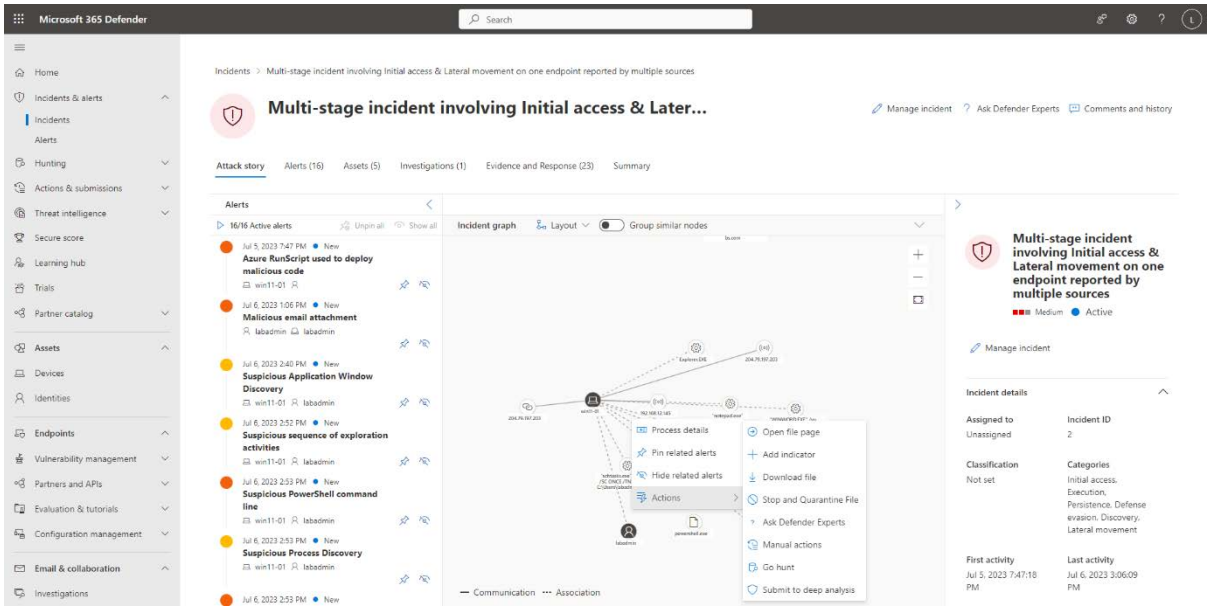

Figure 9.44 – Attack story

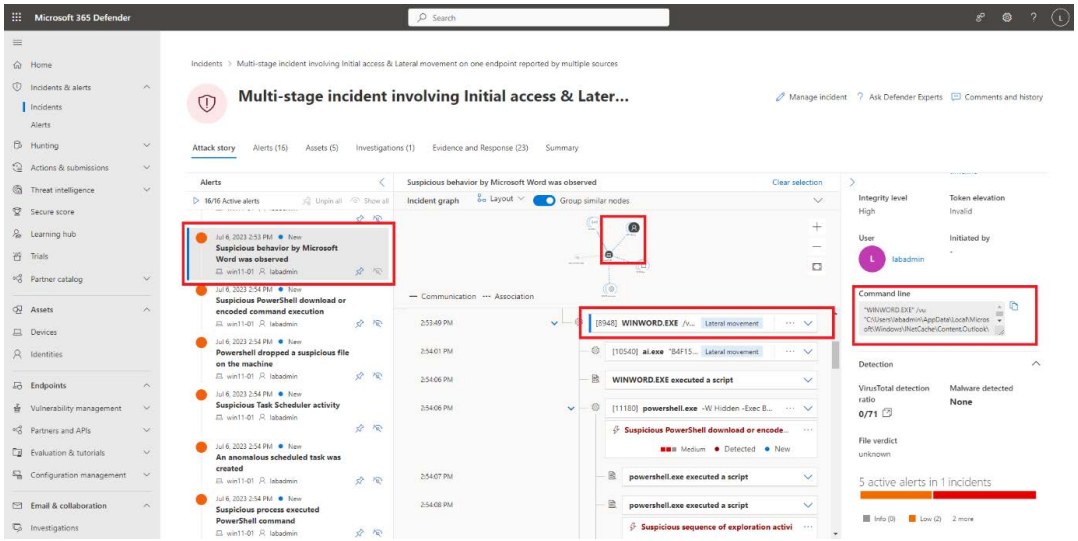

Figure 9.45 – Viewing an alert's details

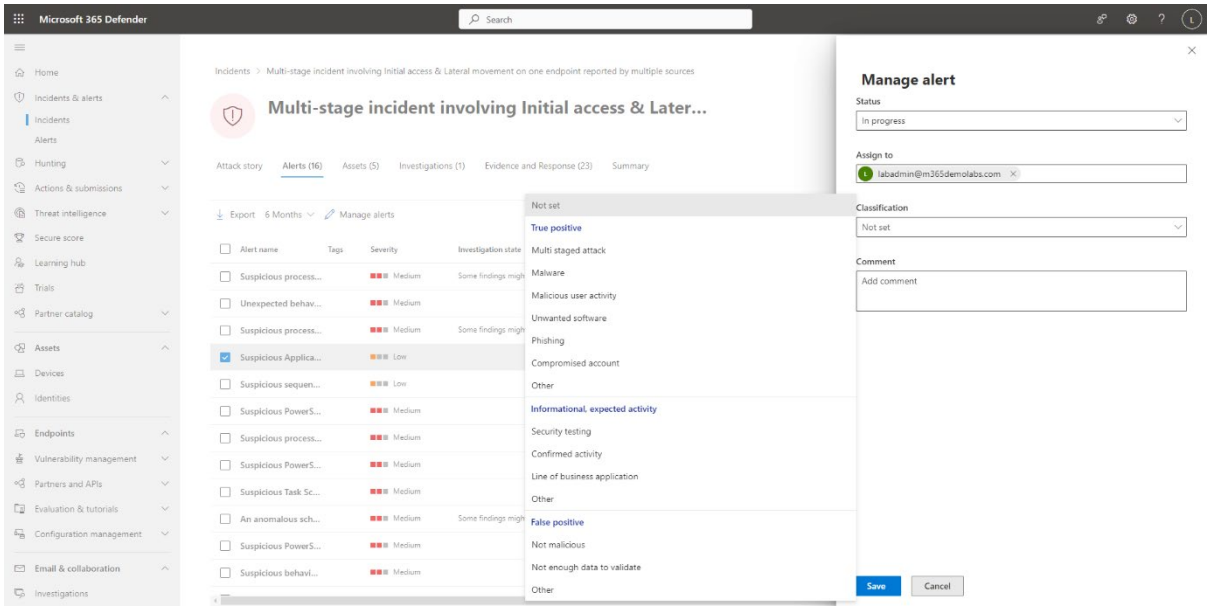

Figure 9.46 – Manage alert details

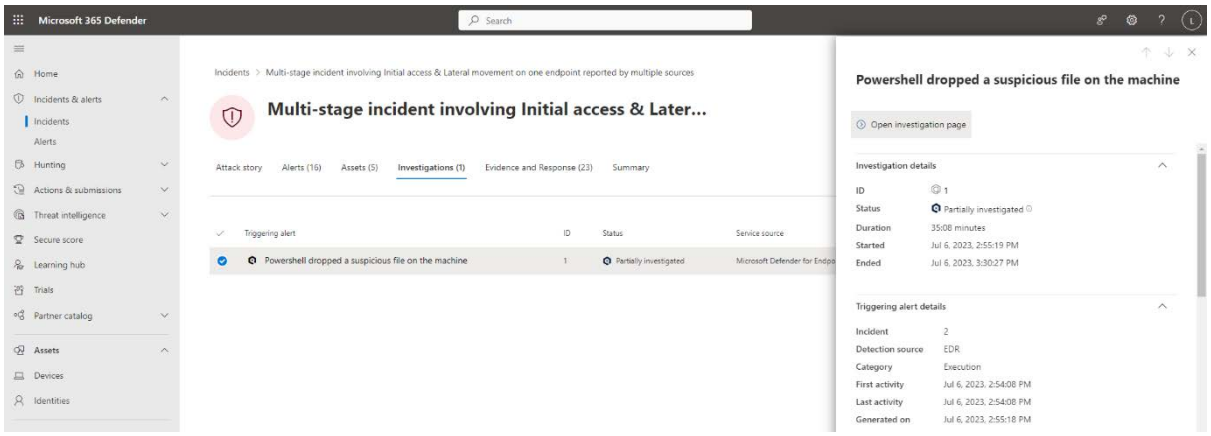

Figure 9.47 – Triggering alert investigation

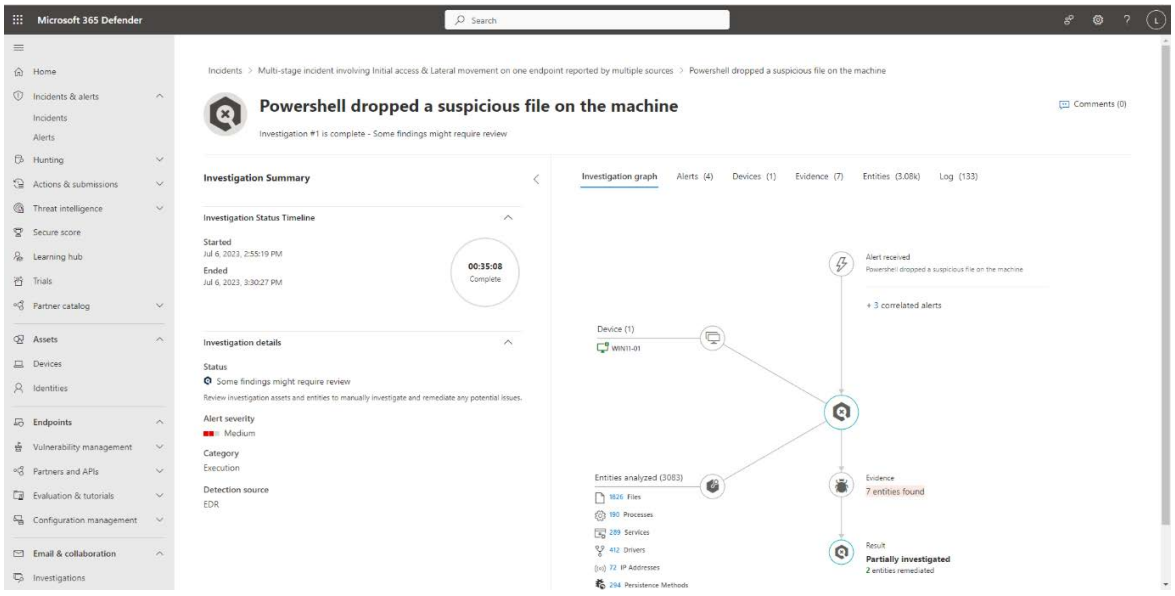

Figure 9.48 – Investigations page

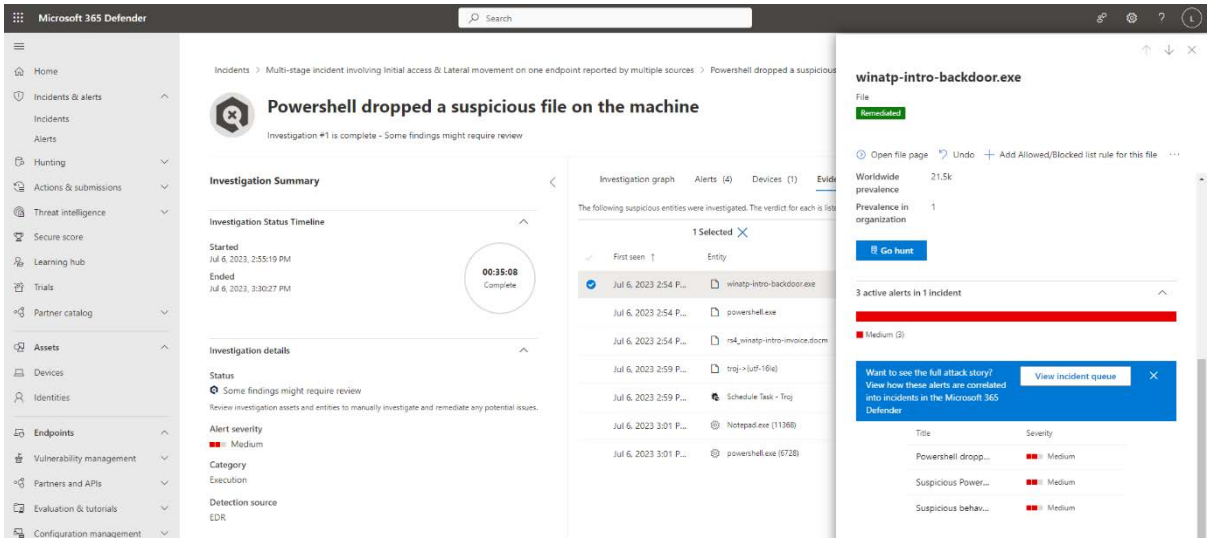

Figure 9.49 – Evidence details

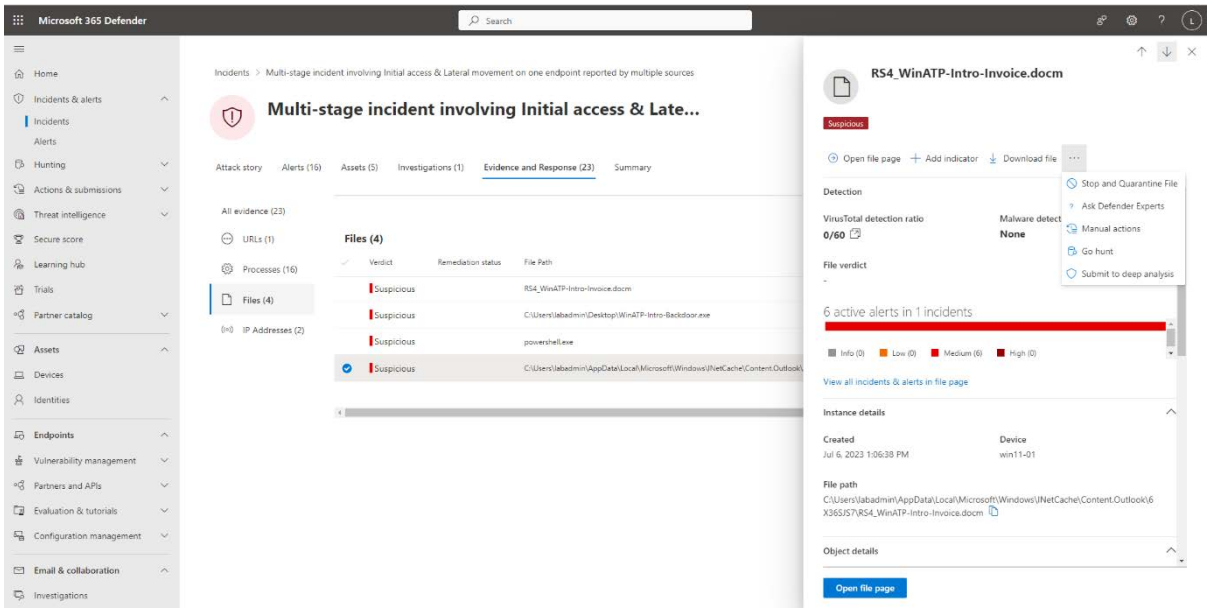

Figure 9.50 – Incident evidence

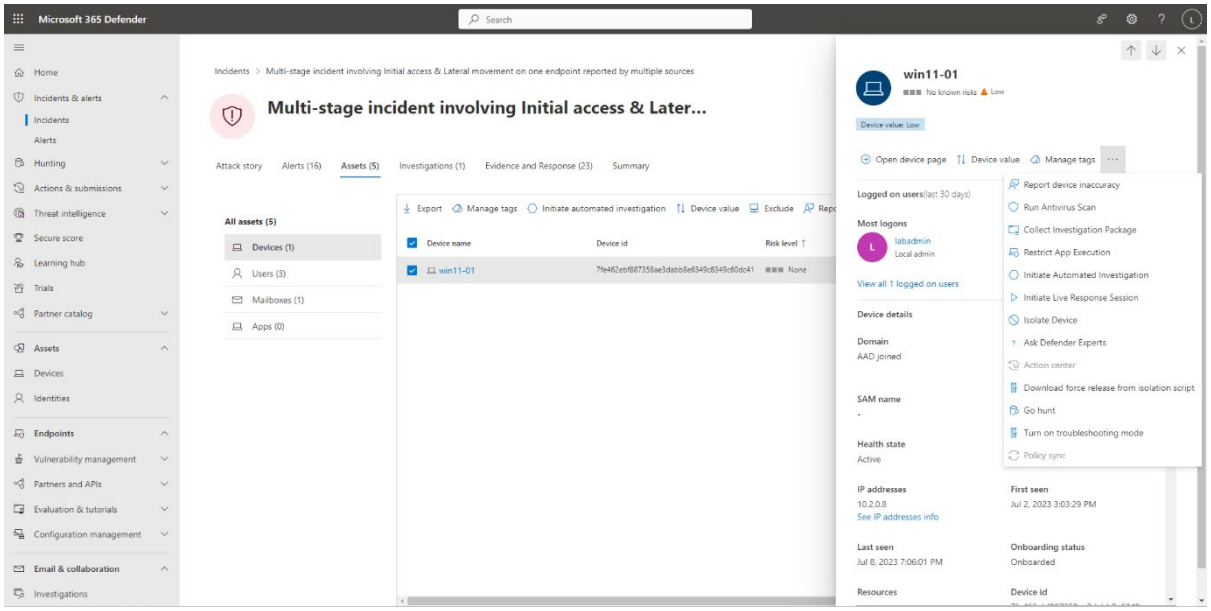

Figure 9.51 – Device remediation actions

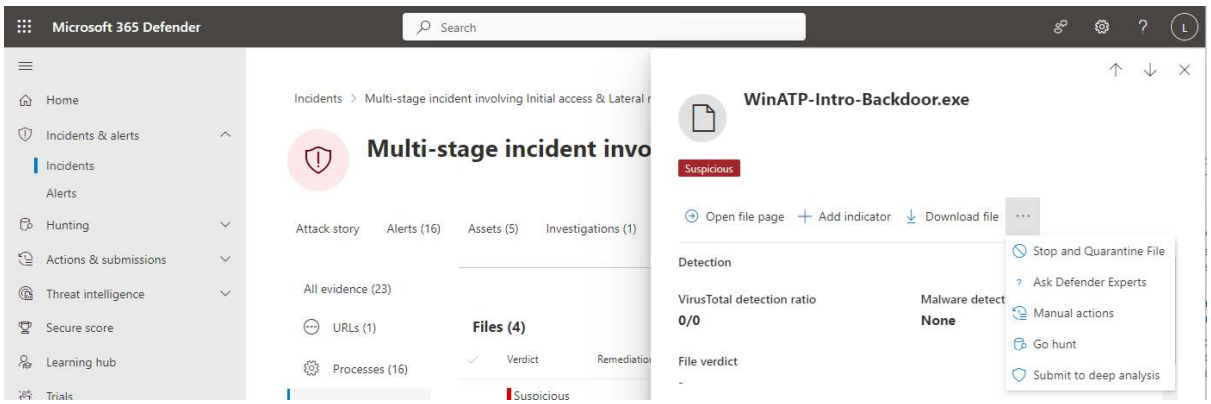

Figure 9.52 – File actions

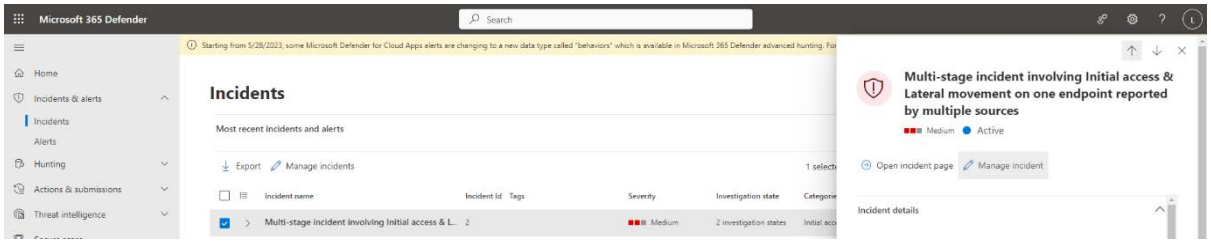

Figure 9.53 – Incident flyout

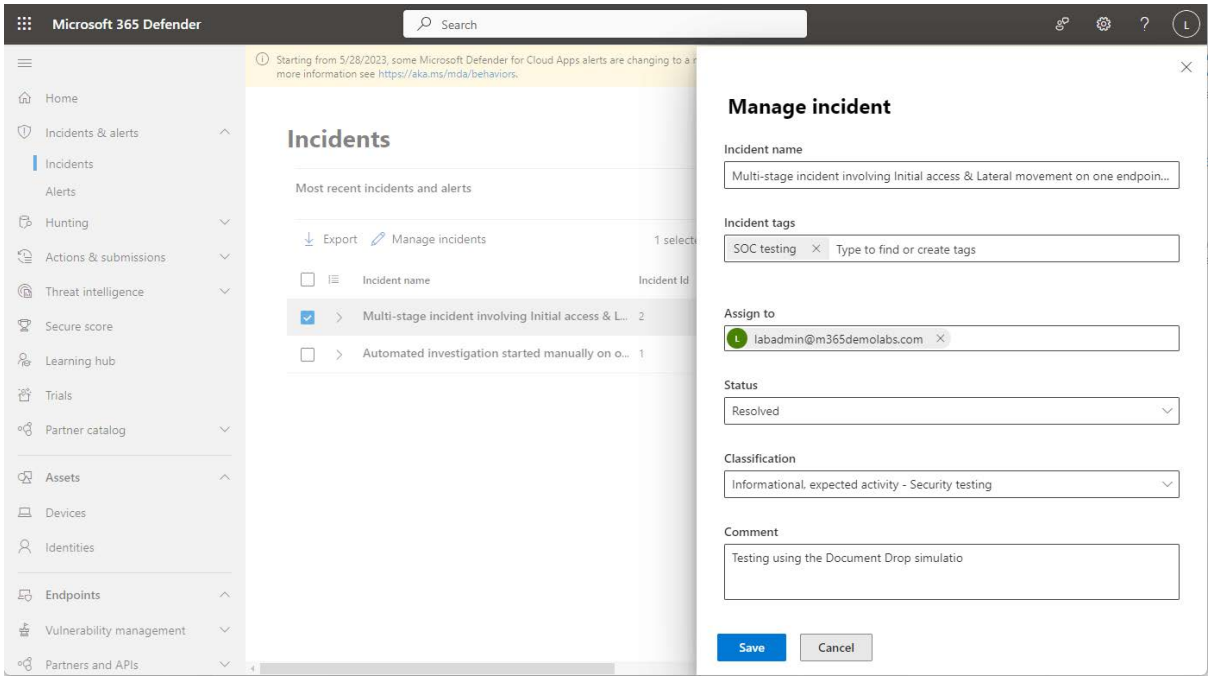

Figure 9.54 – Manage incident flyout

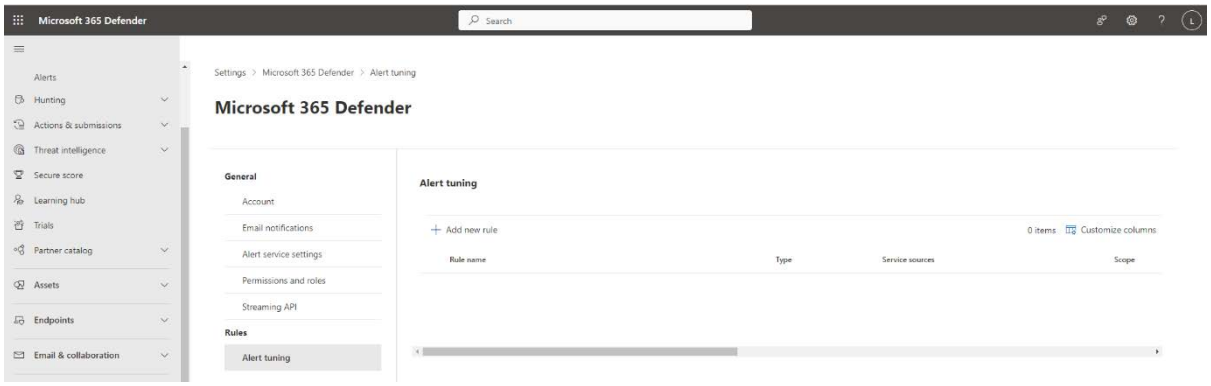

Figure 9.55 – Microsoft 365 Defender rules

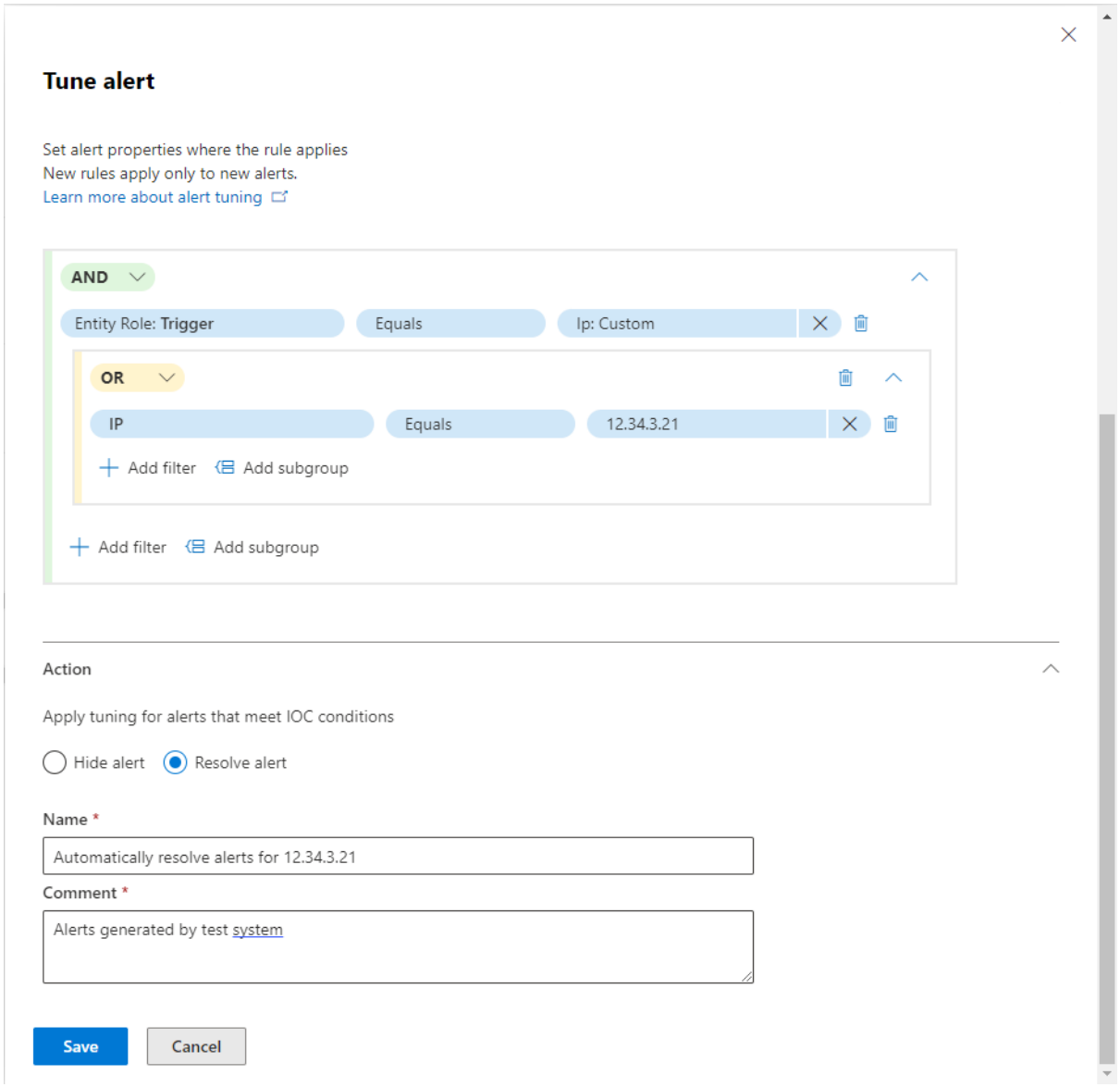

Figure 9.56 – Alert condition parameters

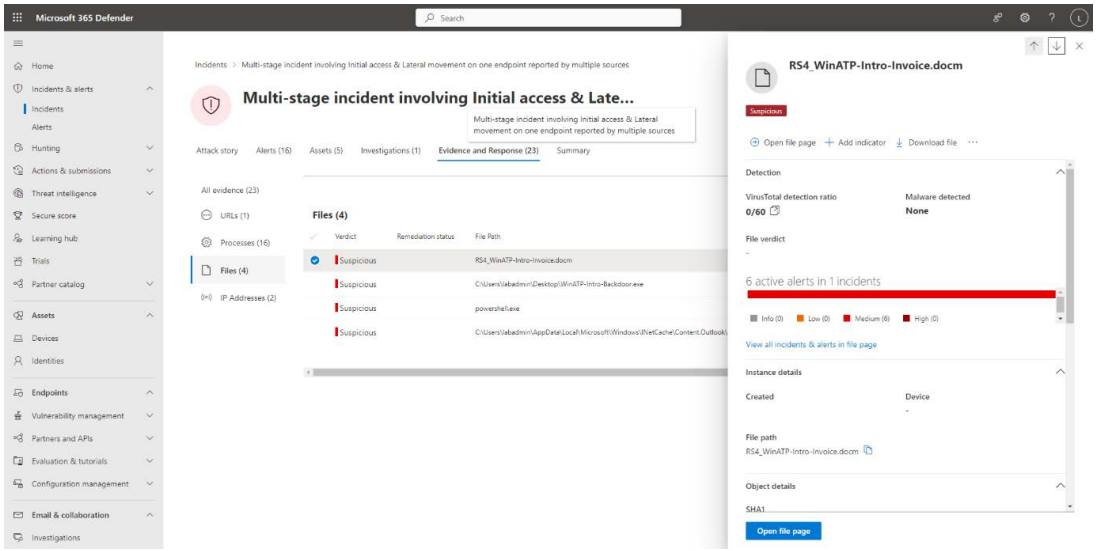

Figure 9.57 – Selecting the evidence to be used as an indicator

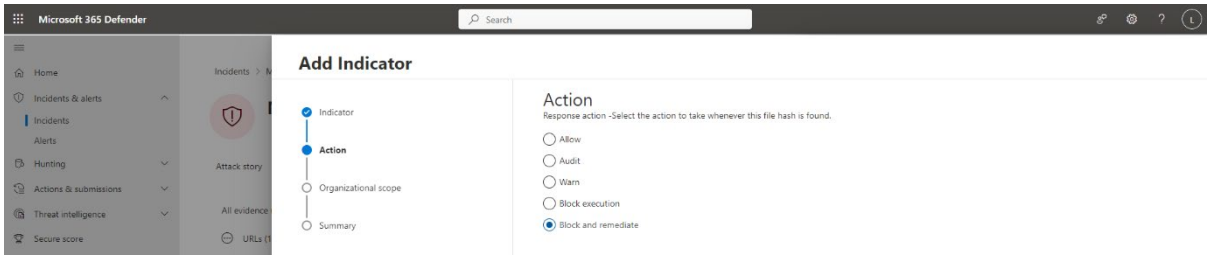

Figure 9.58 – Selecting the Block and remediate action

Figure 9.59 – Indicator rule has been created

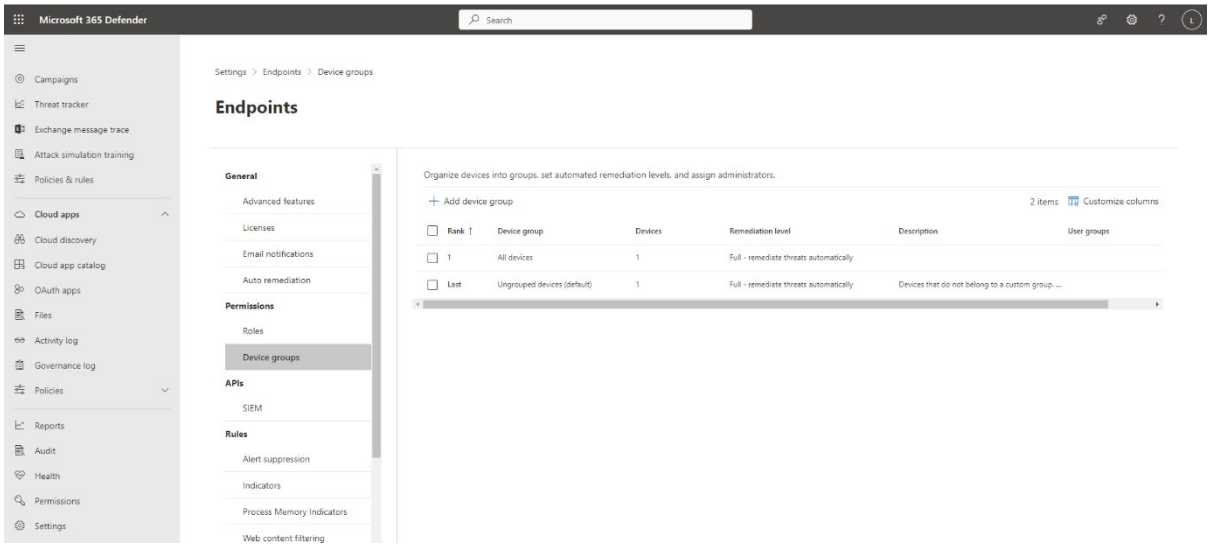

Figure 9.60 – Device groups

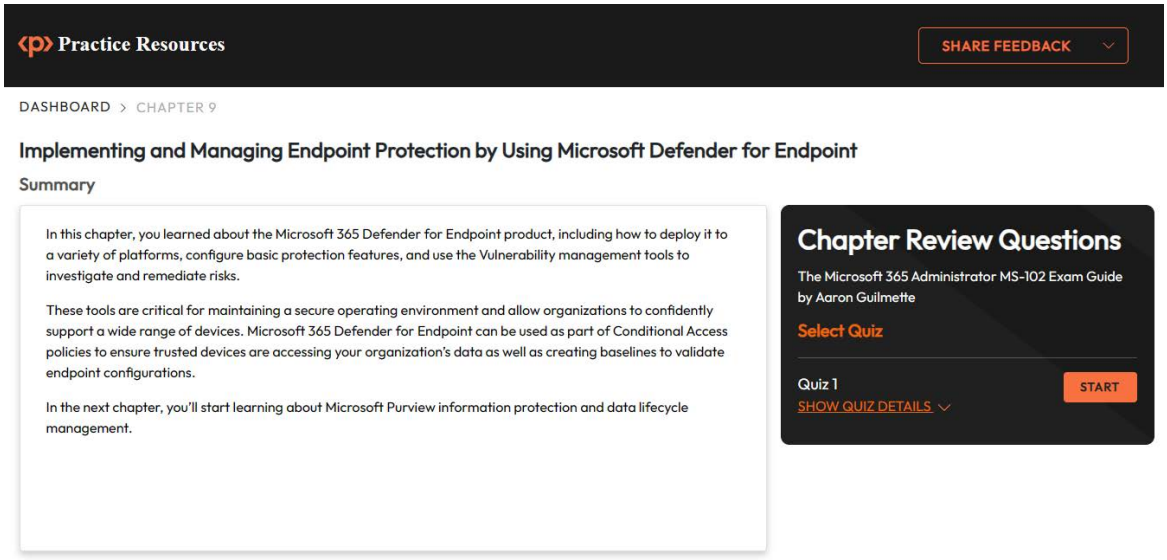

Figure 9.61 – Chapter Review Questions for Chapter 9

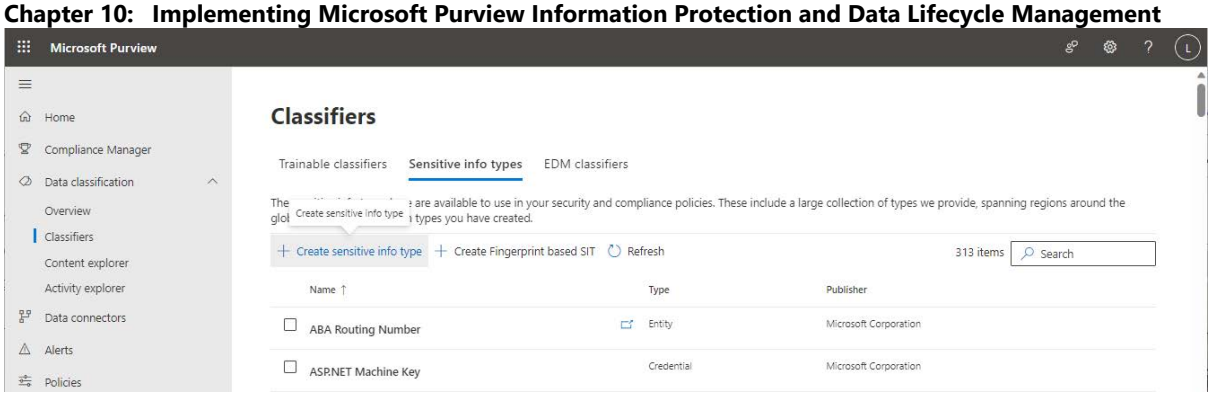

Figure 10.1 – Classifiers page with Sensitive info types tab selected

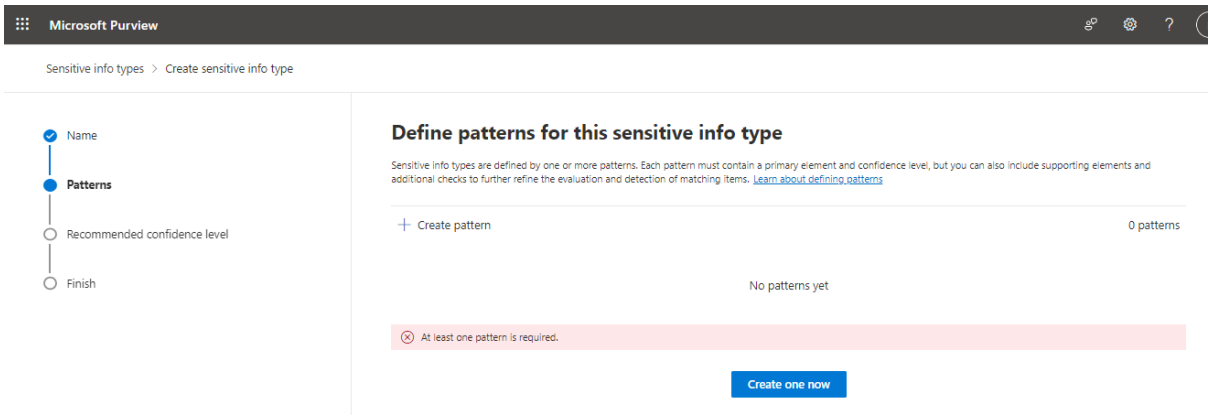

Figure 10.2 – Define a pattern

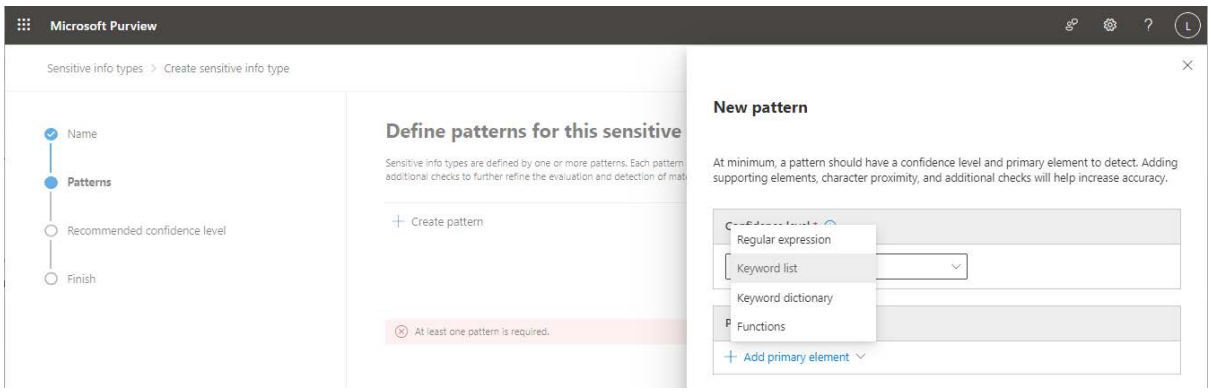

Figure 10.3 – Primary element selection

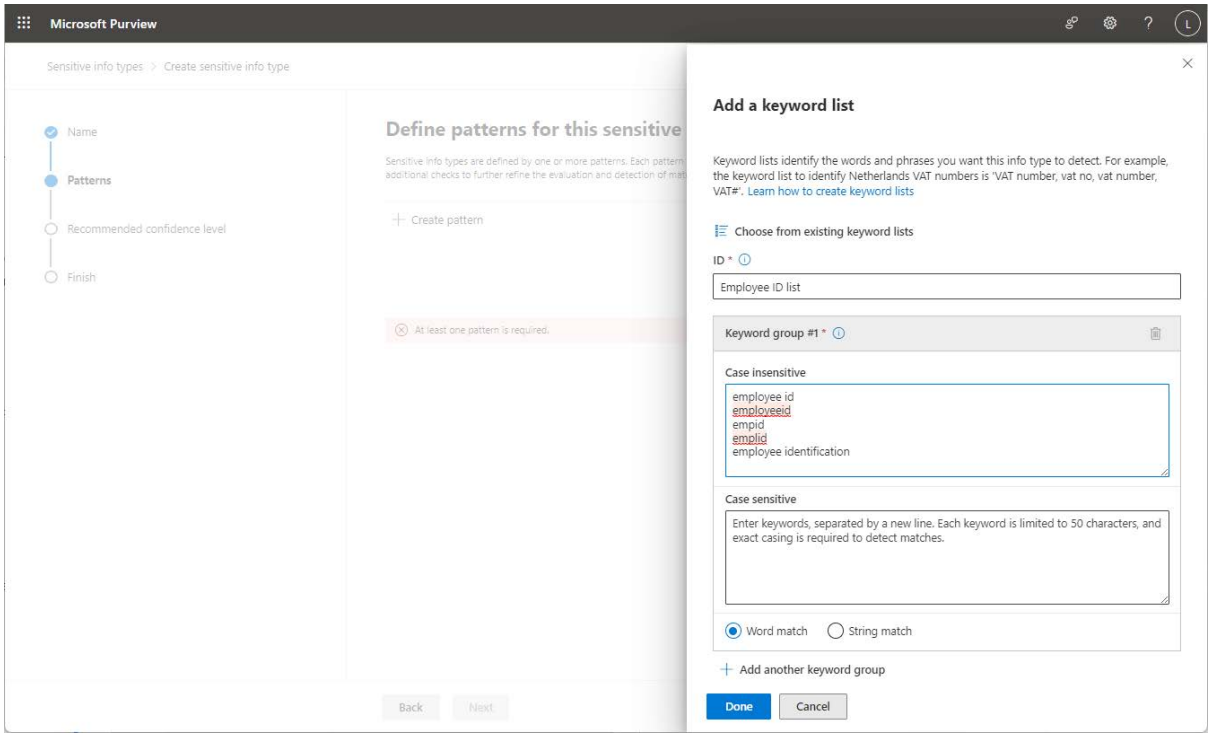

Figure 10.4 – Creating a keyword list

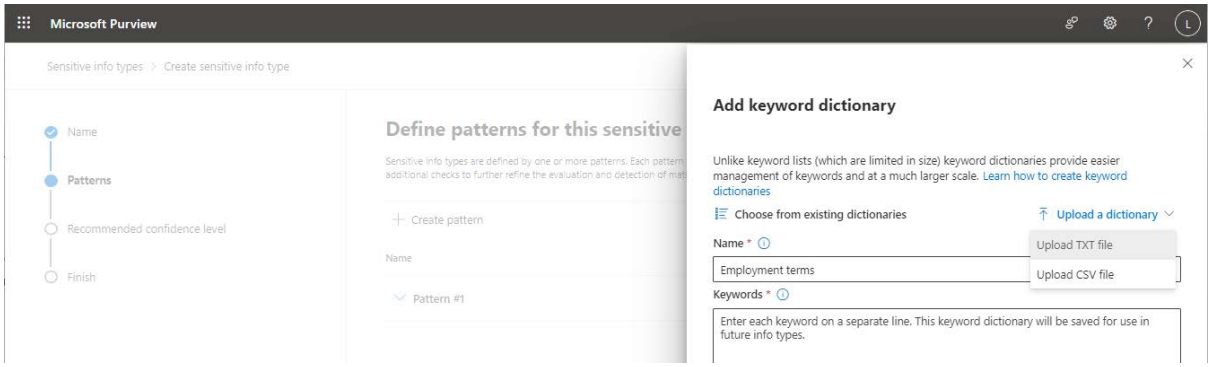

Figure 10.5 – Creating a keyword dictionary

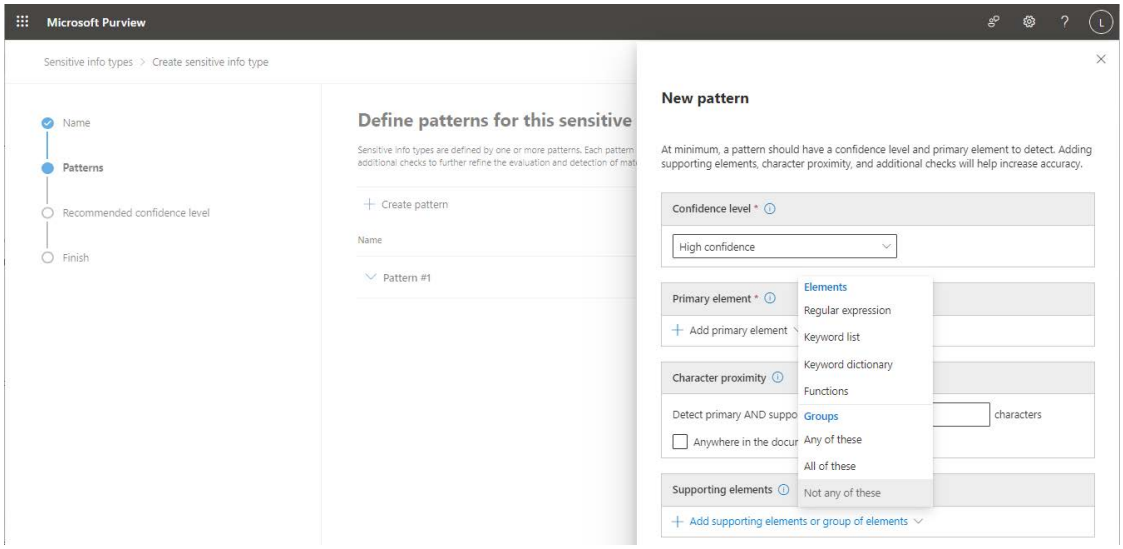

Figure 10.6 – Adding supporting elements

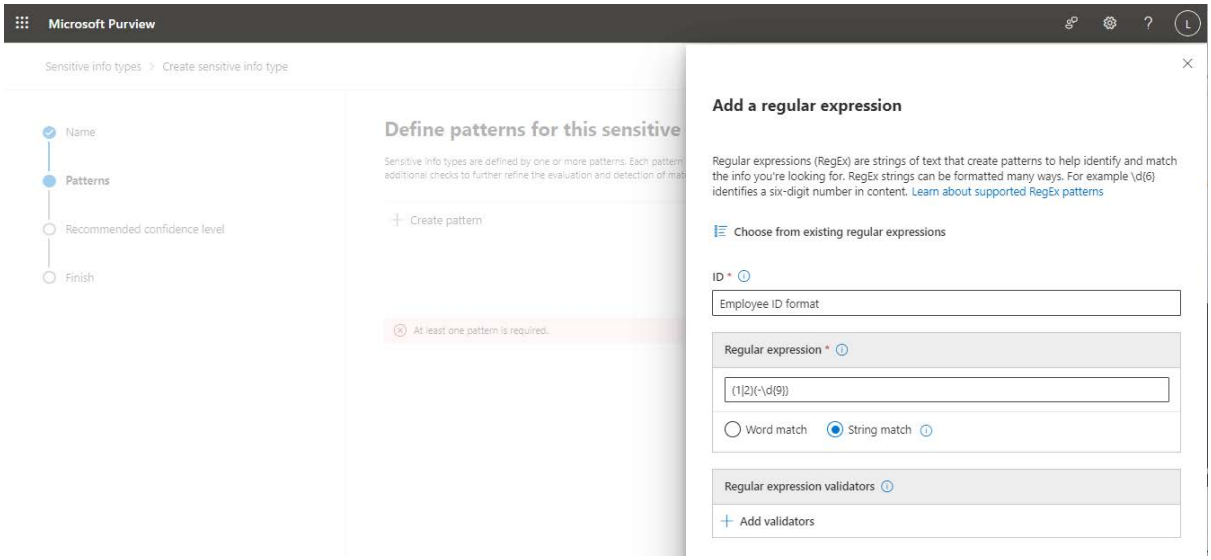

Figure 10.7 – Configuring a regular expression

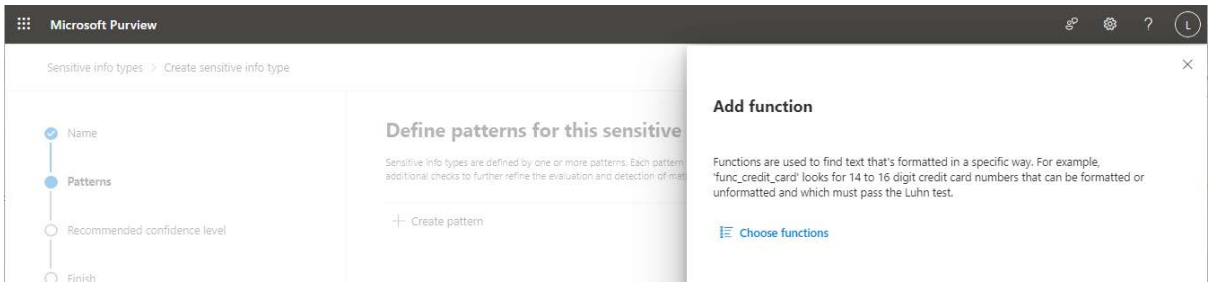

Figure 10.8 – Creating a function-based sensitive information type

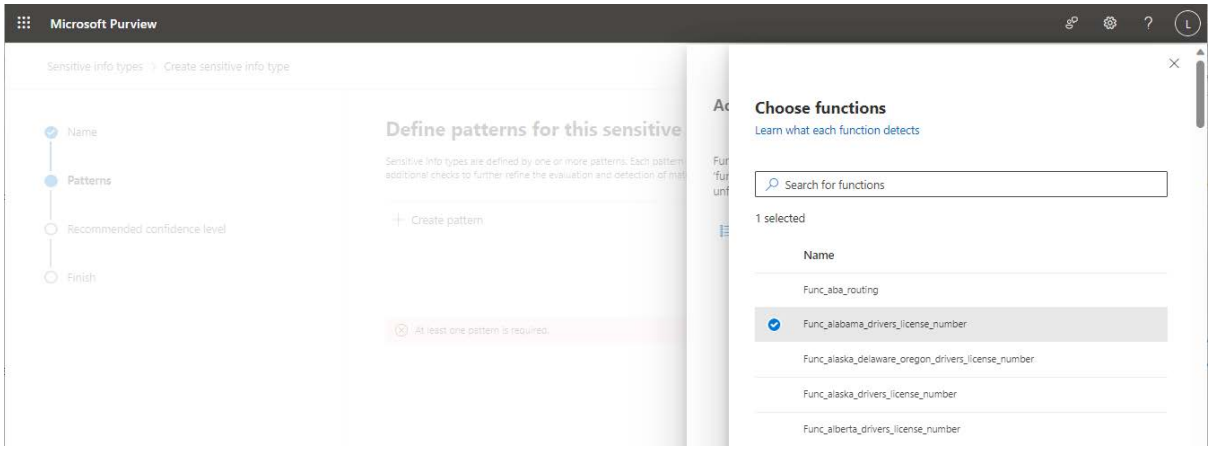

Figure 10.9 – Adding a function

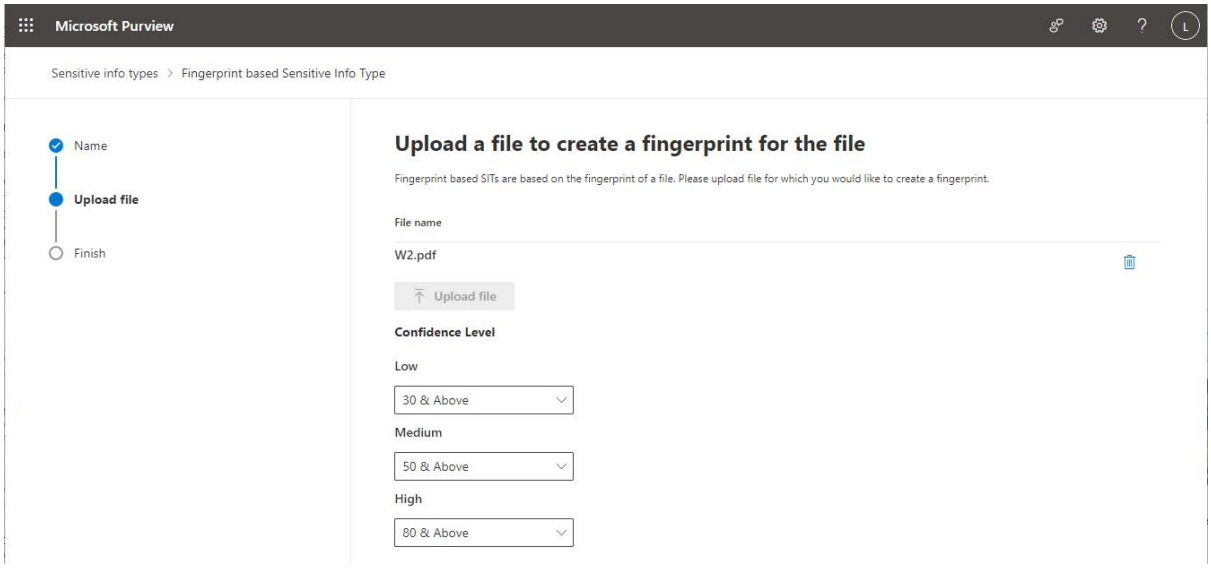

Figure 10.10 – Uploading a form for a document fingerprint

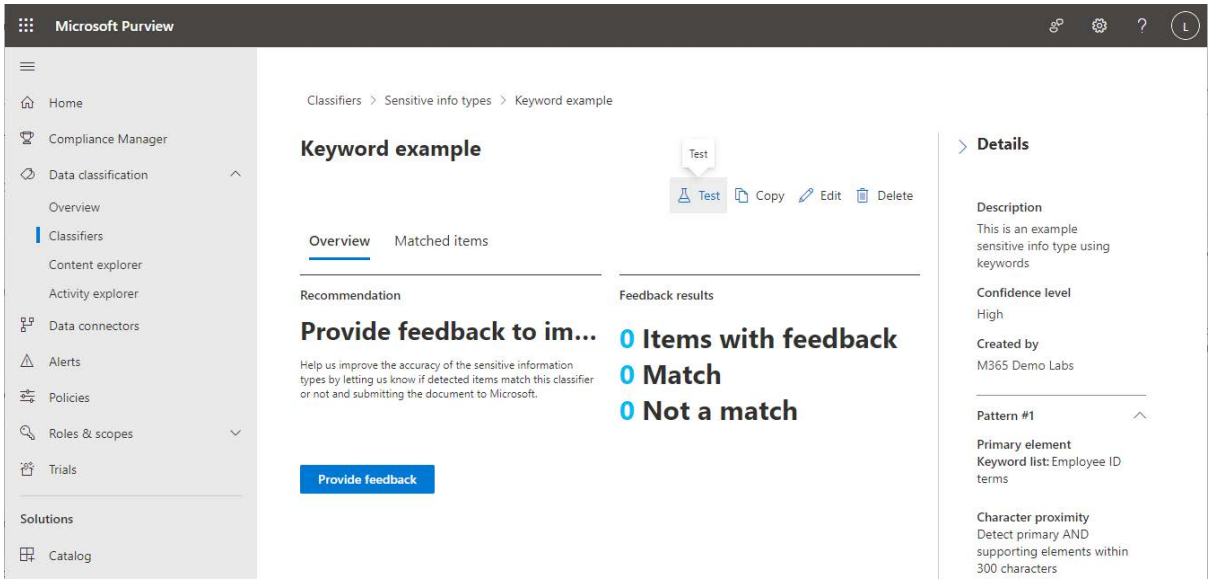

Figure 10.11 – Classifier information page

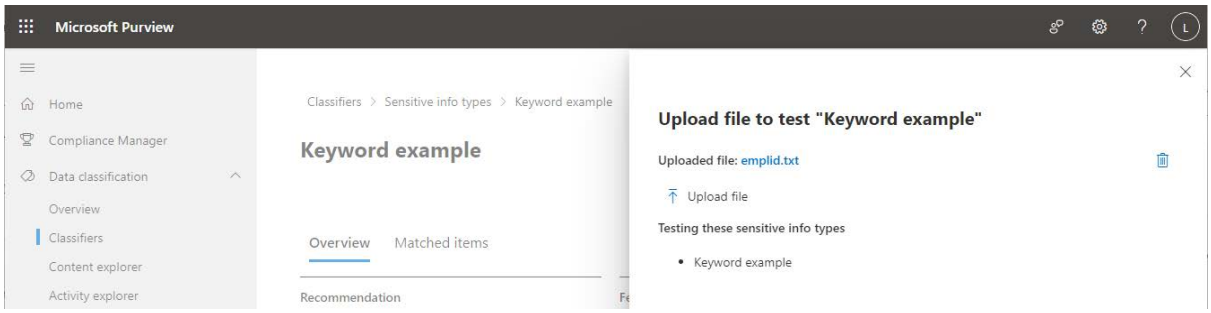

Figure 10.12 – Uploading a sample file

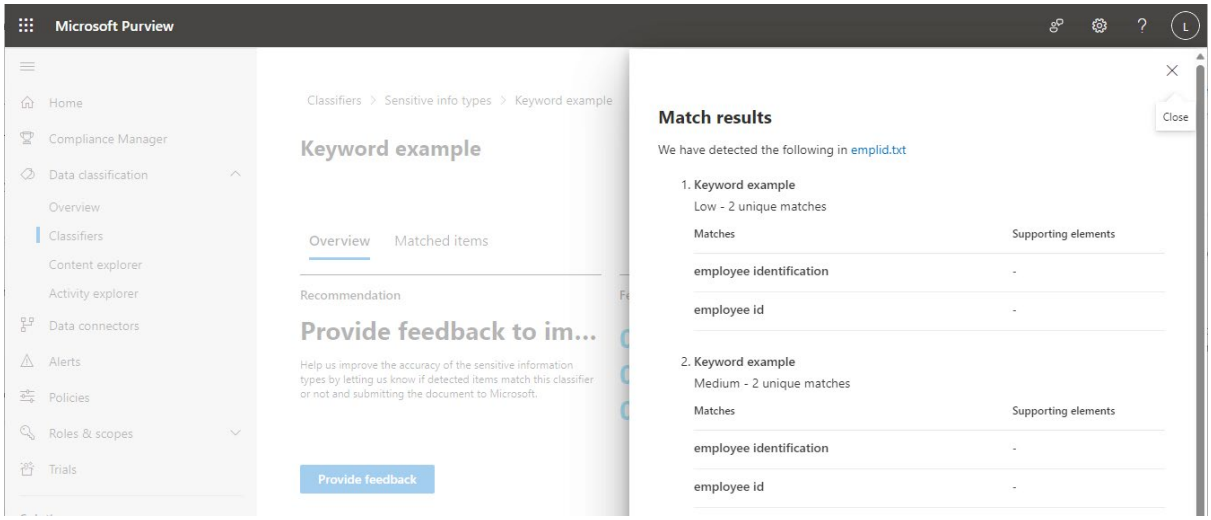

Figure 10.13 – Reviewing the match detections

Figure 10.14 – The principles of retention

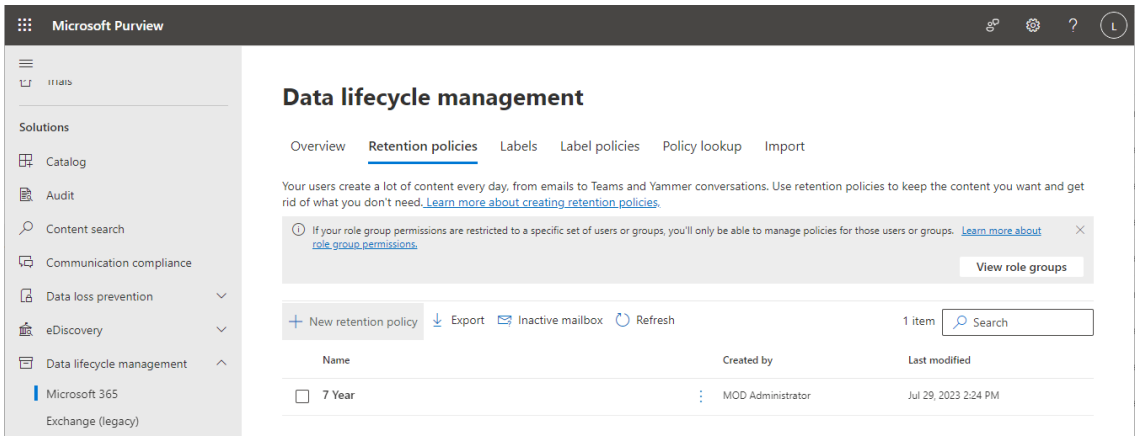

Figure 10.15 – Retention policies tab

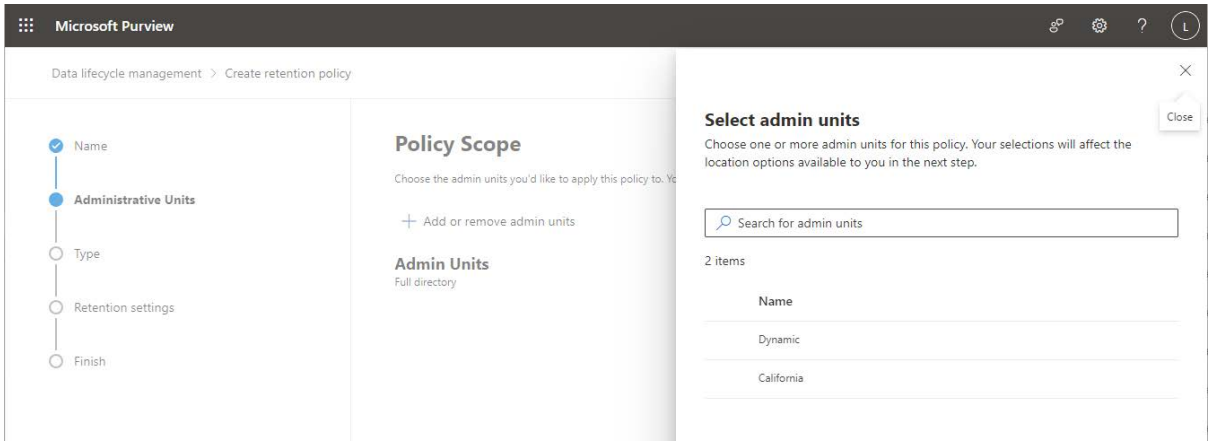

Figure 10.16 – Selecting administrative units

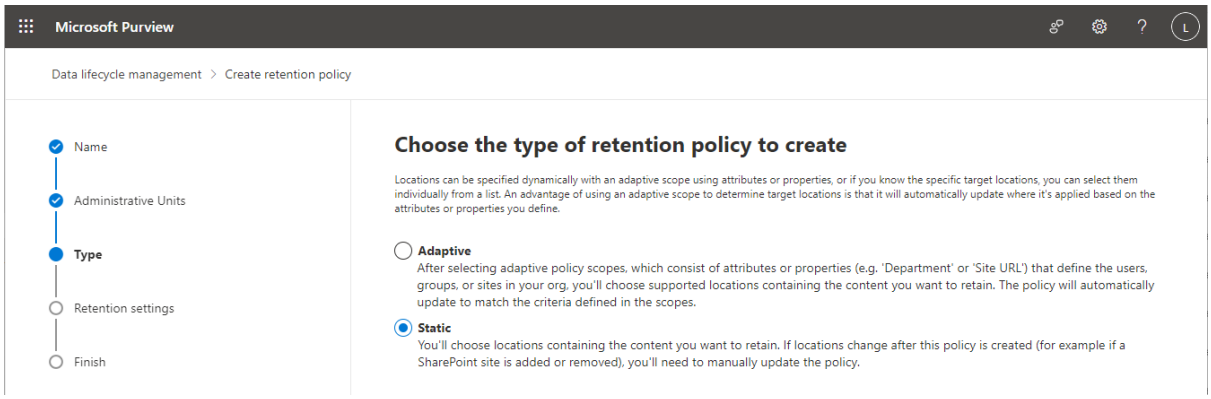

Figure 10.17 – Selecting the policy type

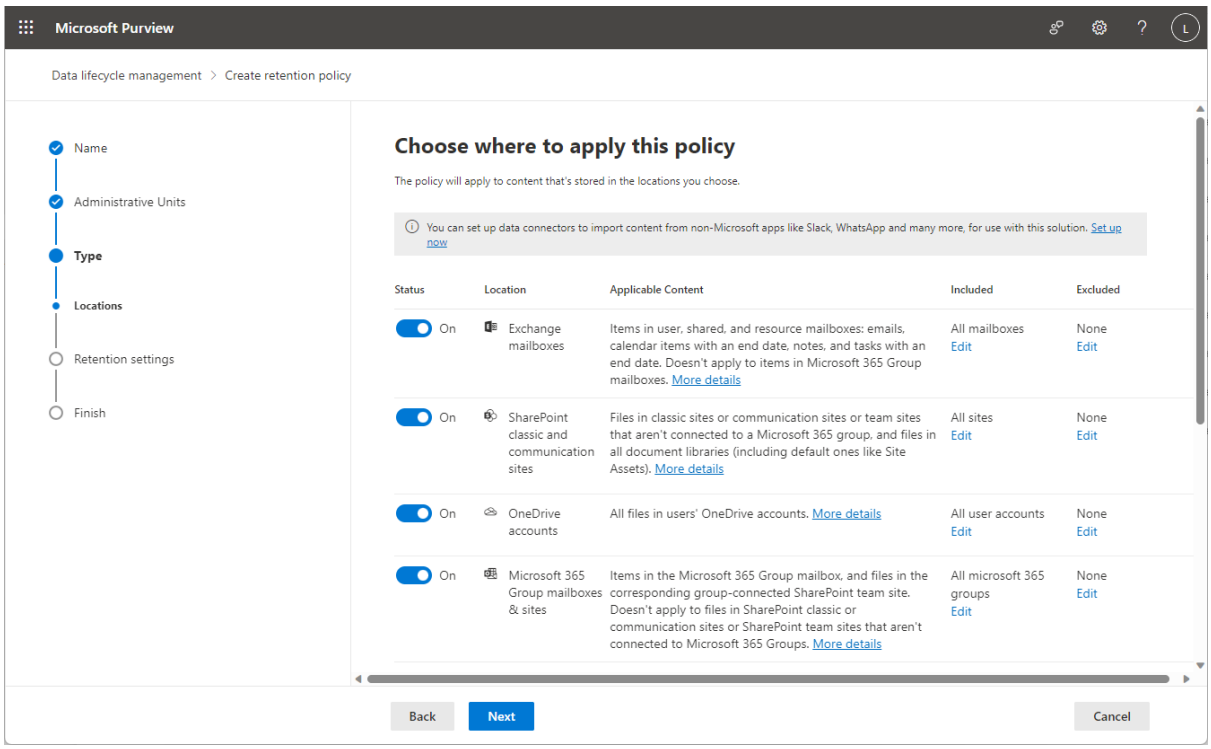

Figure 10.18 – Selecting workloads for policies

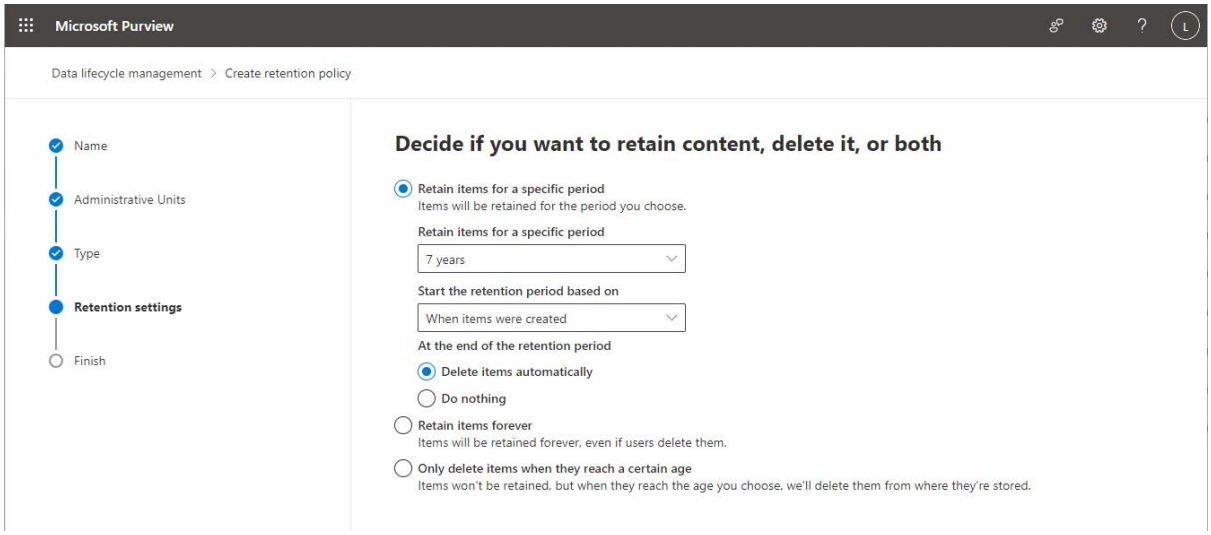

Figure 10.19 – Specifying the retention settings

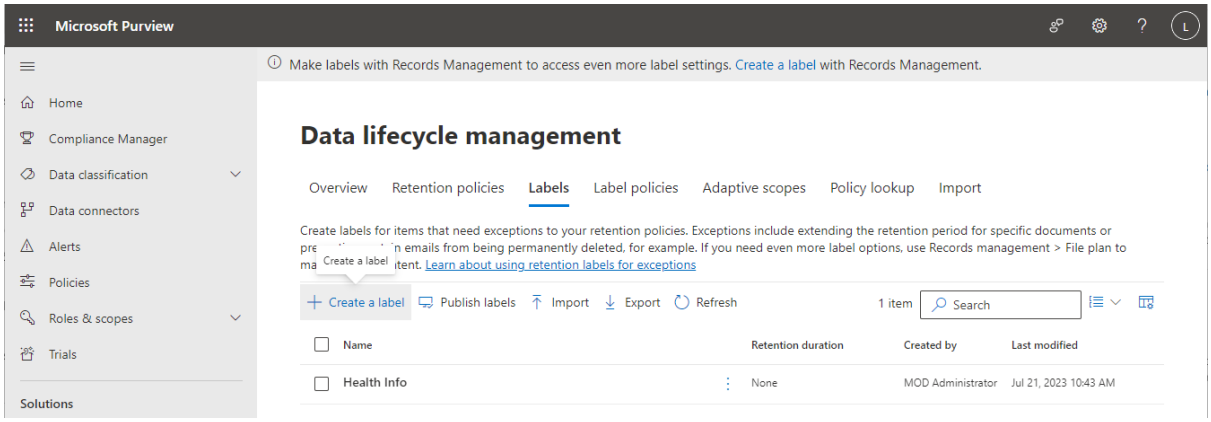

Figure 10.20 – Using the Labels tab

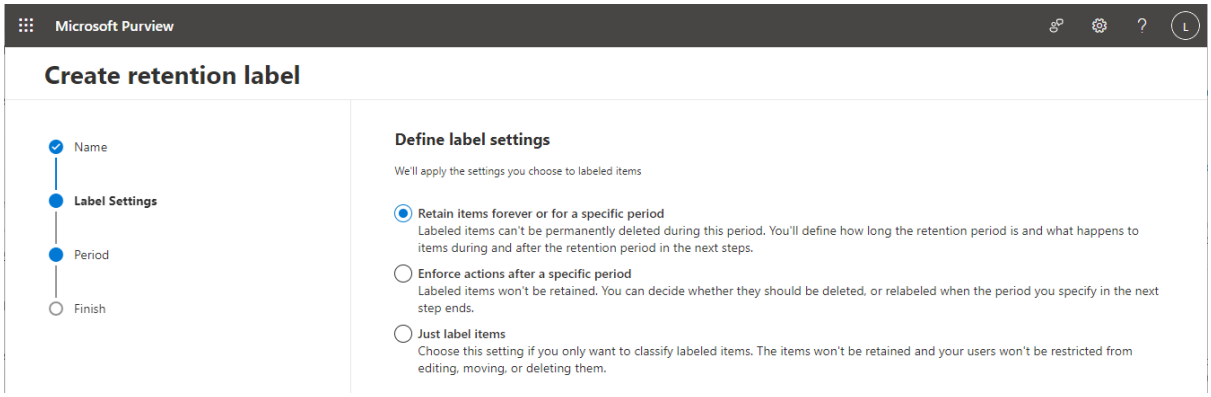

Figure 10.21 – Selecting label settings

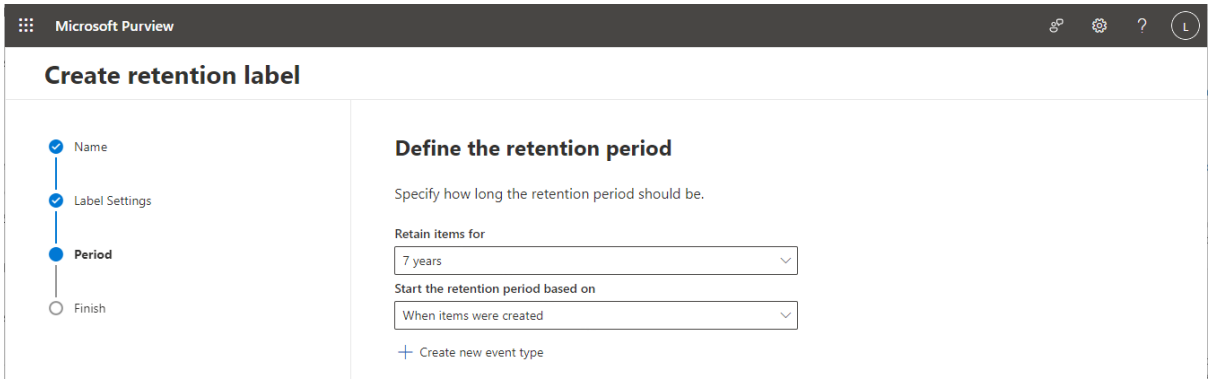

Figure 10.22 – Defining a retention period

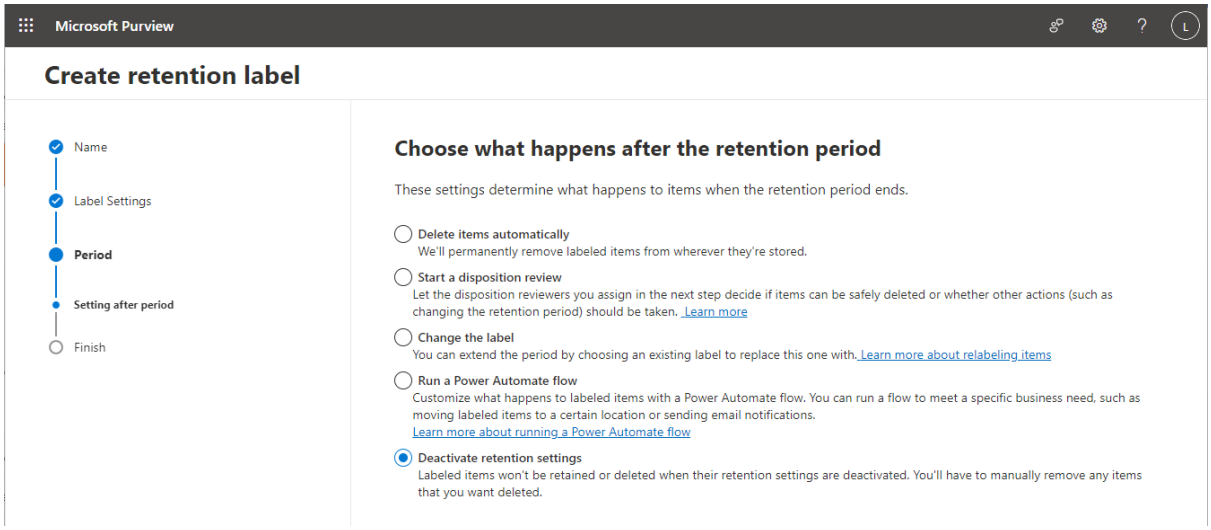

Figure 10.23 – Choosing what happens when the retention period expires

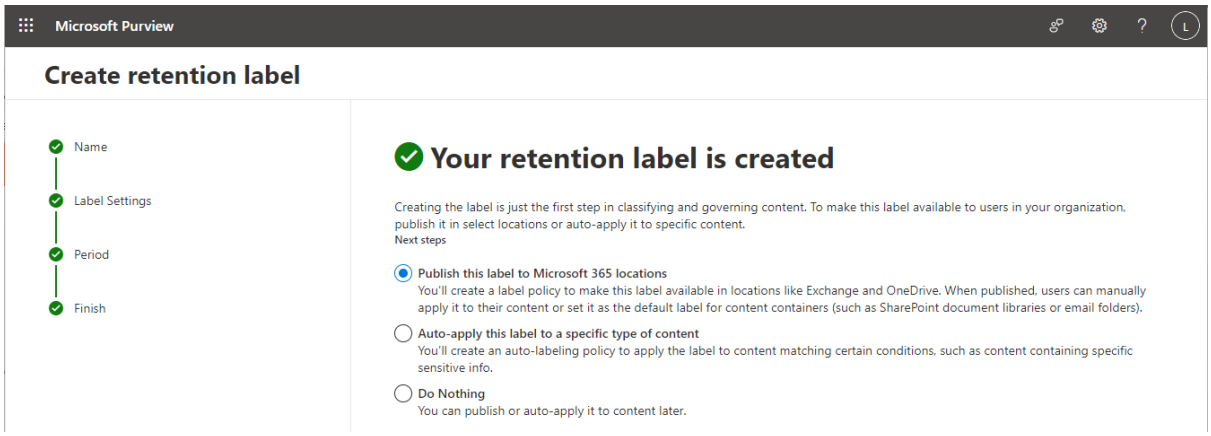

Figure 10.24 – Publishing options

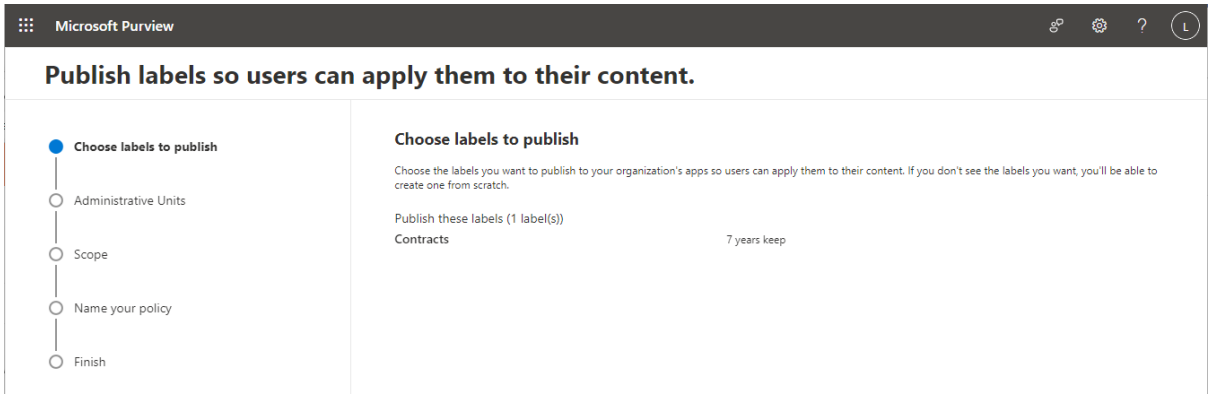

Figure 10.25 – Choosing a label to publish

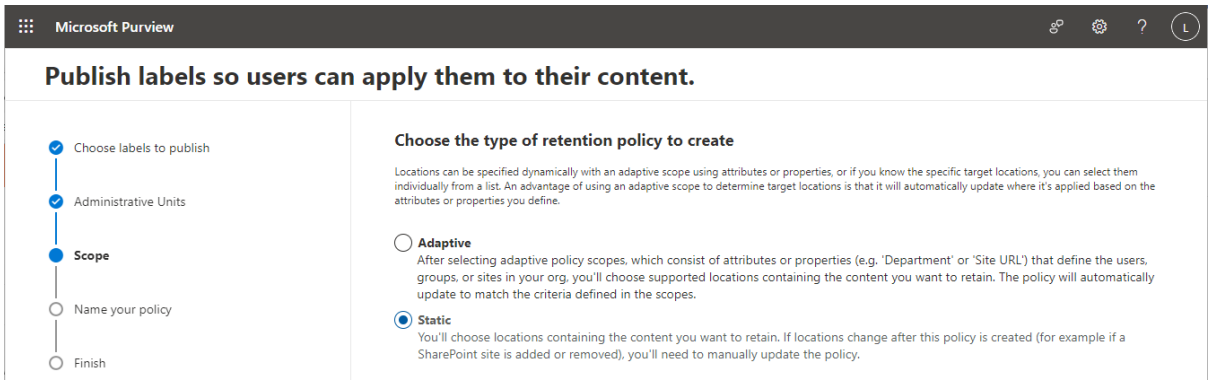

Figure 10.26 – Selecting a scope for the policy

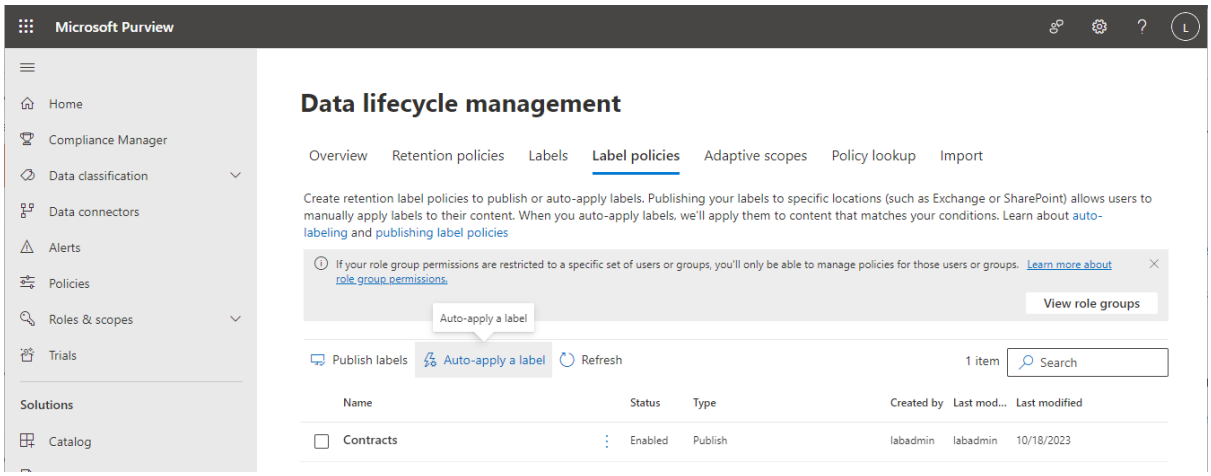

Figure 10.27 – Label policies tab

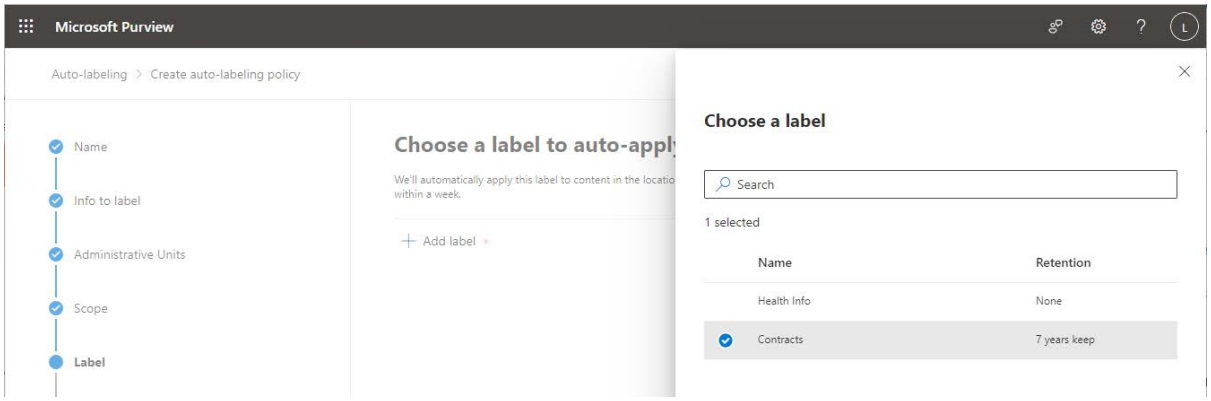

Figure 10.28 – Selecting a label

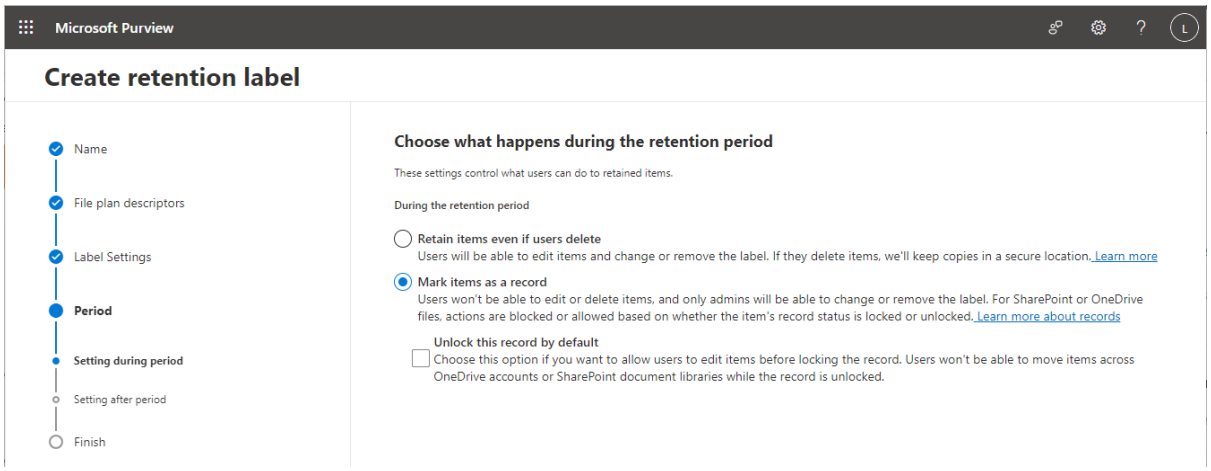

Figure 10.29 – Creating a retention label that marks items as a record

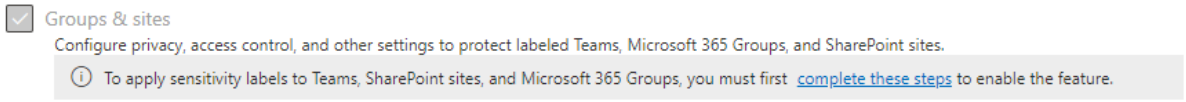

Figure 10.30 – Notice displayed when creating a sensitivity label

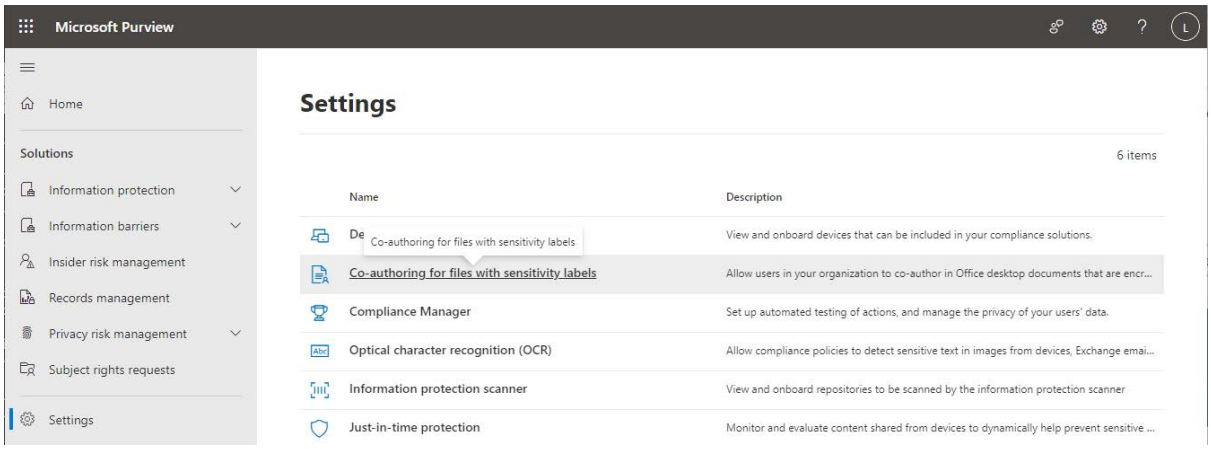

Figure 10.31 – Selecting the Co-authoring for files with sensitivity labels setting

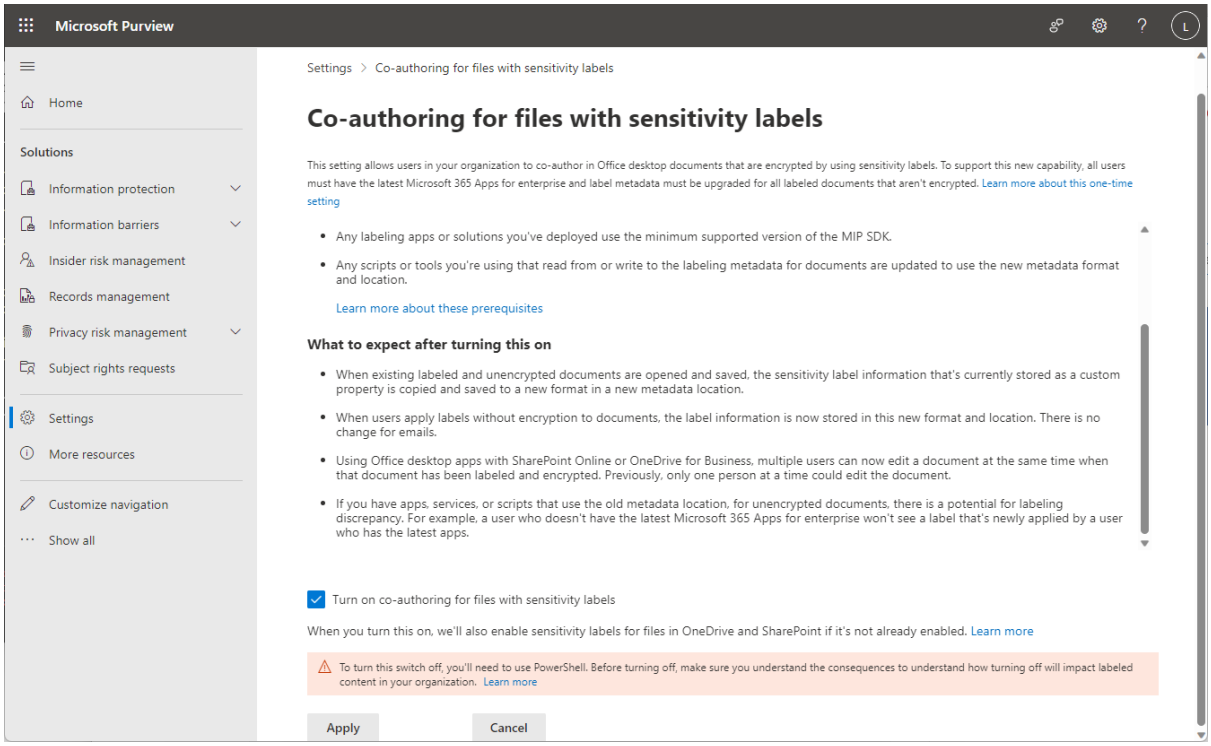

Figure 10.32 – Confirming co-authoring settings

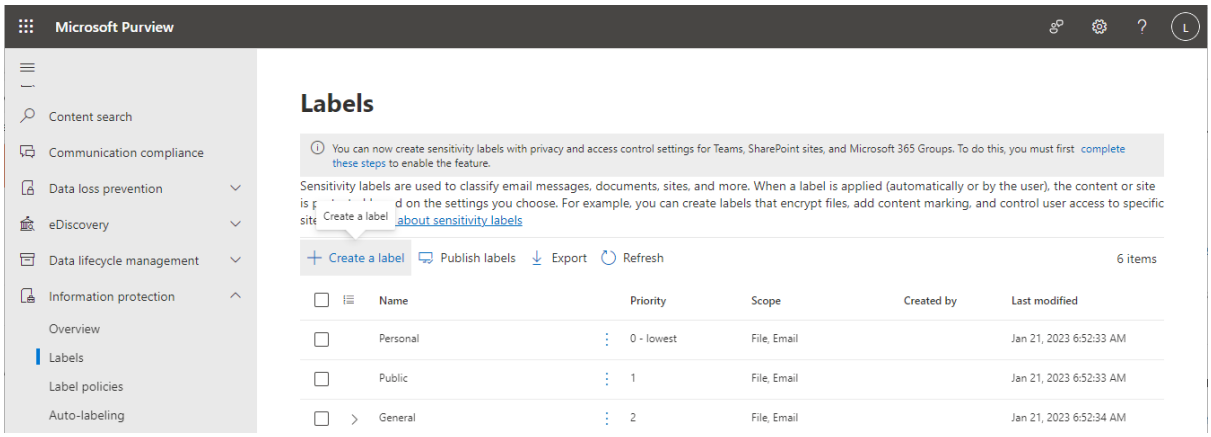

Figure 10.33 – Selecting Create a label from the Labels home page

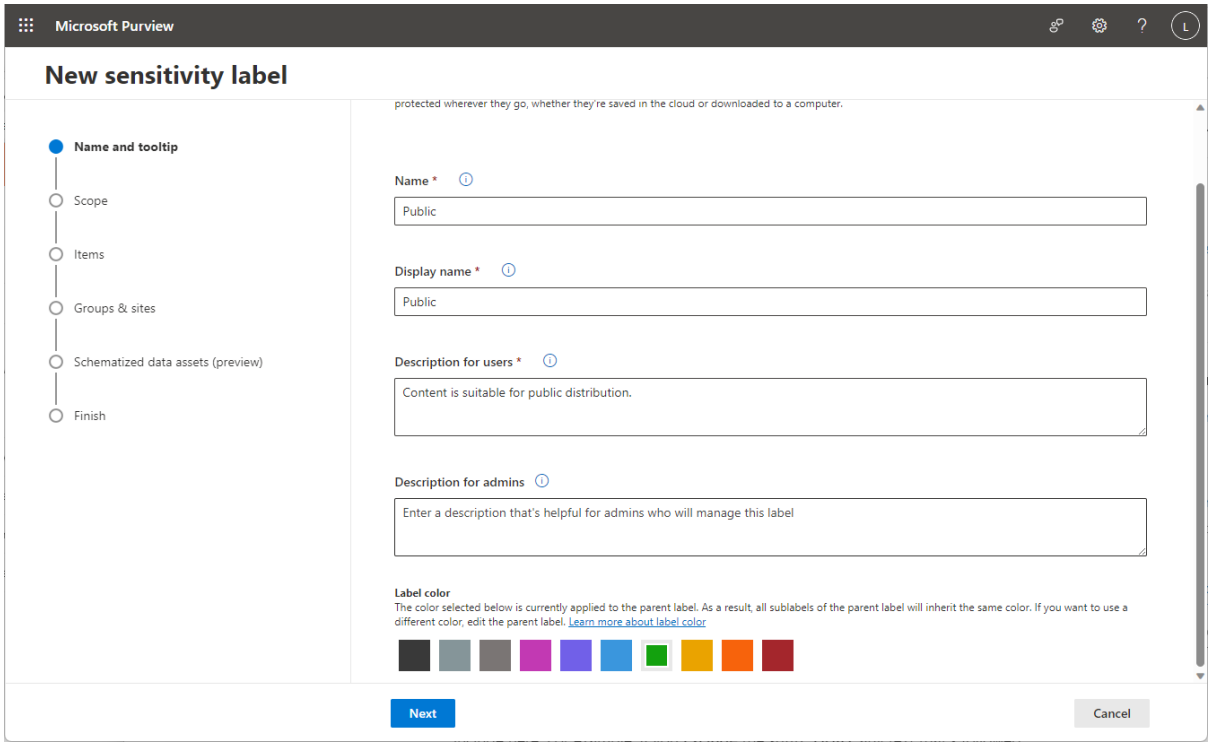

Figure 10.34 – Creating a new sensitivity label

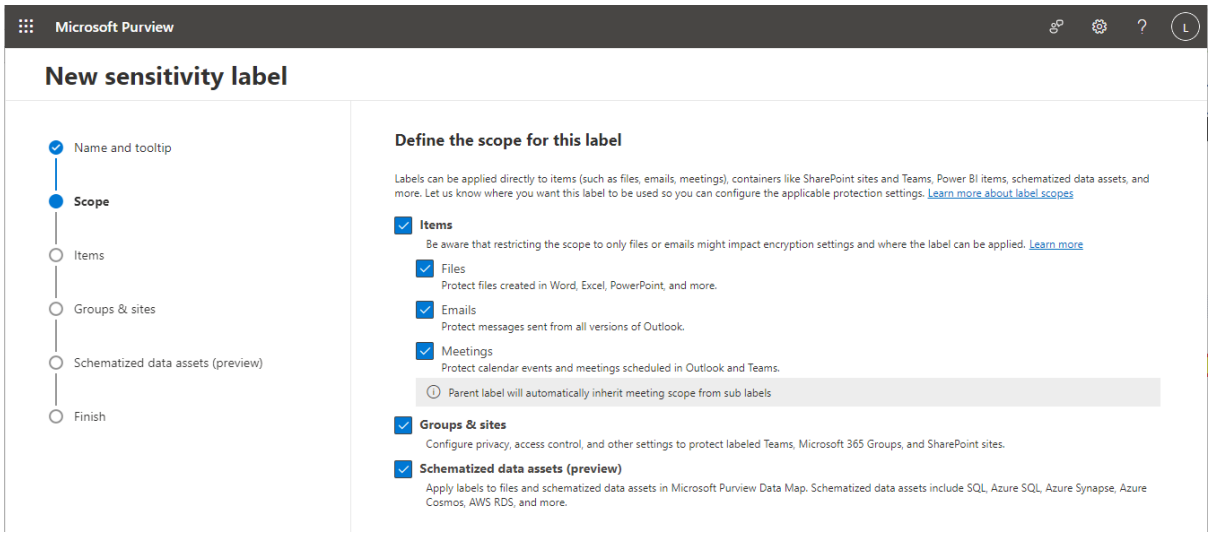

Figure 10.35 – Defining the scope of the label

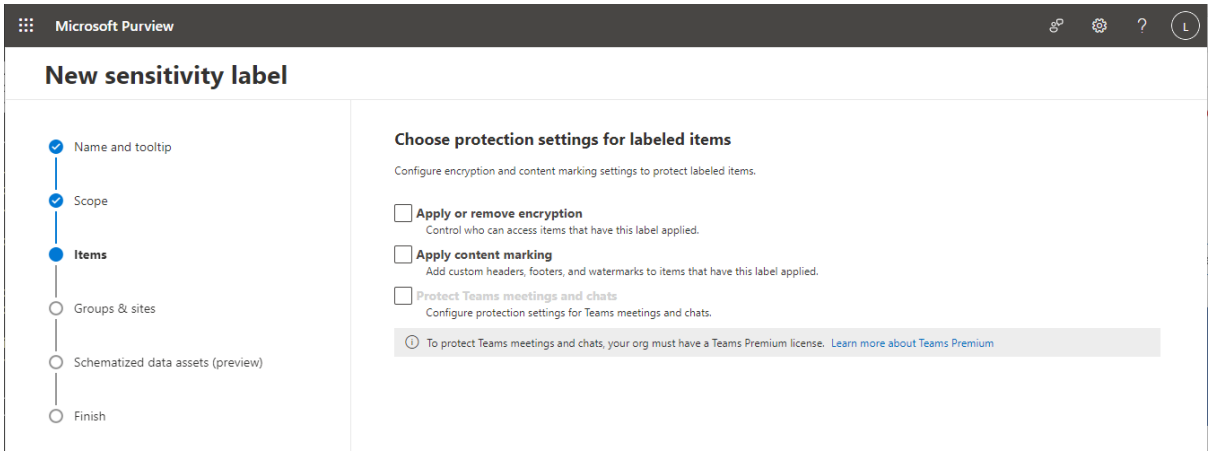

Figure 10.36 – Choosing protection settings

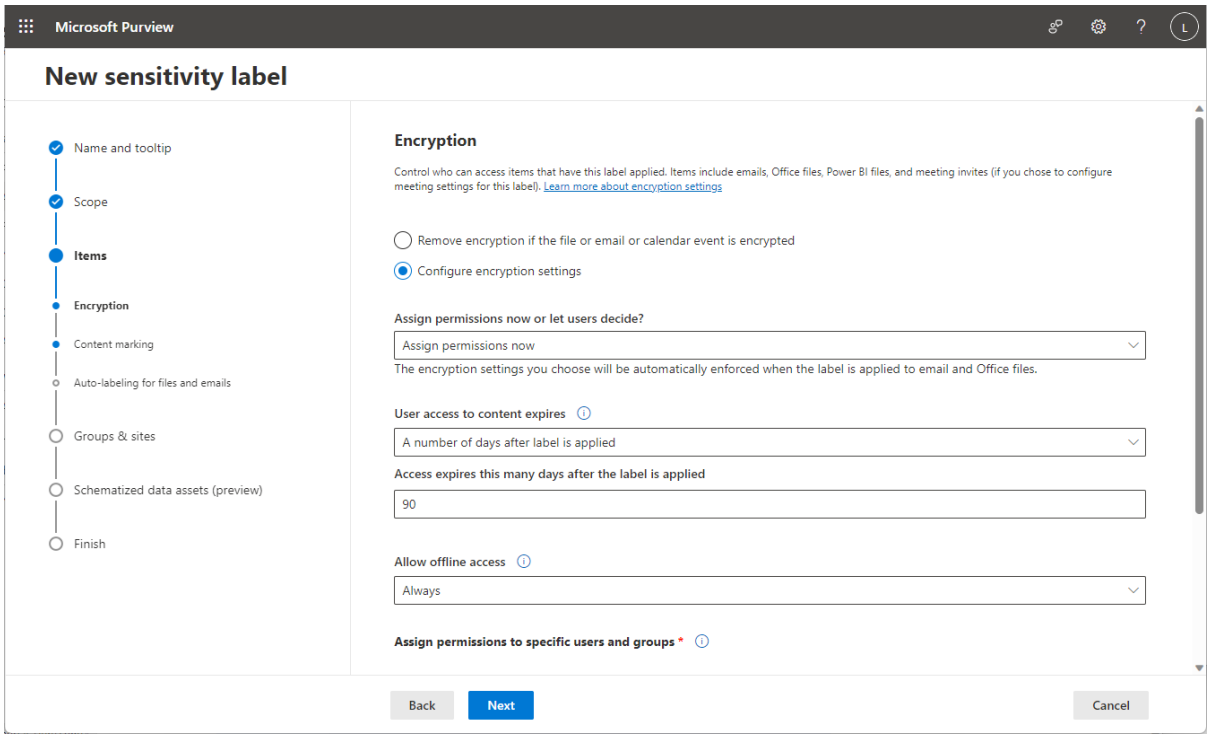

Figure 10.37 – Choosing encryption settings

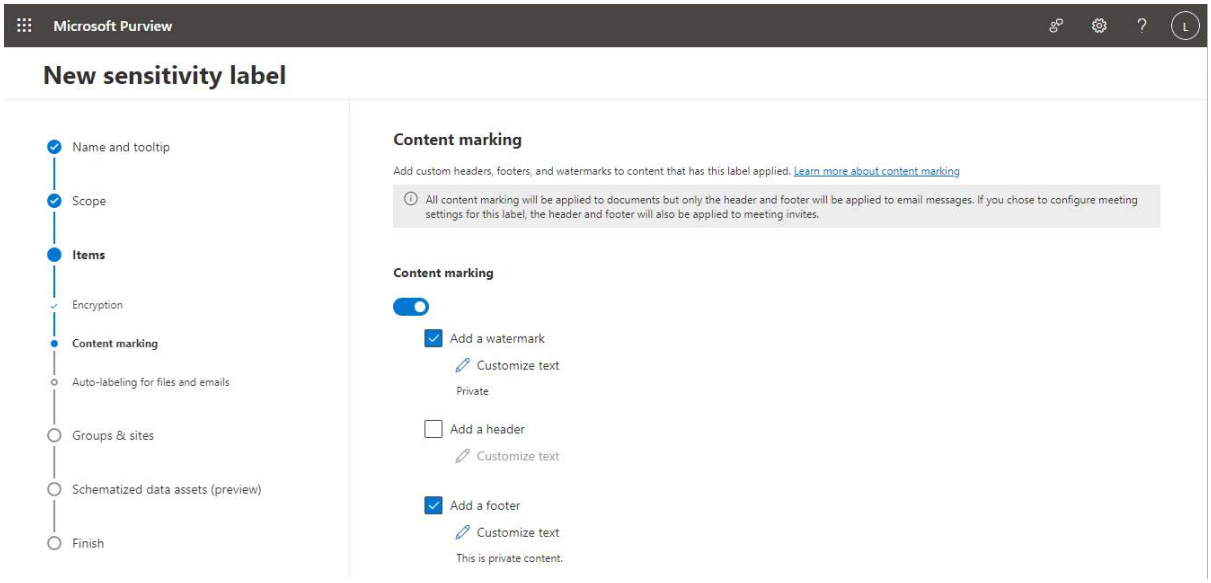

Figure 10.38 – Applying content marking settings

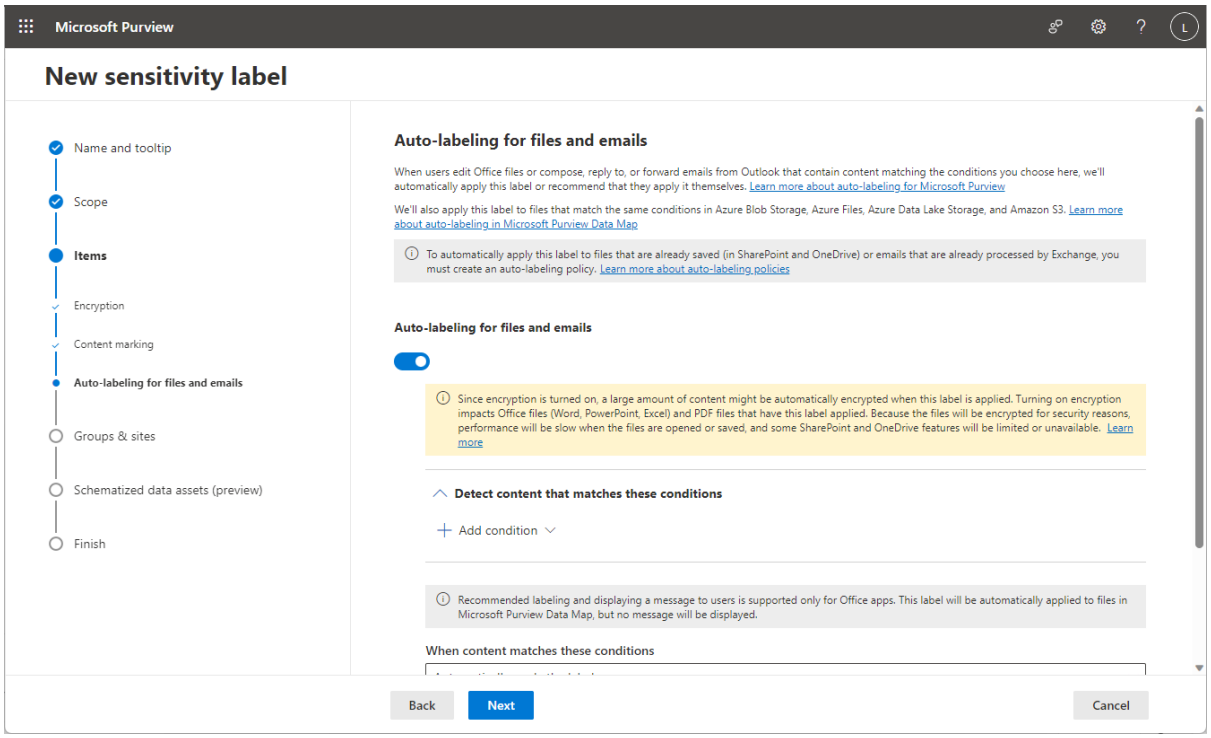

Figure 10.39 – Enabling auto-labeling

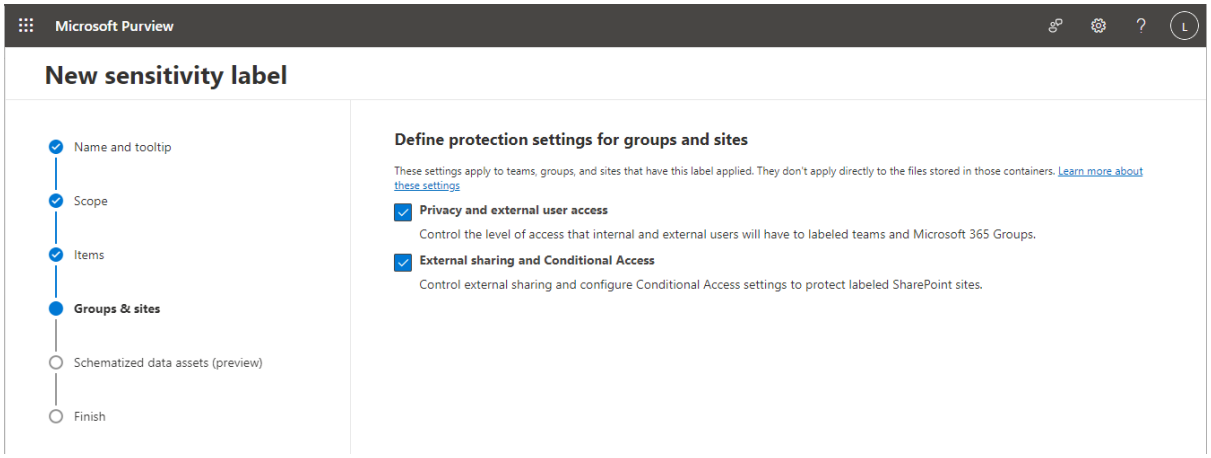

Figure 10.40 – Defining protections for groups and sites

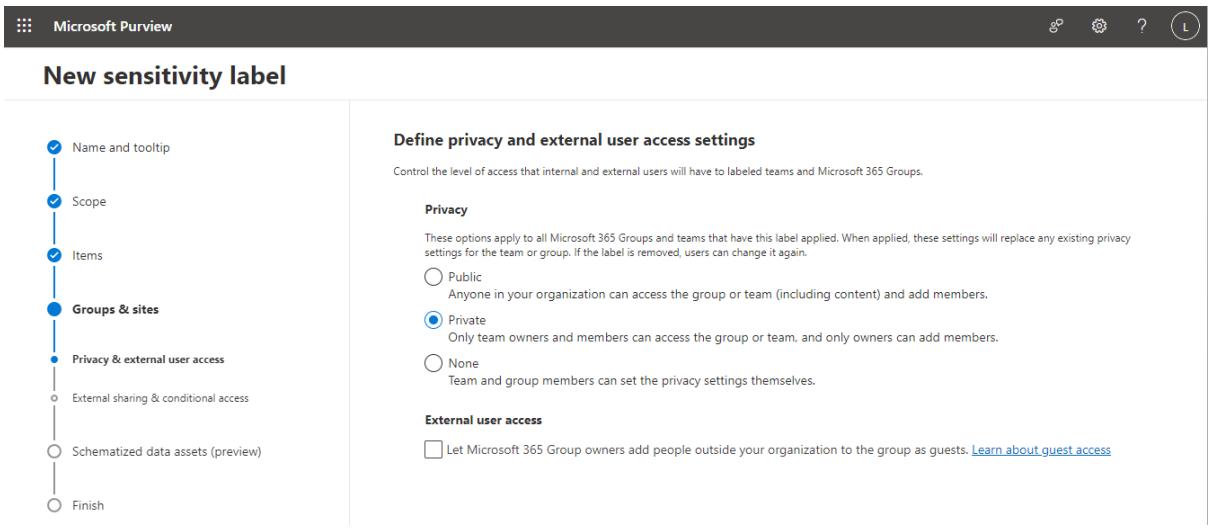

Figure 10.41 – Configuring privacy and external access settings

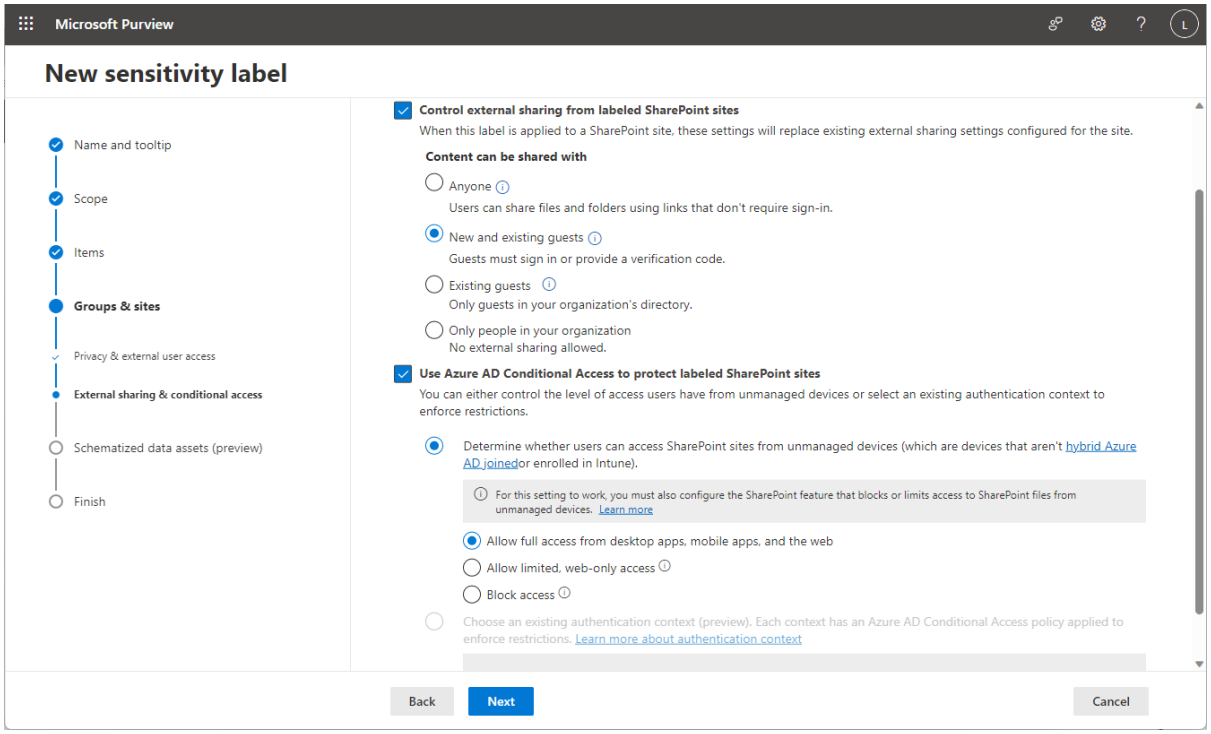

Figure 10.42 – Configuring external sharing and Conditional Access controls

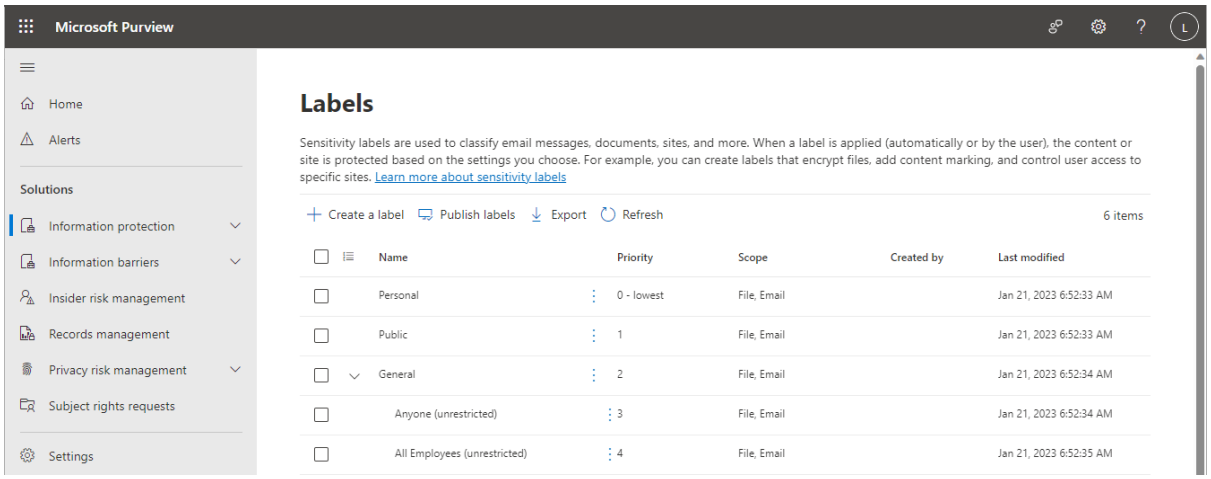

Figure 10.43 – Sublabel example

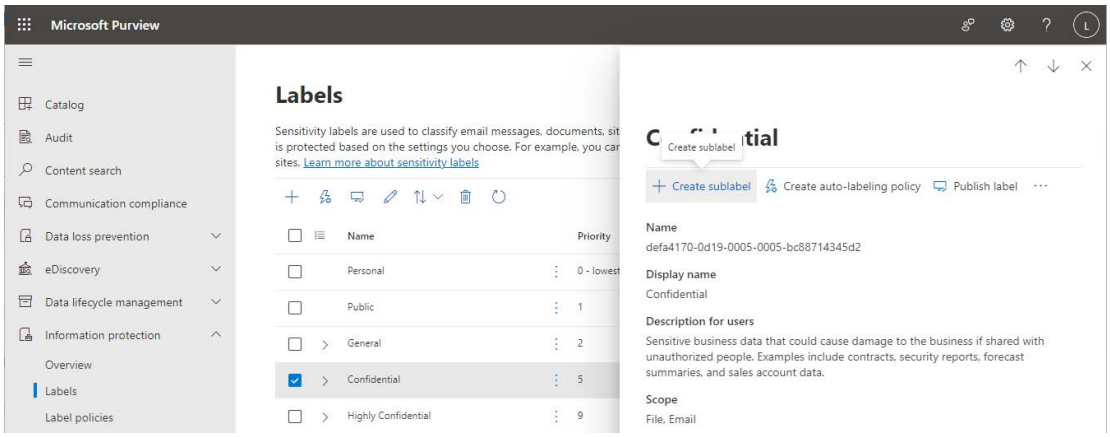

Figure 10.44 – Creating a sublabel

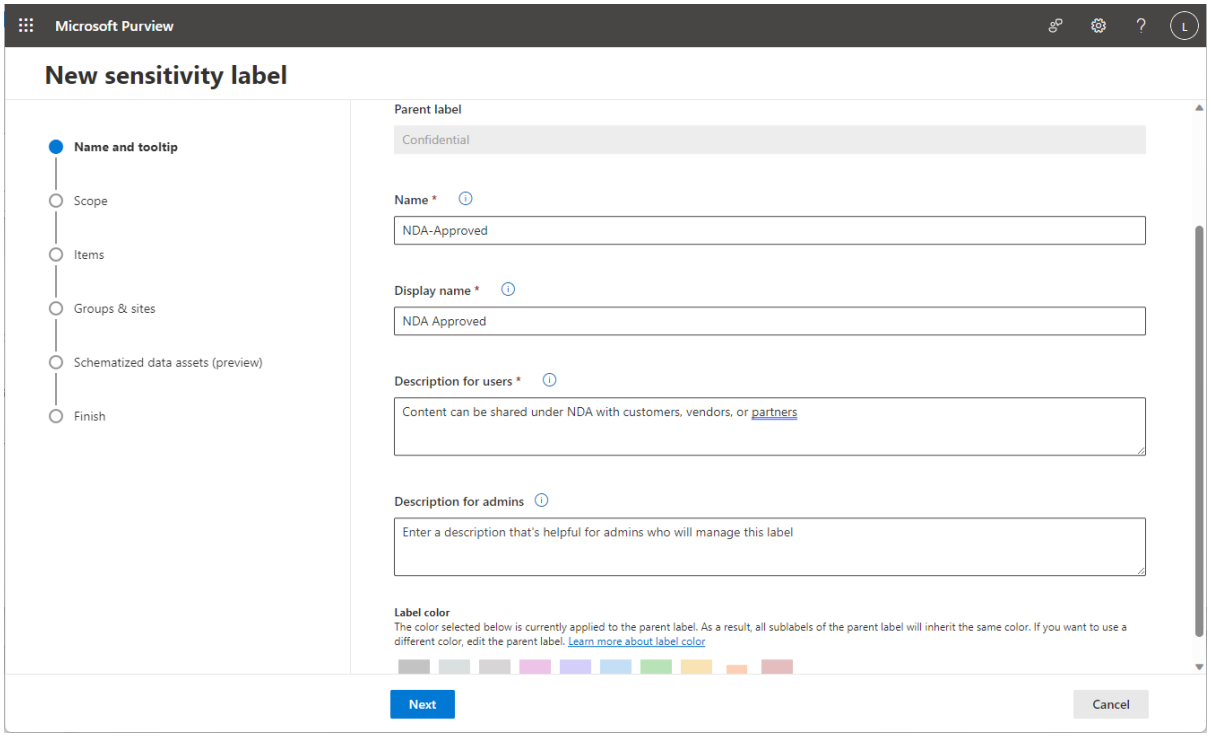

Figure 10.45 – Reviewing name and tooltip settings

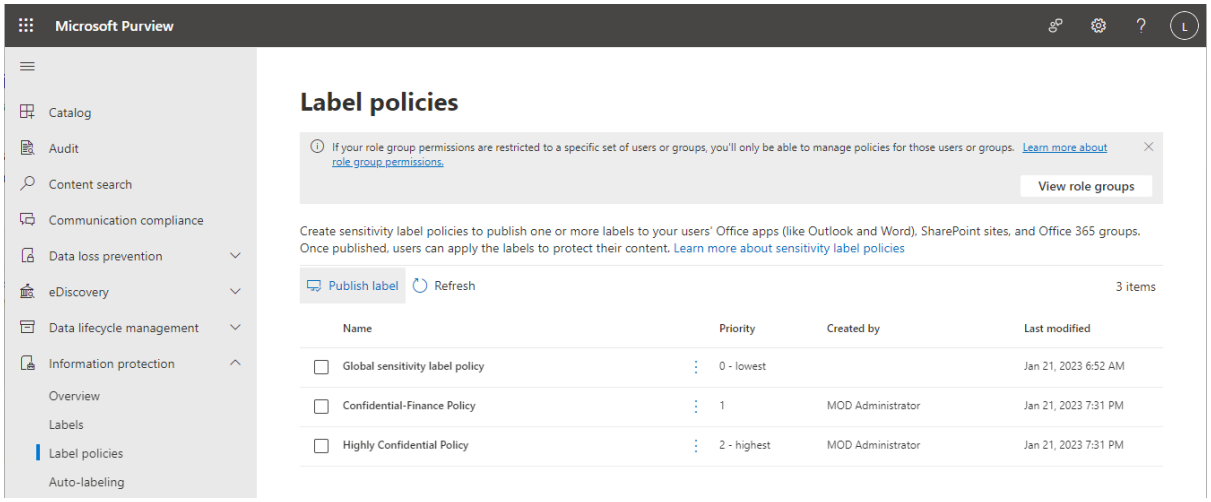

Figure 10.46 – Publishing a label

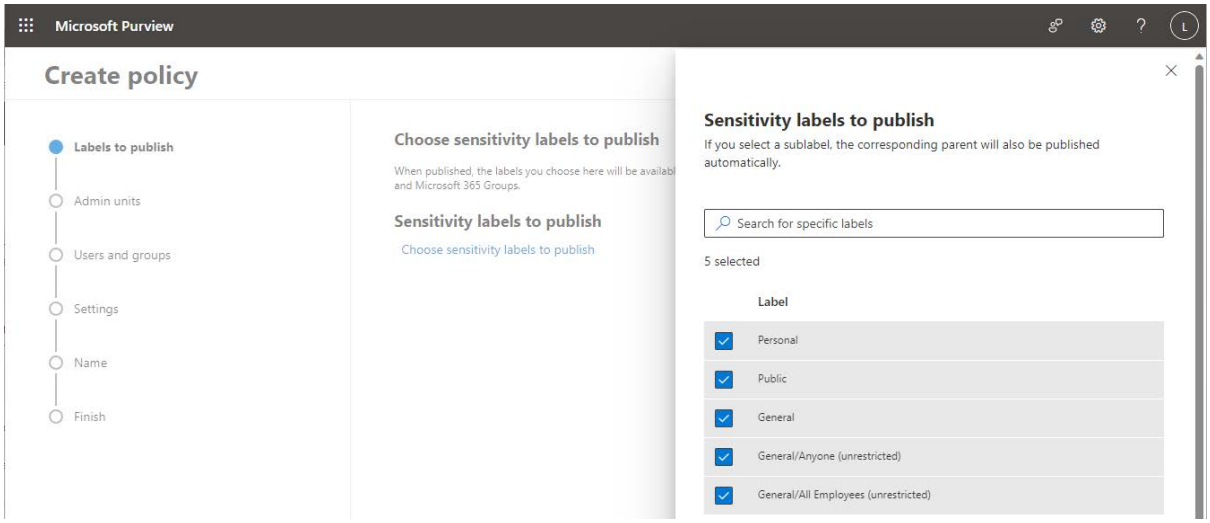

Figure 10.47 – Selecting labels to publish

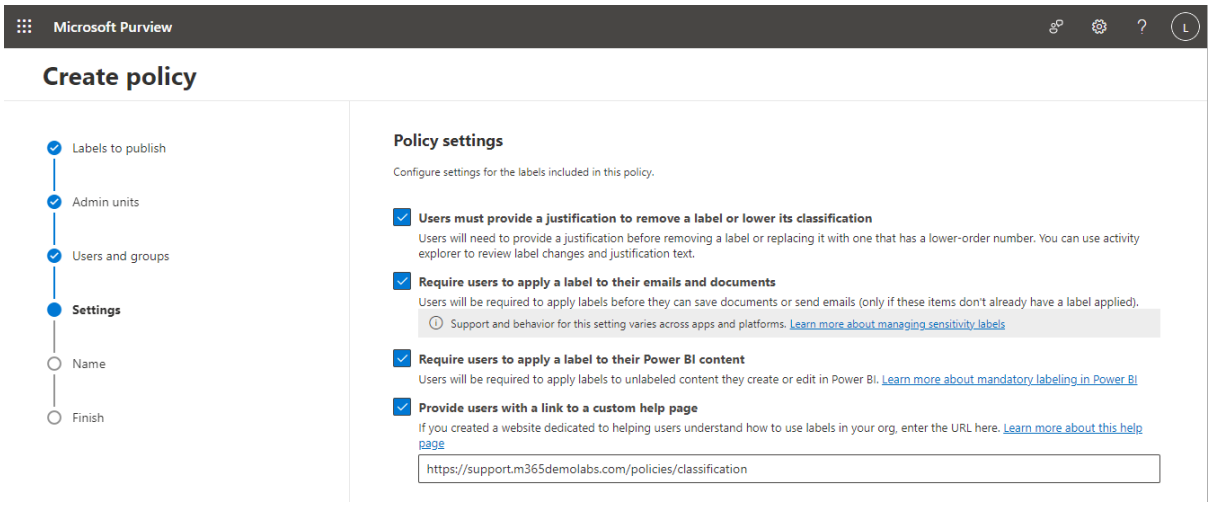

Figure 10.48 – Configuring policy settings

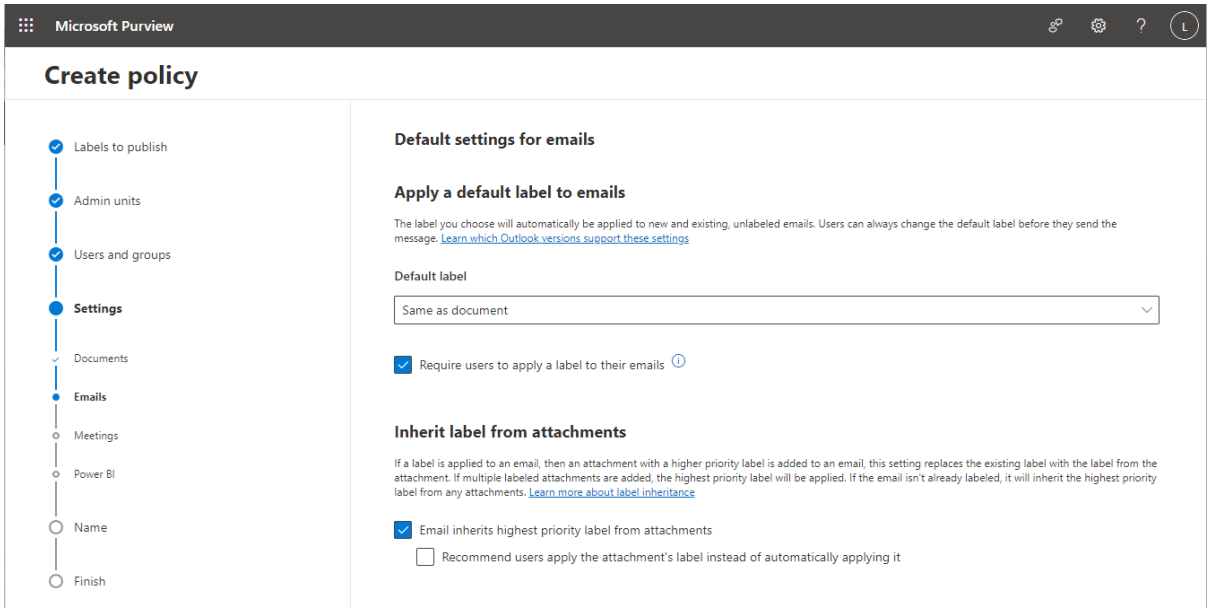

Figure 10.49 – Configuring email settings

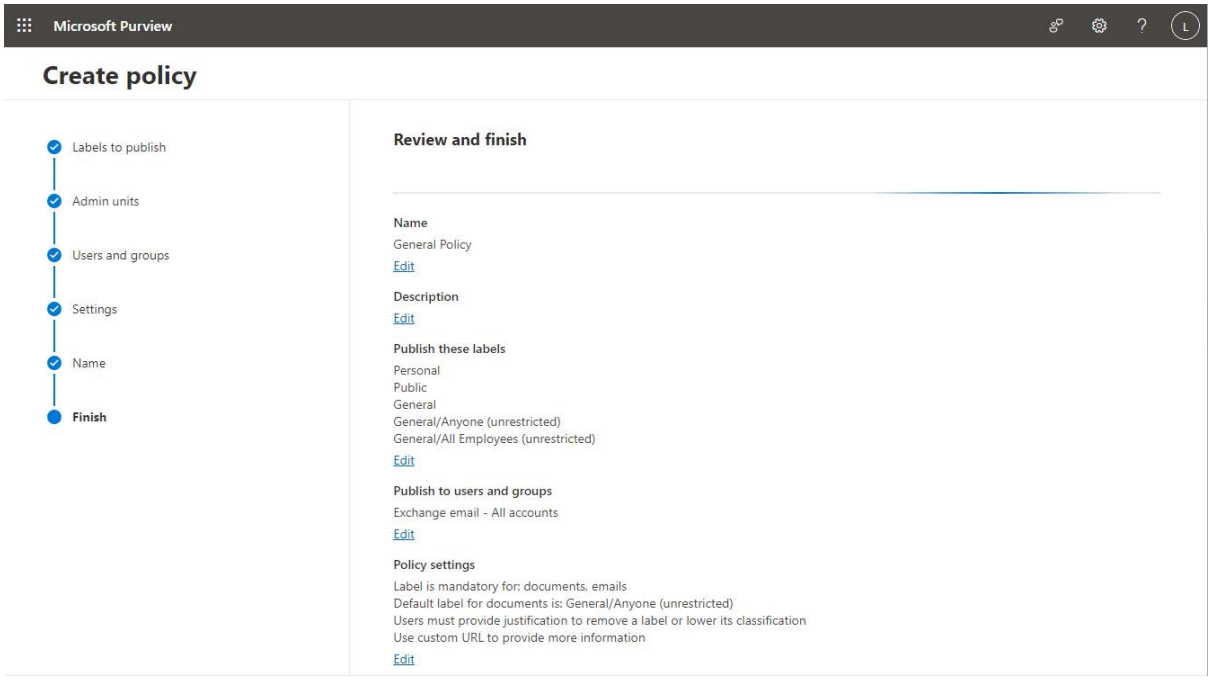

Figure 10.50 – Reviewing the final settings

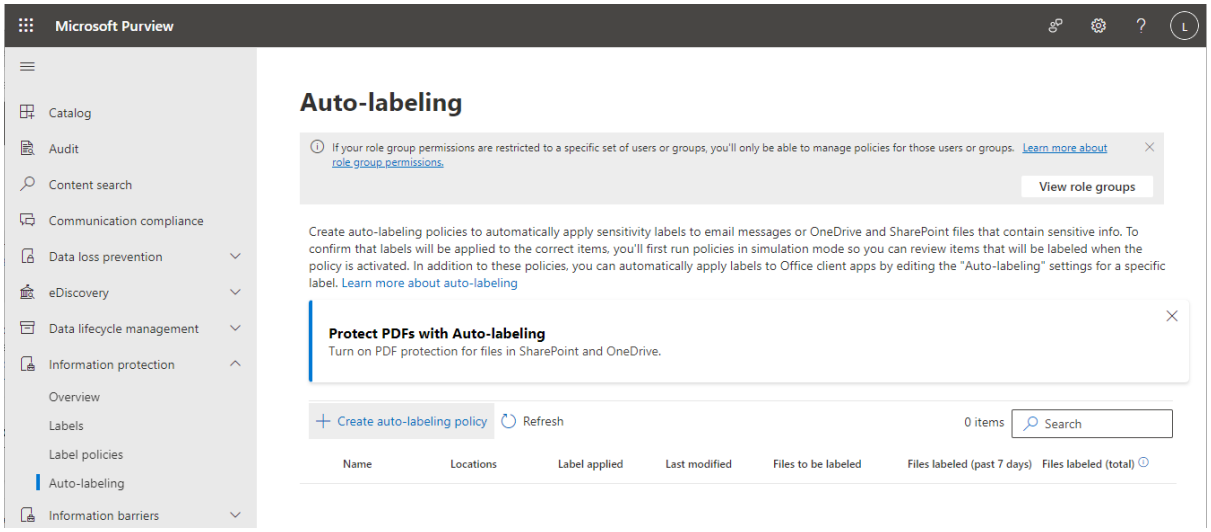

Figure 10.51 – Selecting Create auto-labeling policy

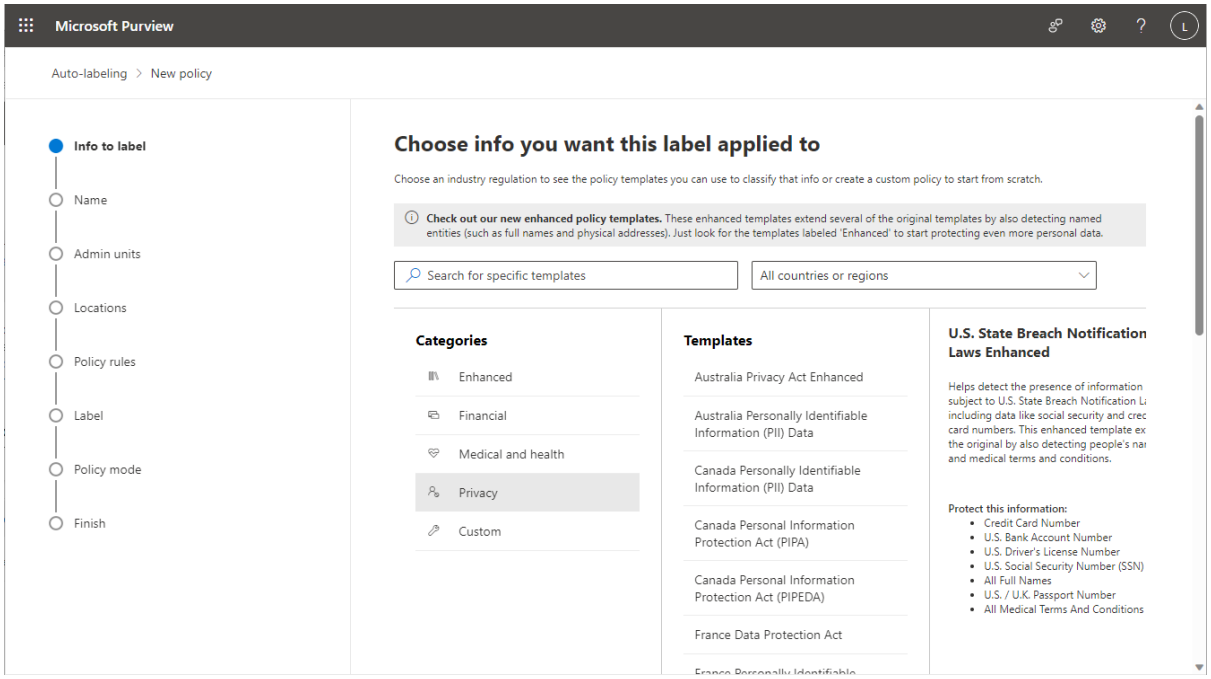

Figure 10.52 – Selecting a category template

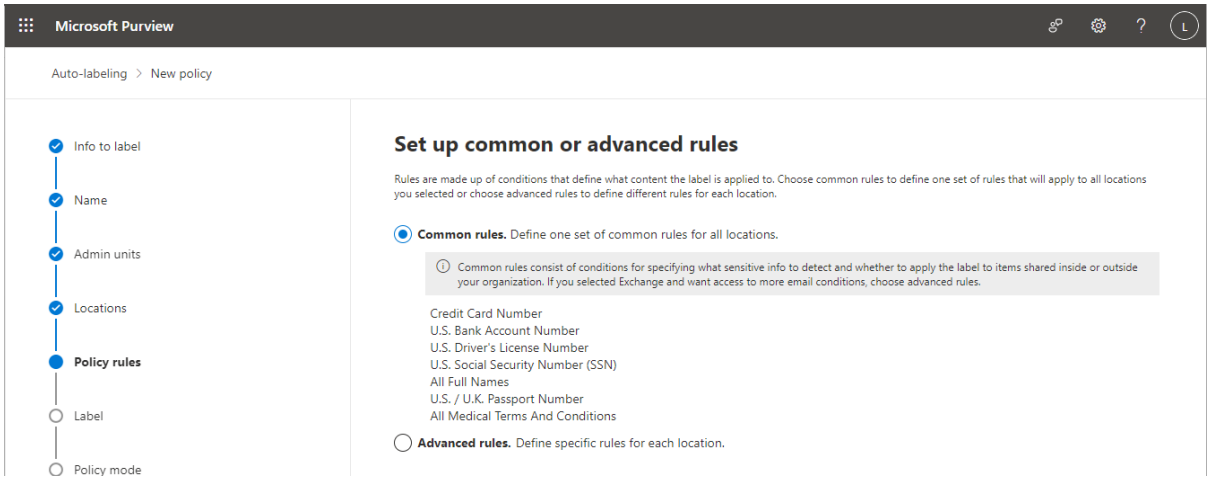

Figure 10.53 – Selecting policy rules

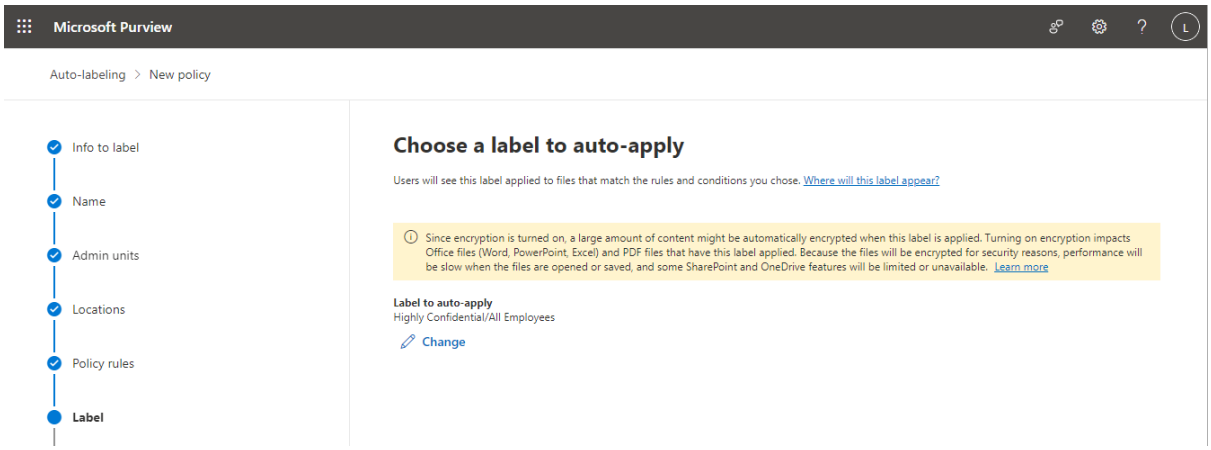

Figure 10.54 – Selecting the label to apply

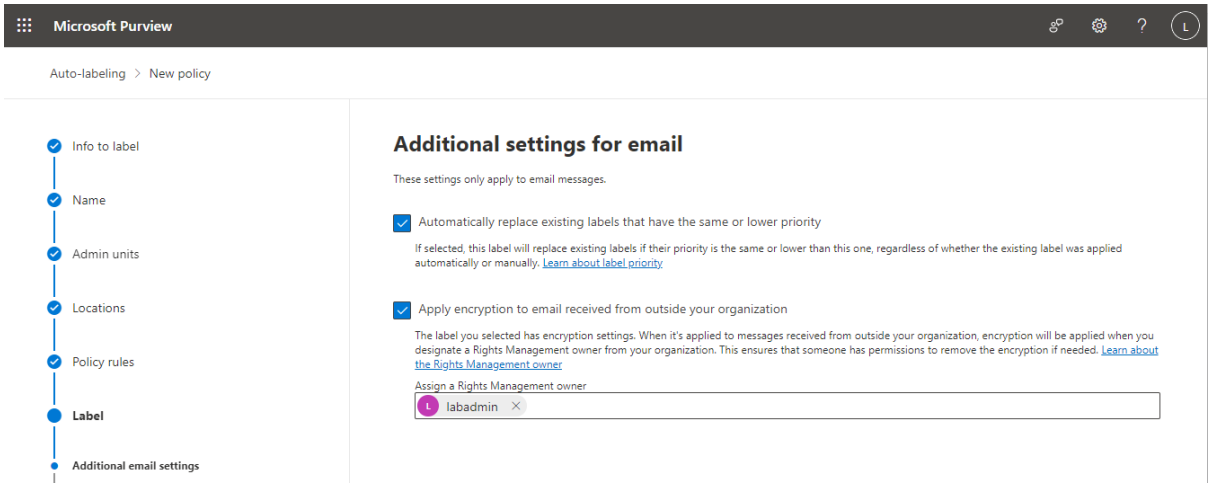

Figure 10.55 – Specifying additional settings for email

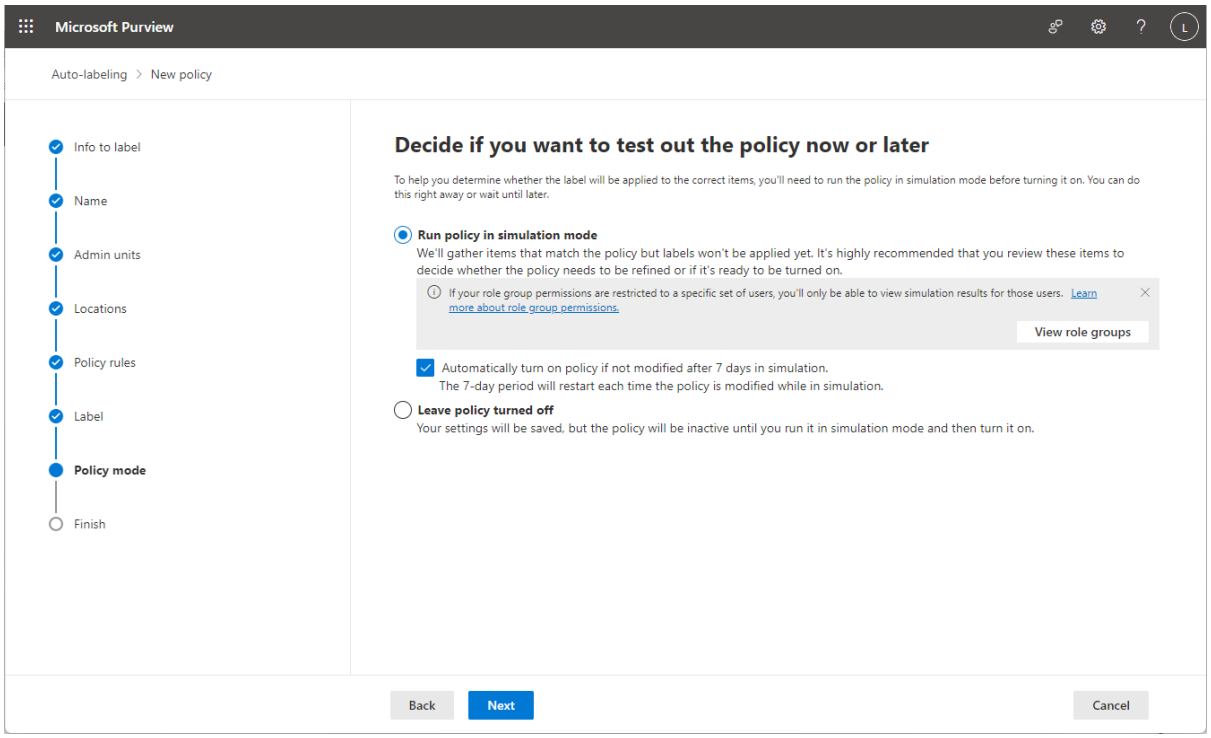

Figure 10.56 – Choosing the policy mode

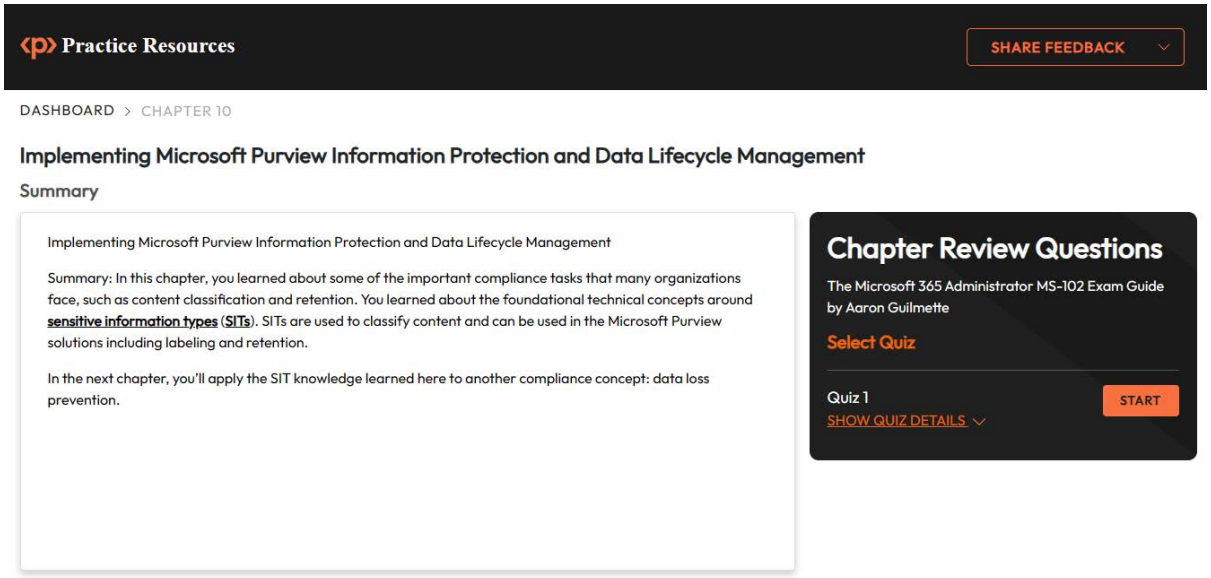

Figure 10.57 – Chapter Review Questions for Chapter 10

Chapter 11: Implementing Microsoft Purview Data Loss Prevention

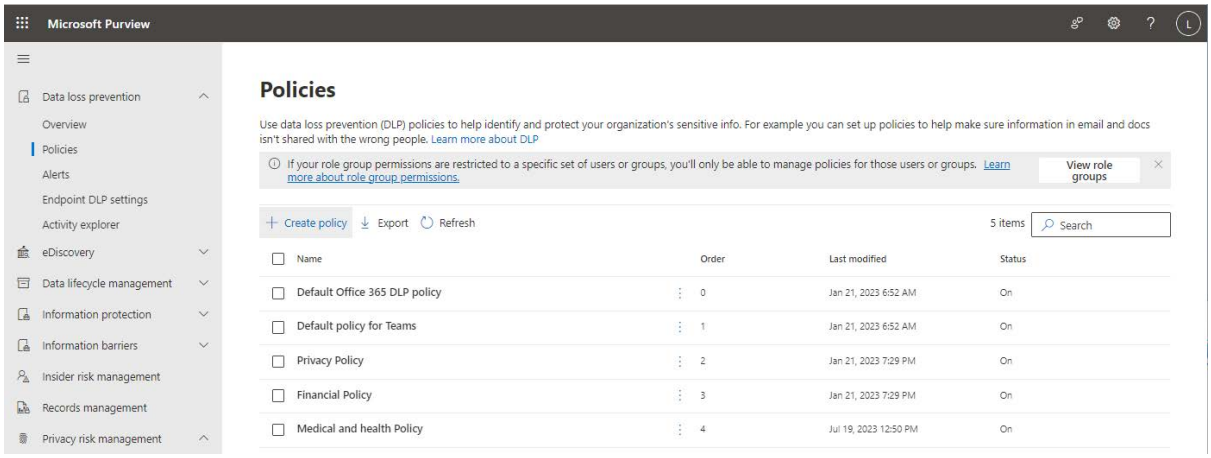

Figure 11.1 – Microsoft Purview compliance policies page

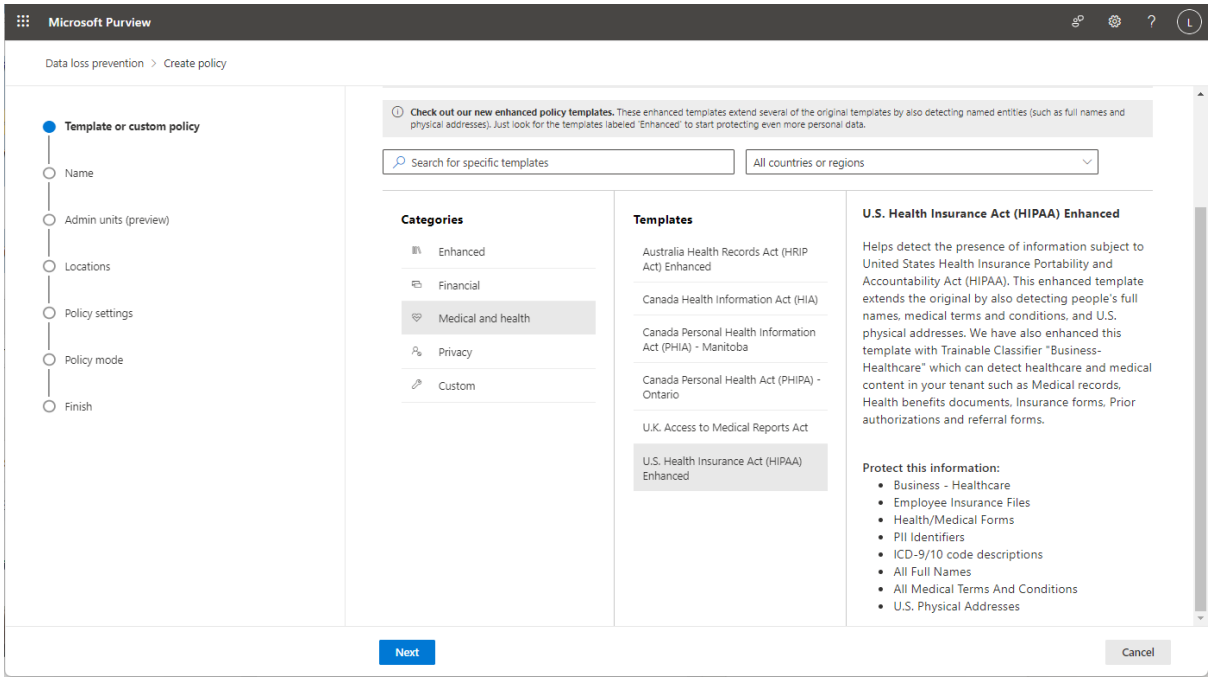

Figure 11.2 – Selecting a template or policy type

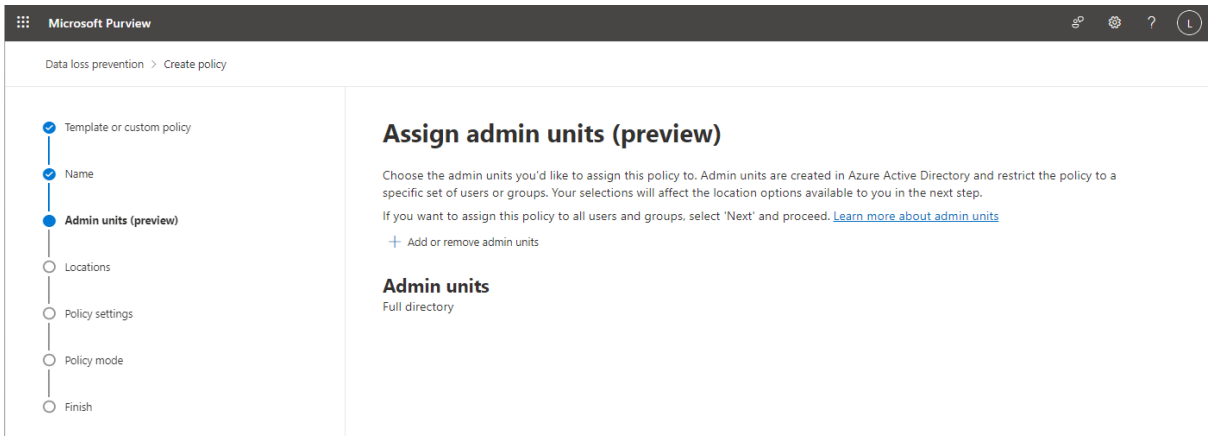

Figure 11.3 – Assigning an administrative unit

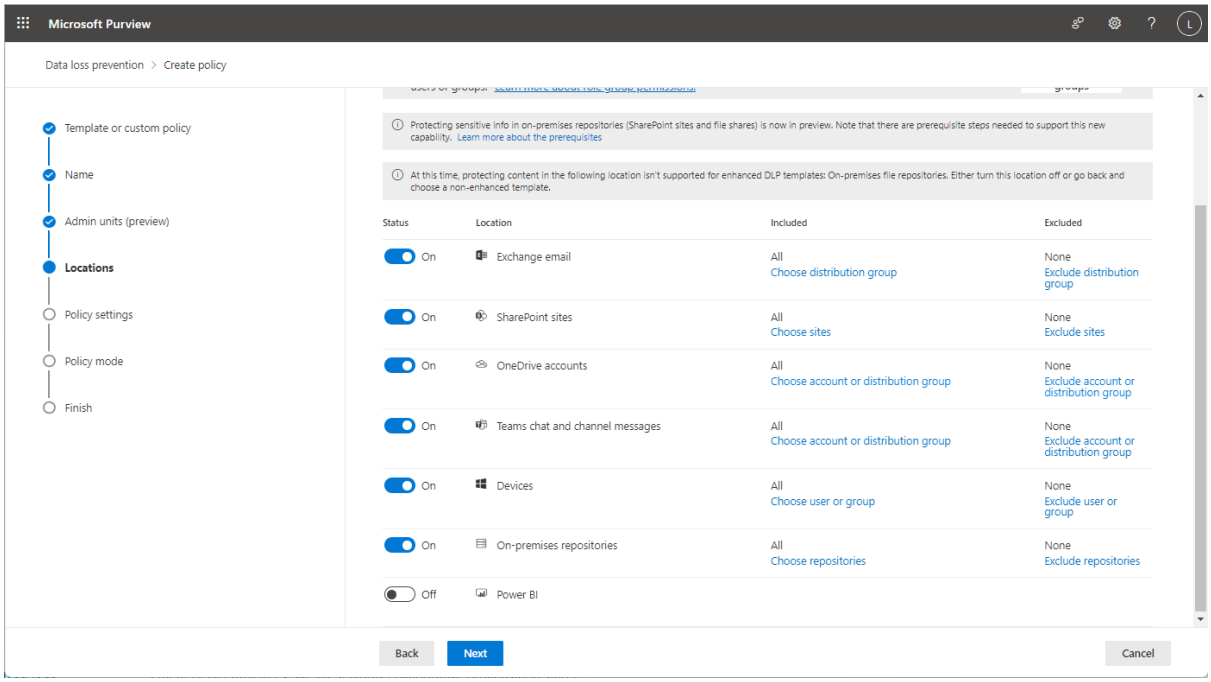

Figure 11.4 – Adding workloads and locations to the policy

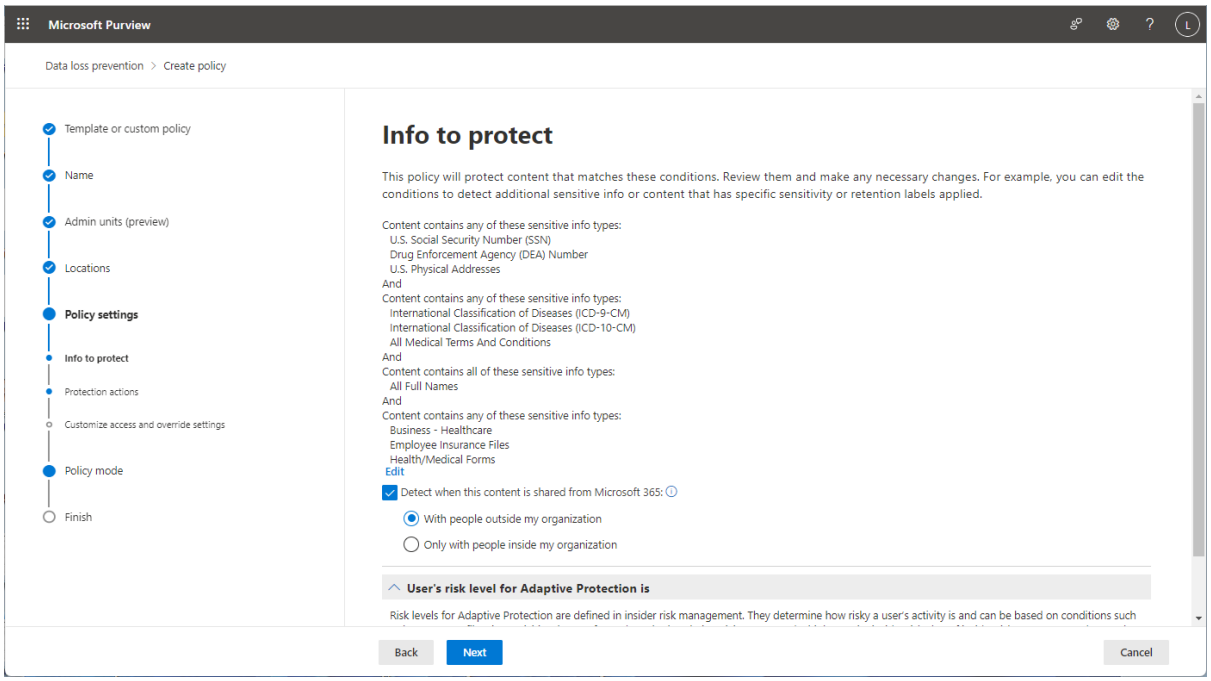

Figure 11.5 – Reviewing the Info to protect page

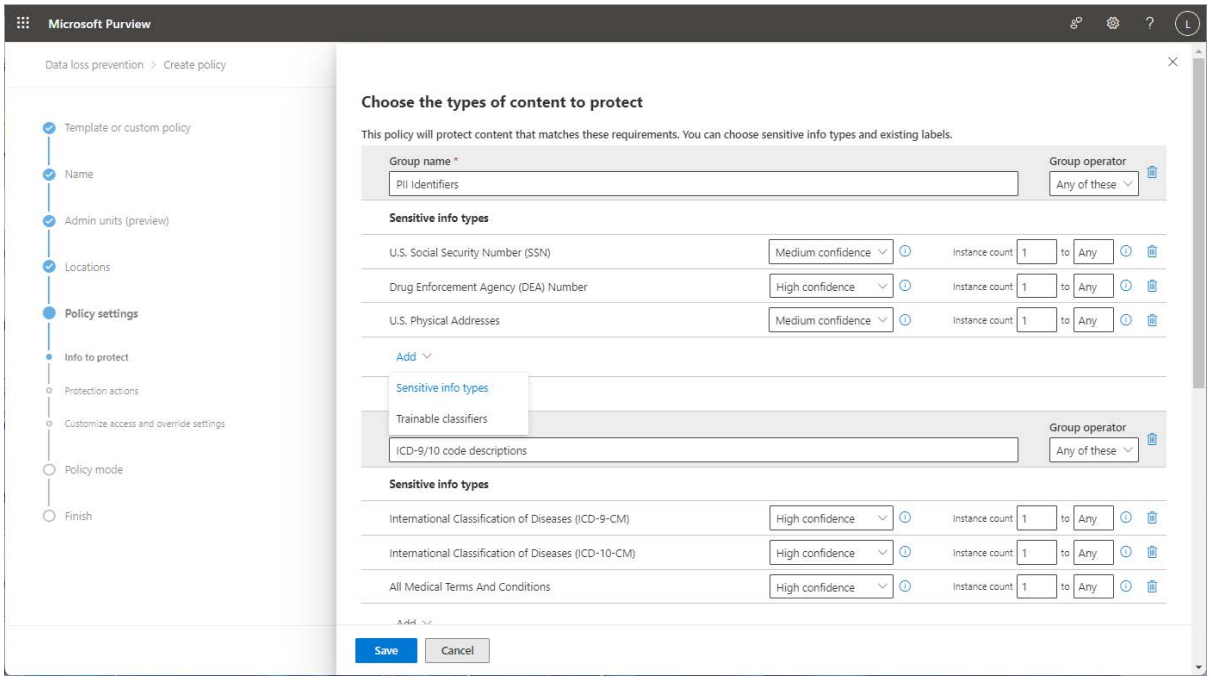

Figure 11.6 – Editing a DLP match rule

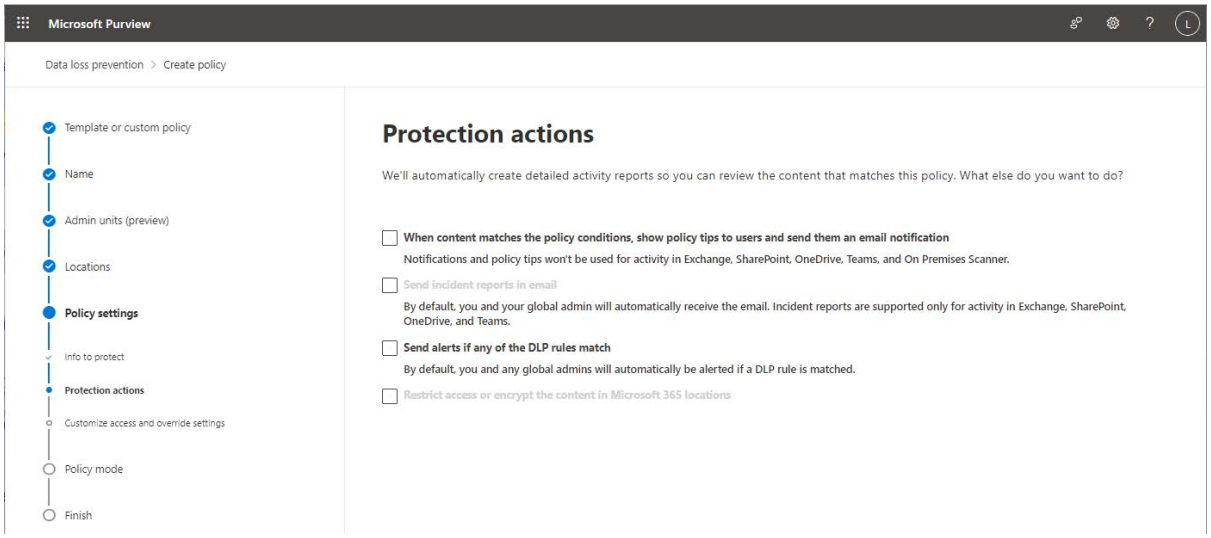

Figure 11.7 – Configuring protection actions

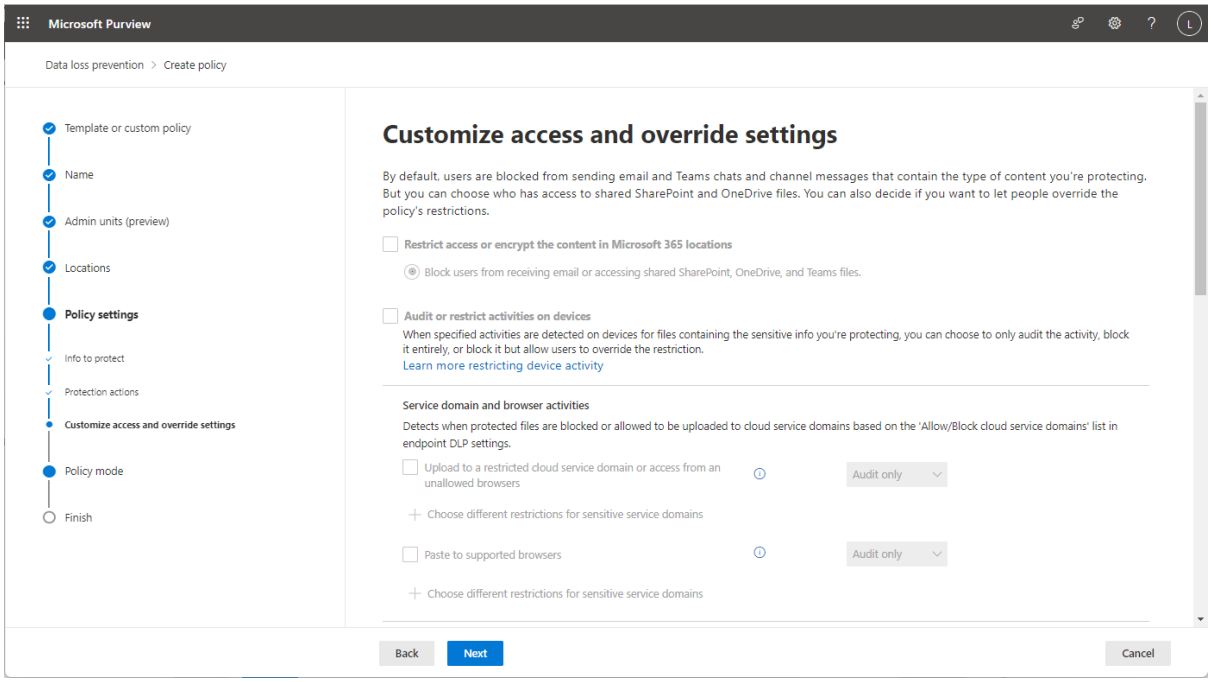

Figure 11.8 – Customize access and override settings

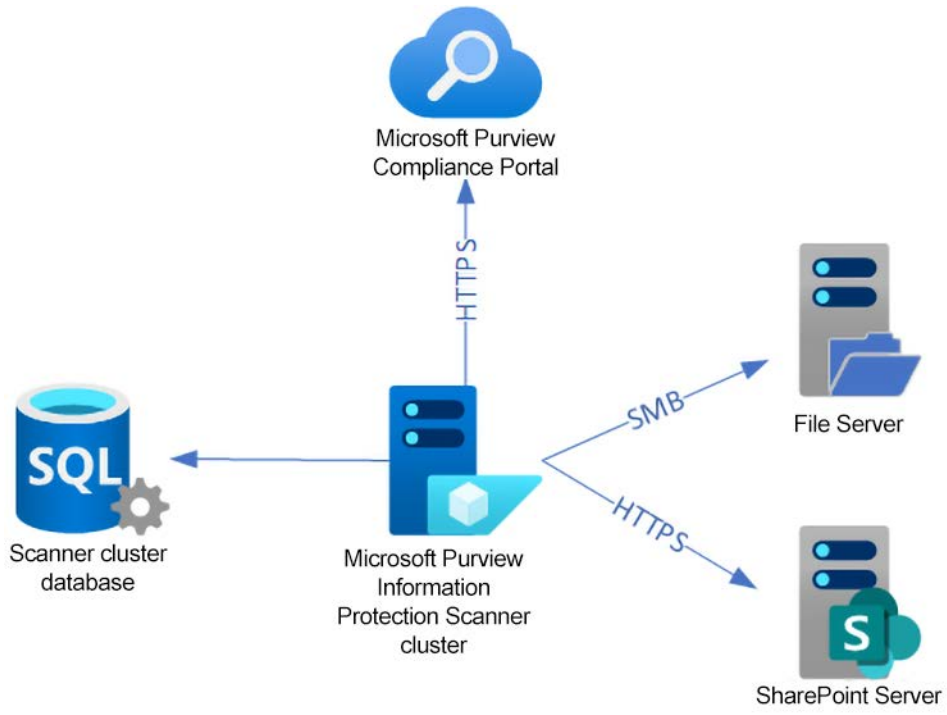

Figure 11.9 – On-premises DLP architecture

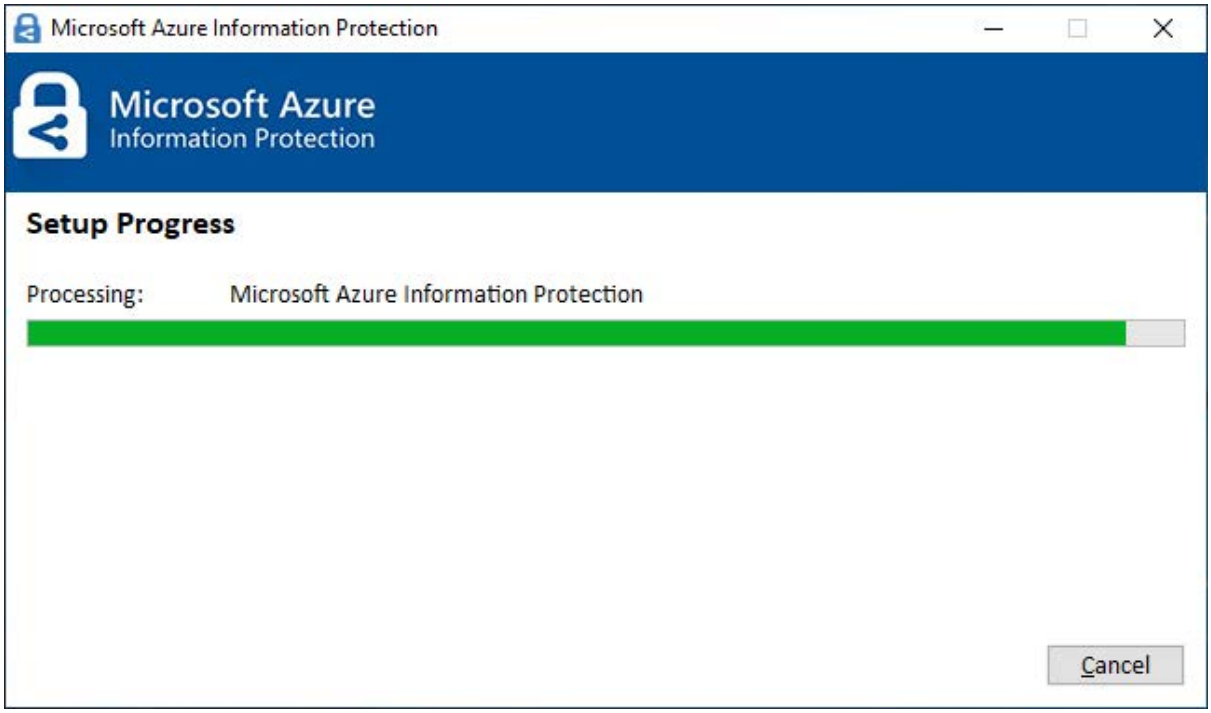

Figure 11.10 – AIP UL client installation

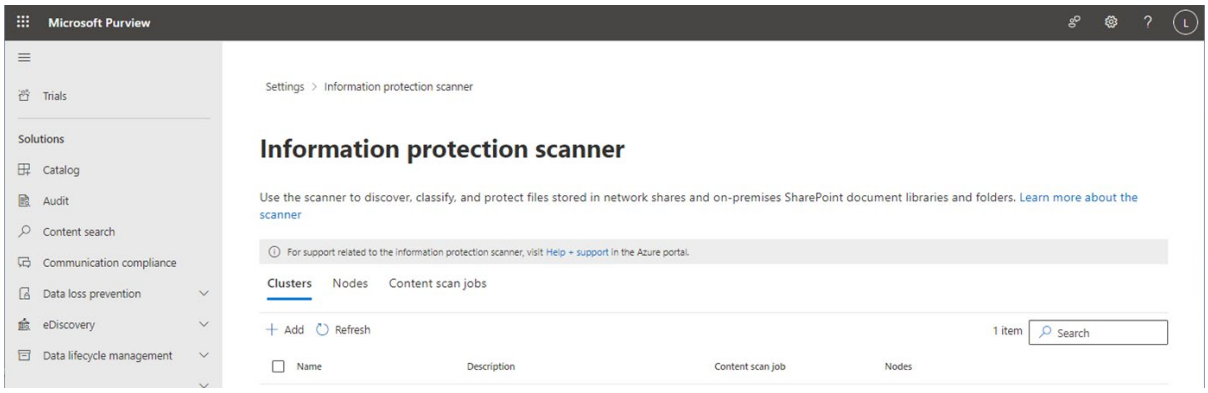

Figure 11.11 – AIP clusters page

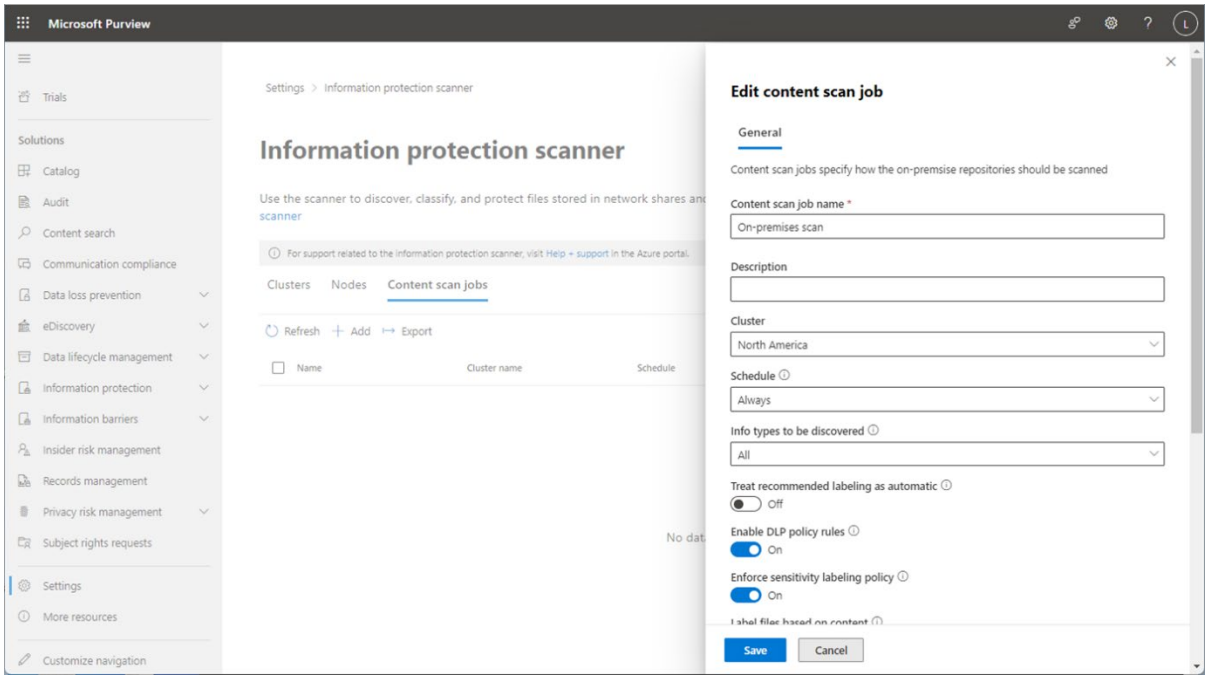

Figure 11.12 – Configuring content scan job settings

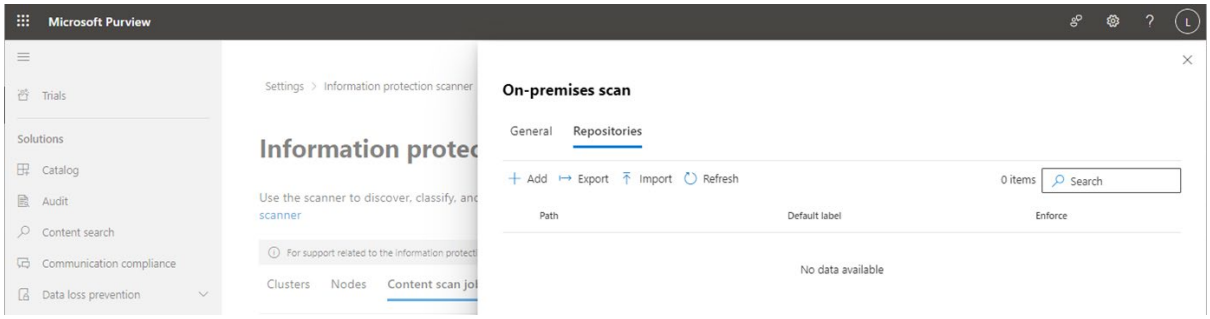

Figure 11.13 – Configuring repositories for the scan

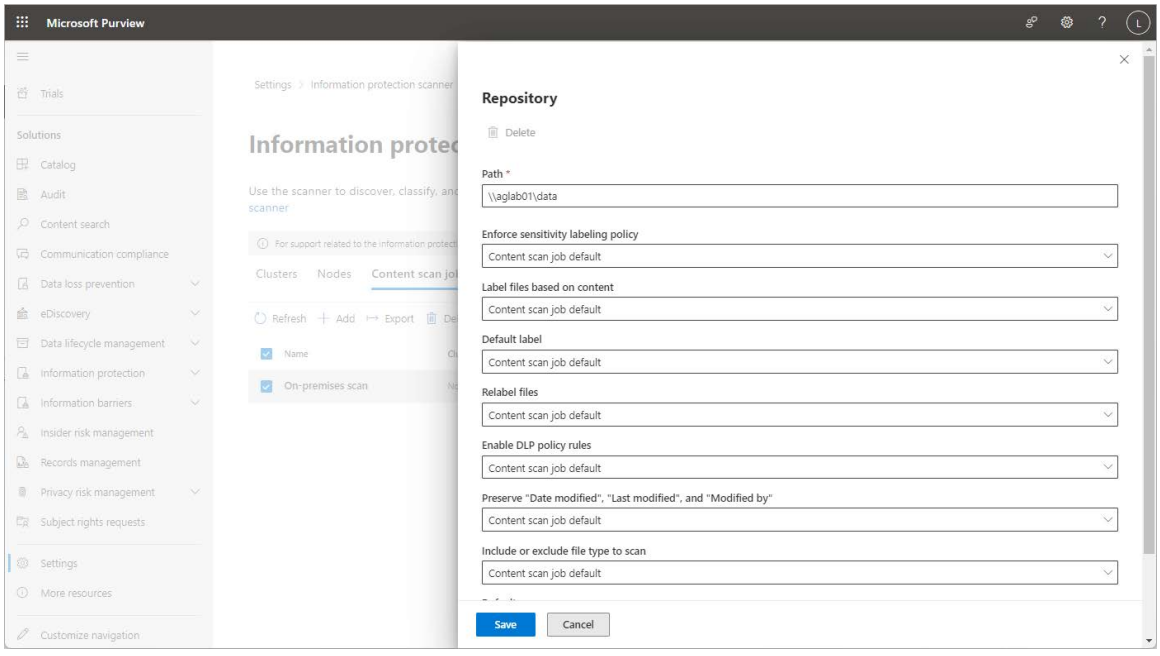

Figure 11.14 – Configuring repository settings

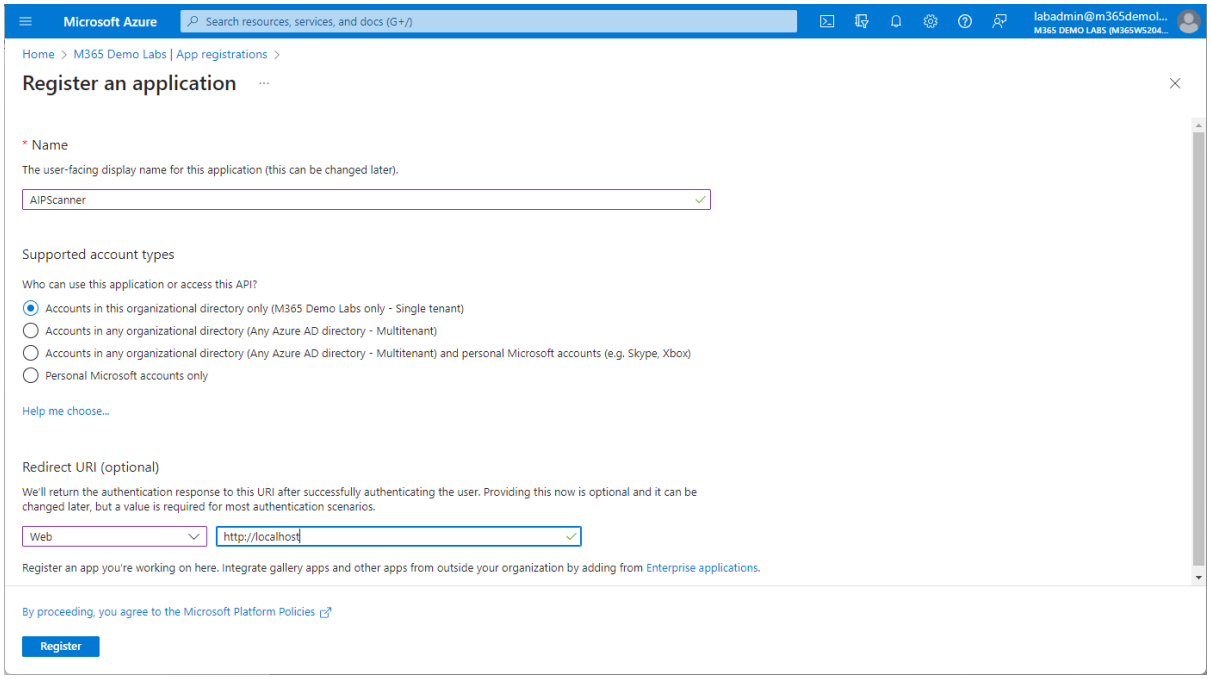

Figure 11.15 – Configuring an app registration

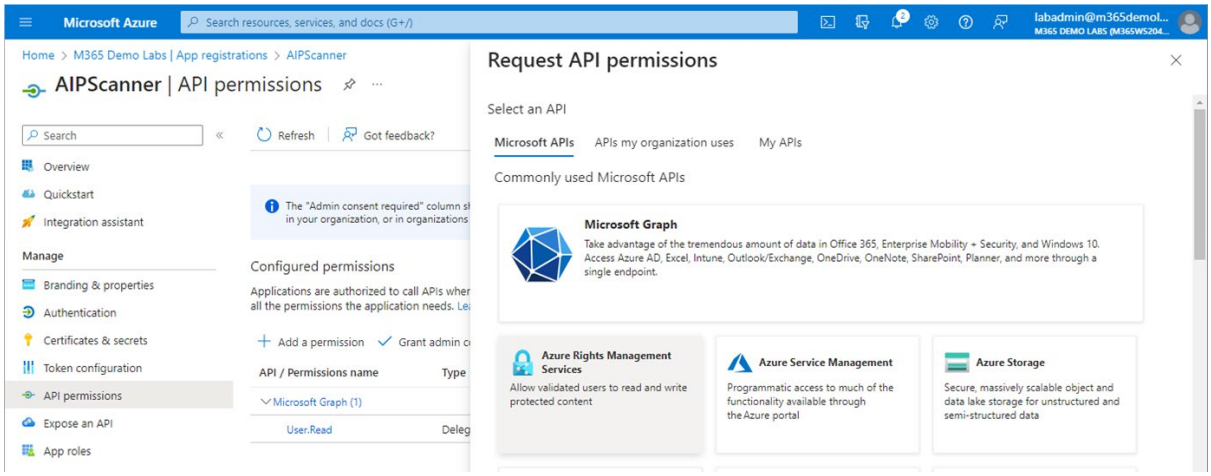

Figure 11.16 – Adding permissions on the Request API permissions flyout

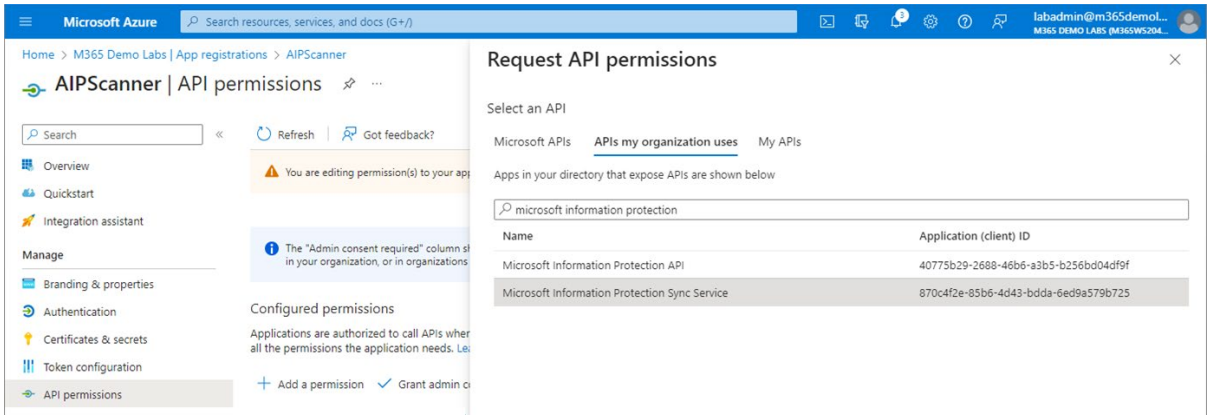

Figure 11.17 – Choosing the Microsoft Information Protection Sync Service API

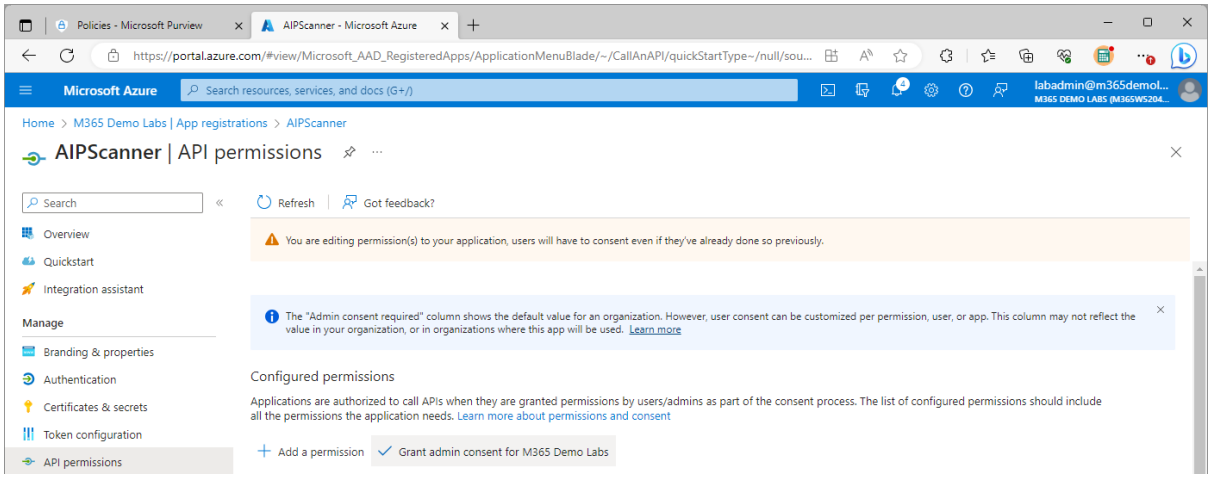

Figure 11.18 – Granting admin consent

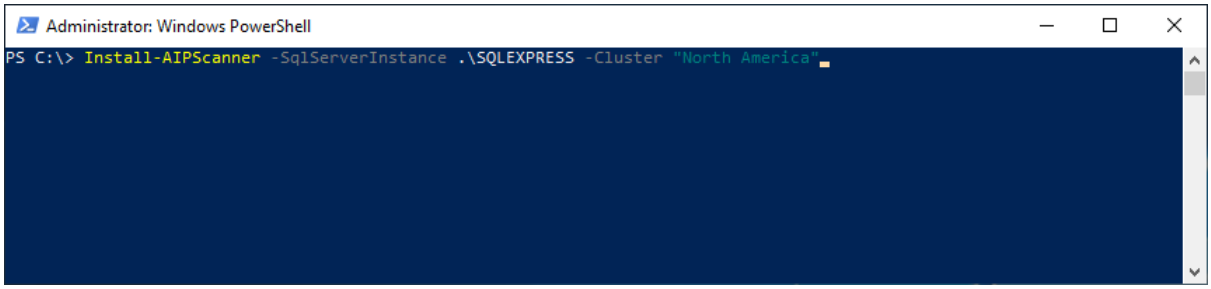

Figure 11.19 – Starting the AIP scanner installation

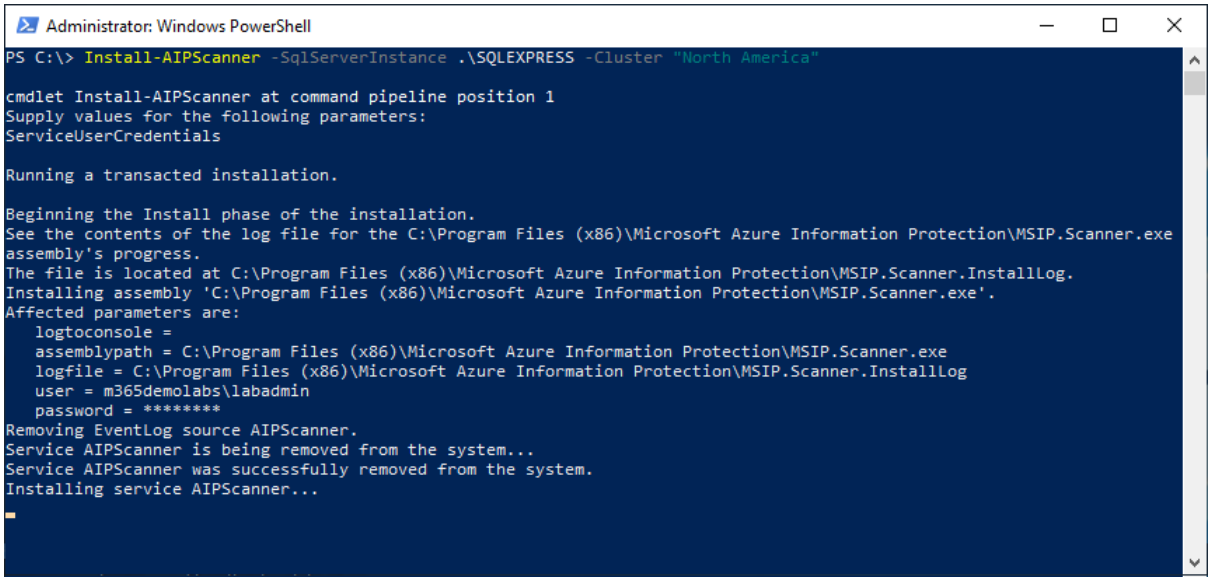

Figure 11.20 – Installing the AIP scanner

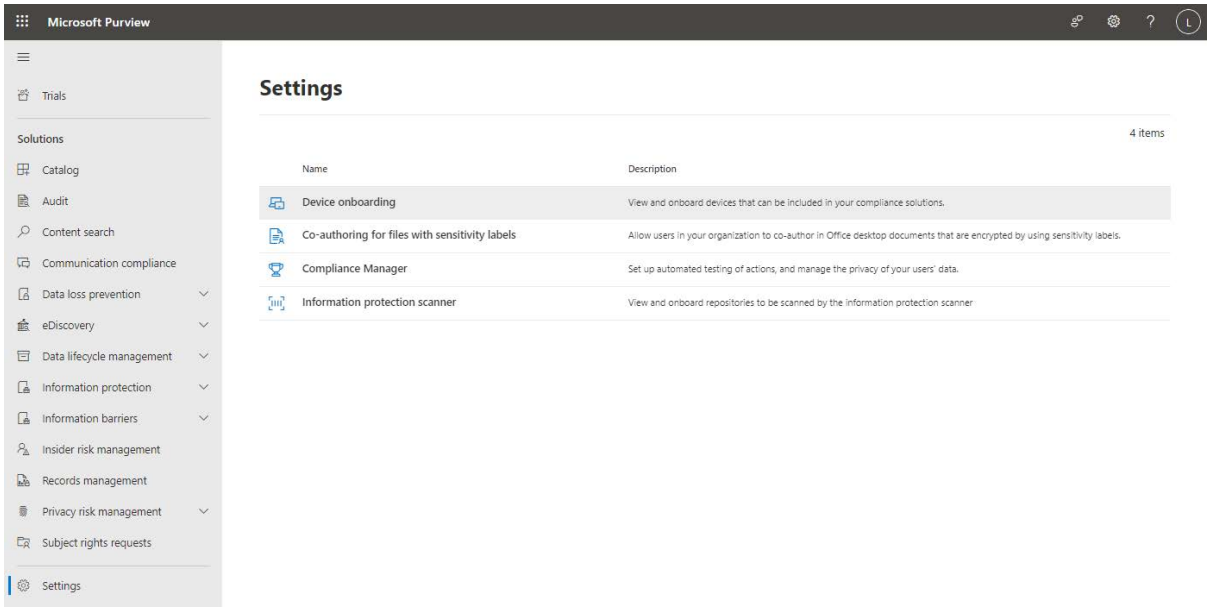

Figure 11.21 – Device onboarding

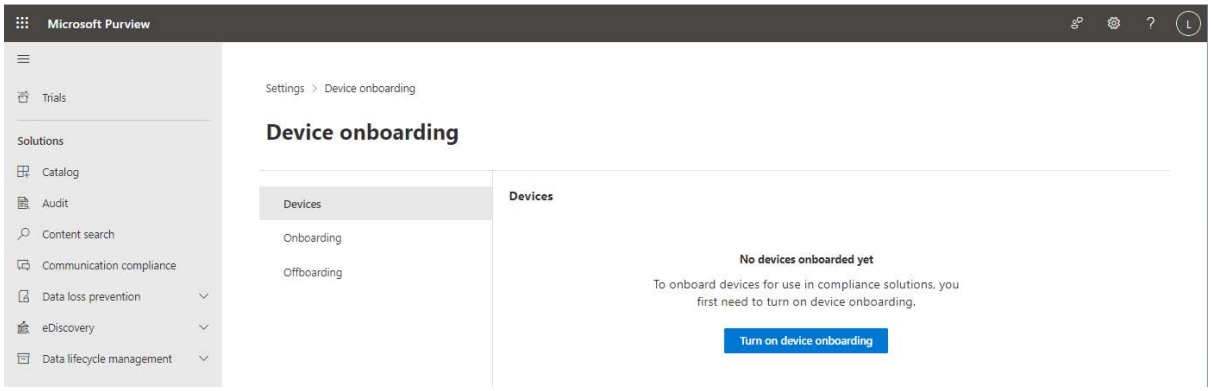

Figure 11.22 – Turning on device onboarding

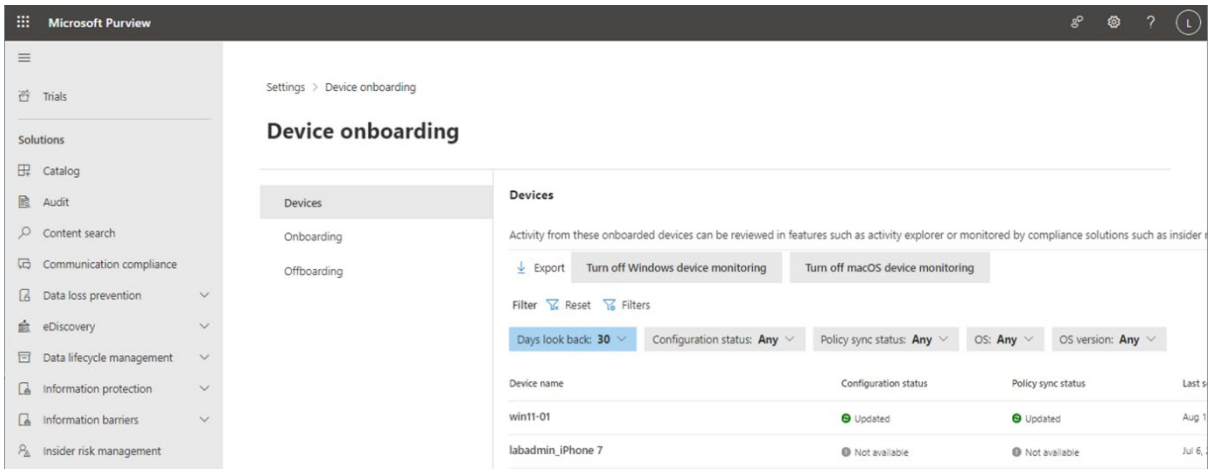

Figure 11.23 – List of onboarded devices

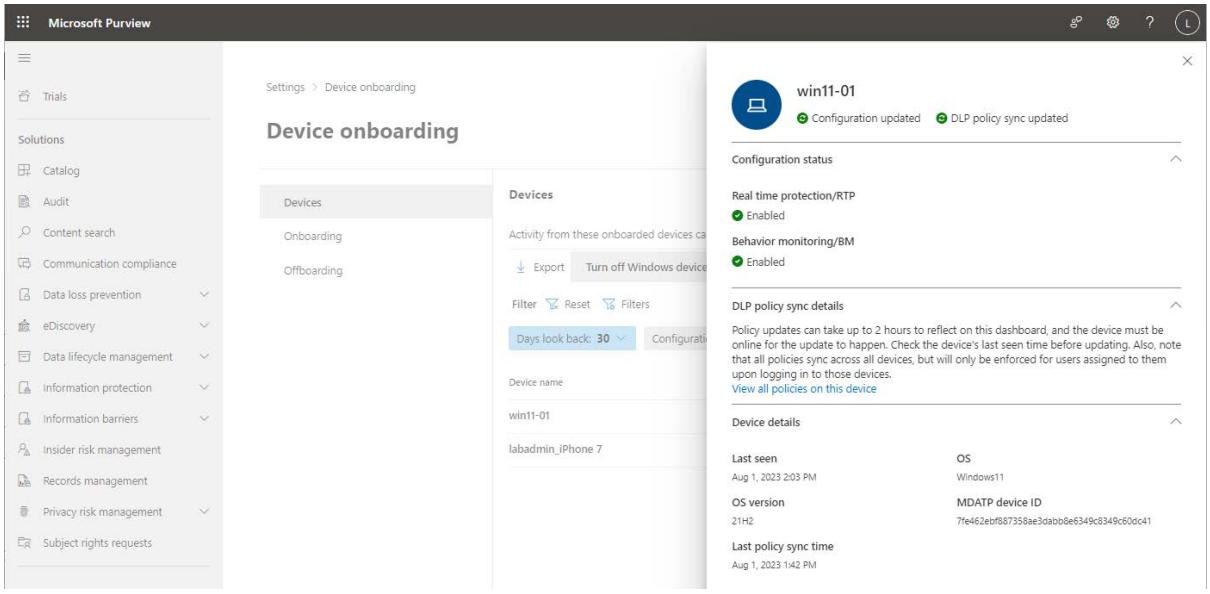

Figure 11.24 – Viewing synchronized DLP policies

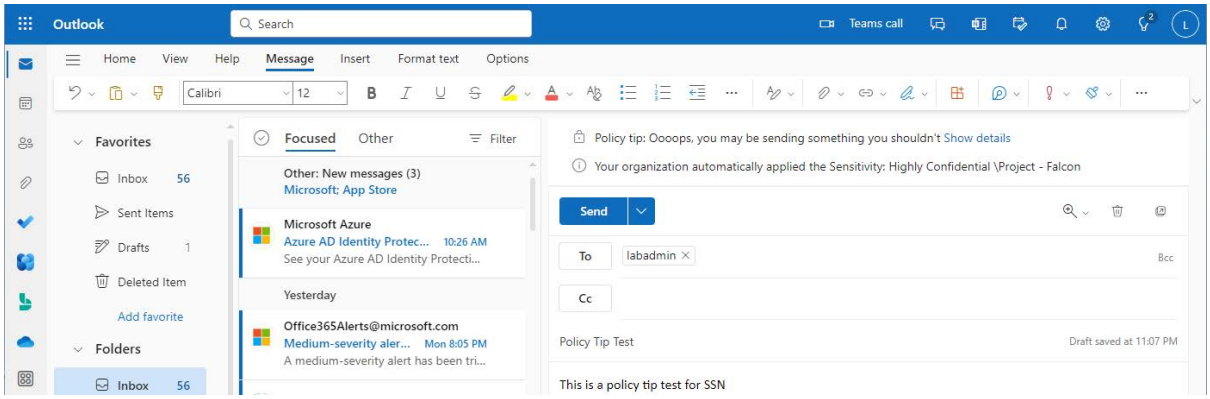

Figure 11.25 – Policy tip test

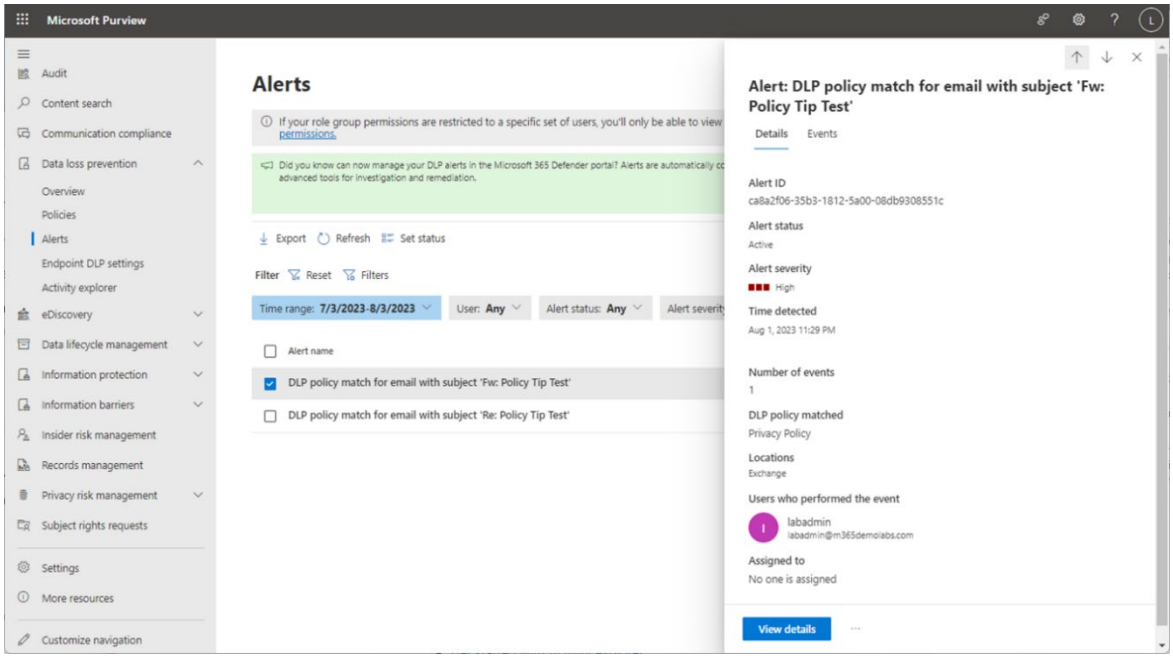

Figure 11.26 – Viewing a DLP alert

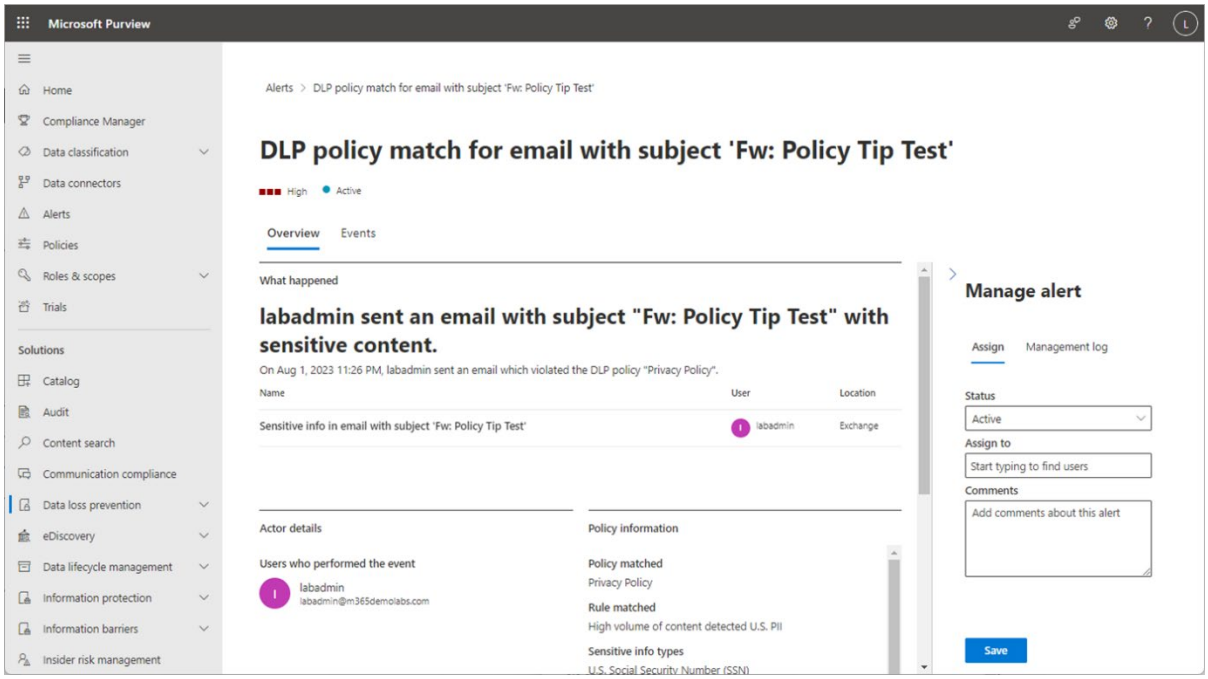

Figure 11.27 – Alert detail page

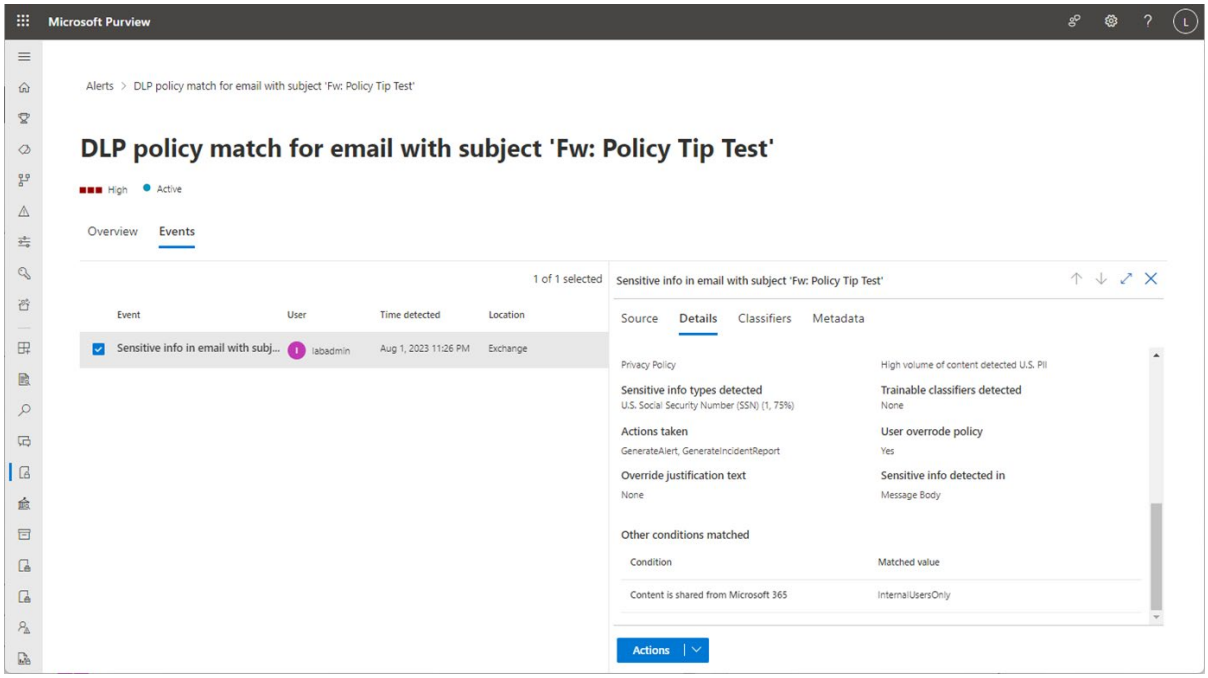

Figure 11.28 – Event detail view of an alert

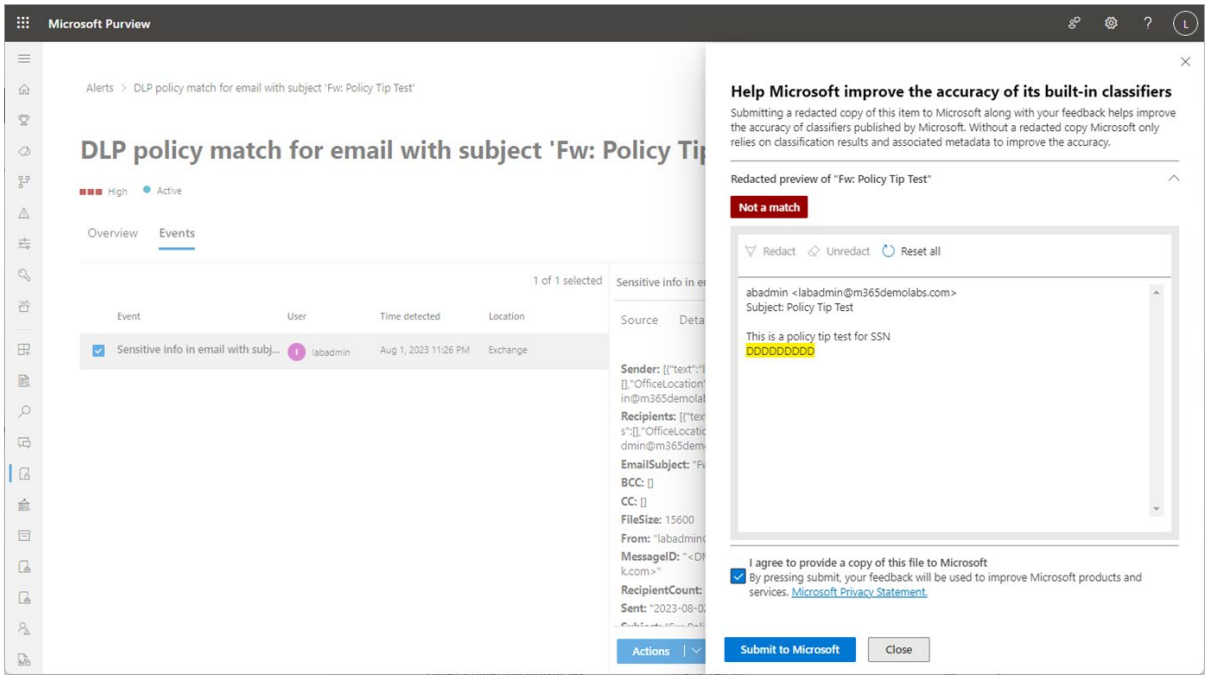

Figure 11.29 – Submitting a redacted false positive sample to Microsoft

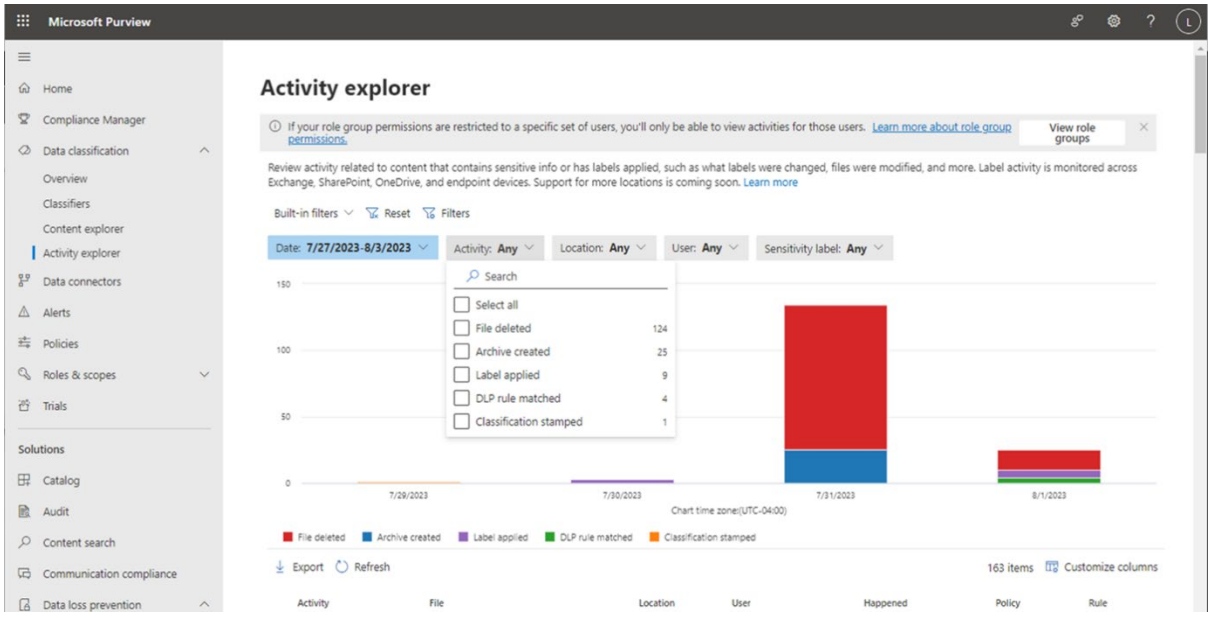

Figure 11.30 – Activity explorer dashboard

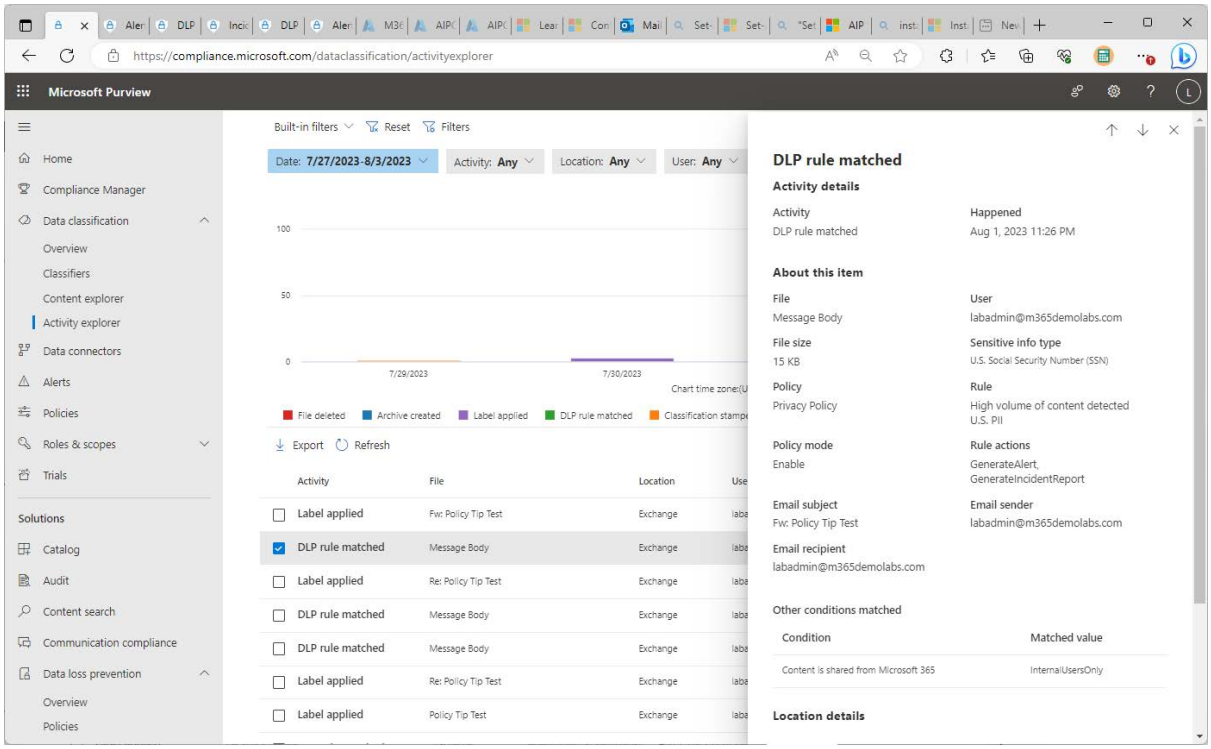

Figure 11.31 – Viewing details of an event in Activity explorer

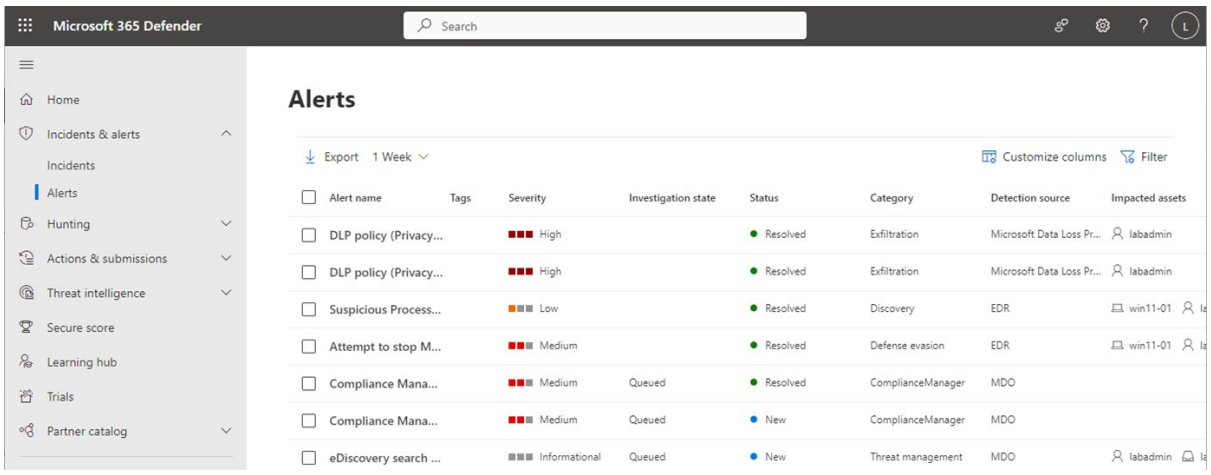

Figure 11.32 – Microsoft 365 Defender Alerts dashboard

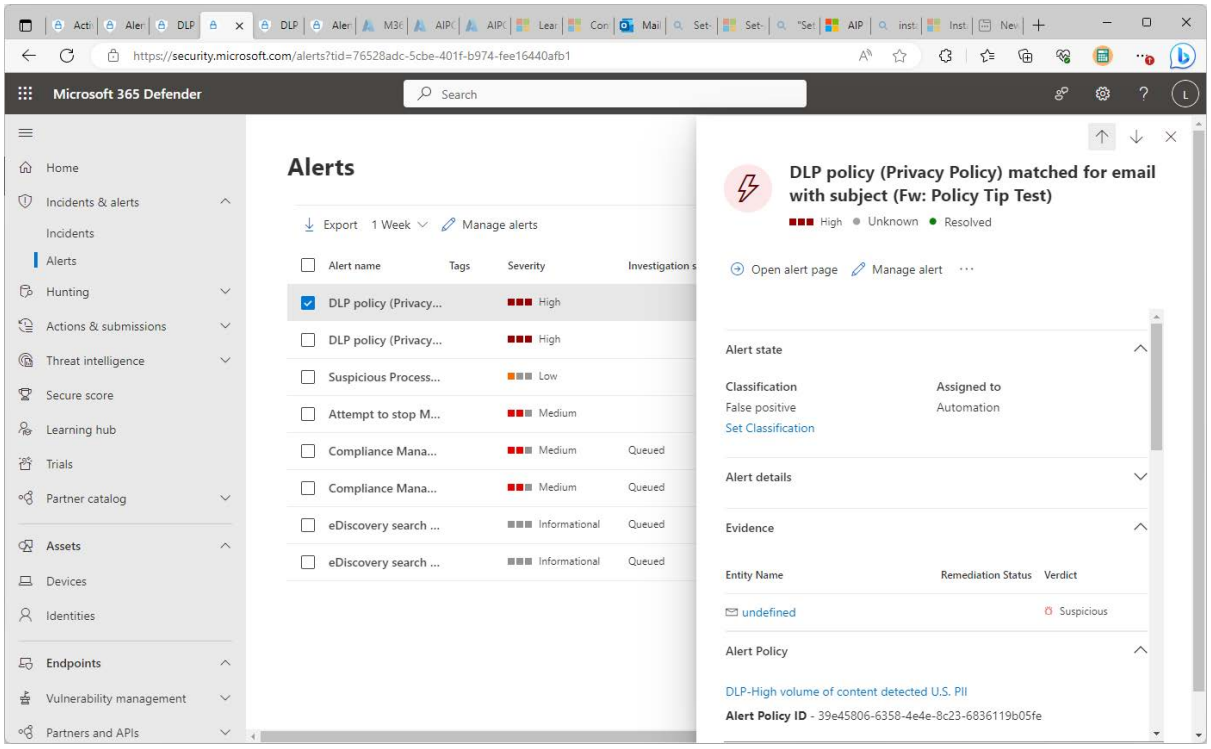

Figure 11.33 – Alert detail flyout

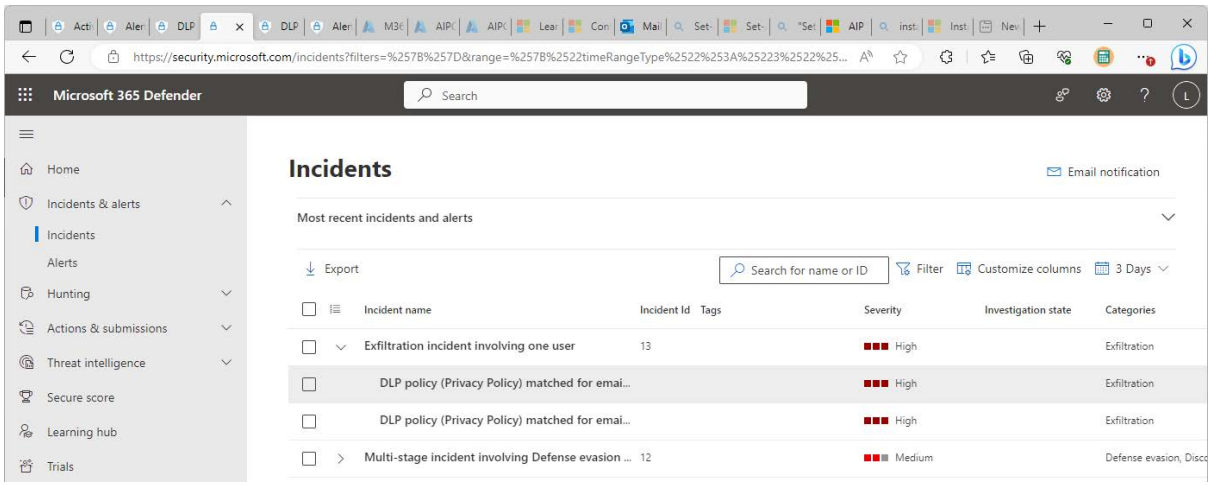

Figure 11.34 – Microsoft 365 Defender Incidents dashboard

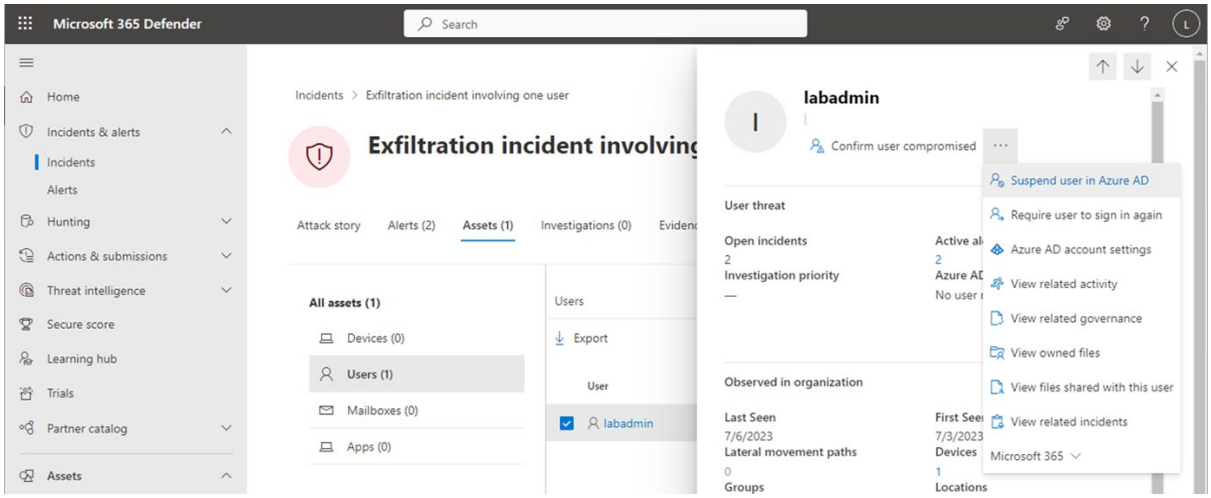

Figure 11.35 – Viewing the user actions in a DLP incident

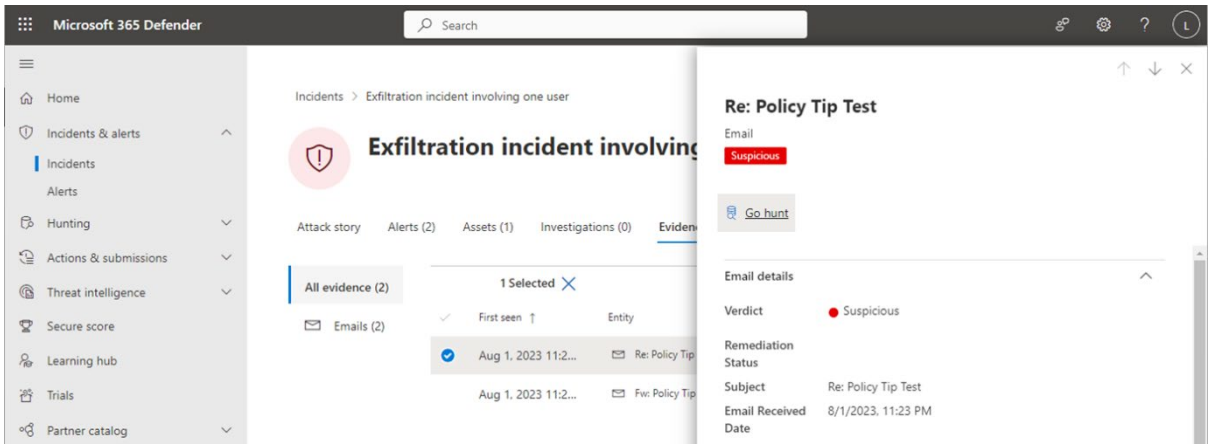

Figure 11.36 – Microsoft 365 Defender incident evidence

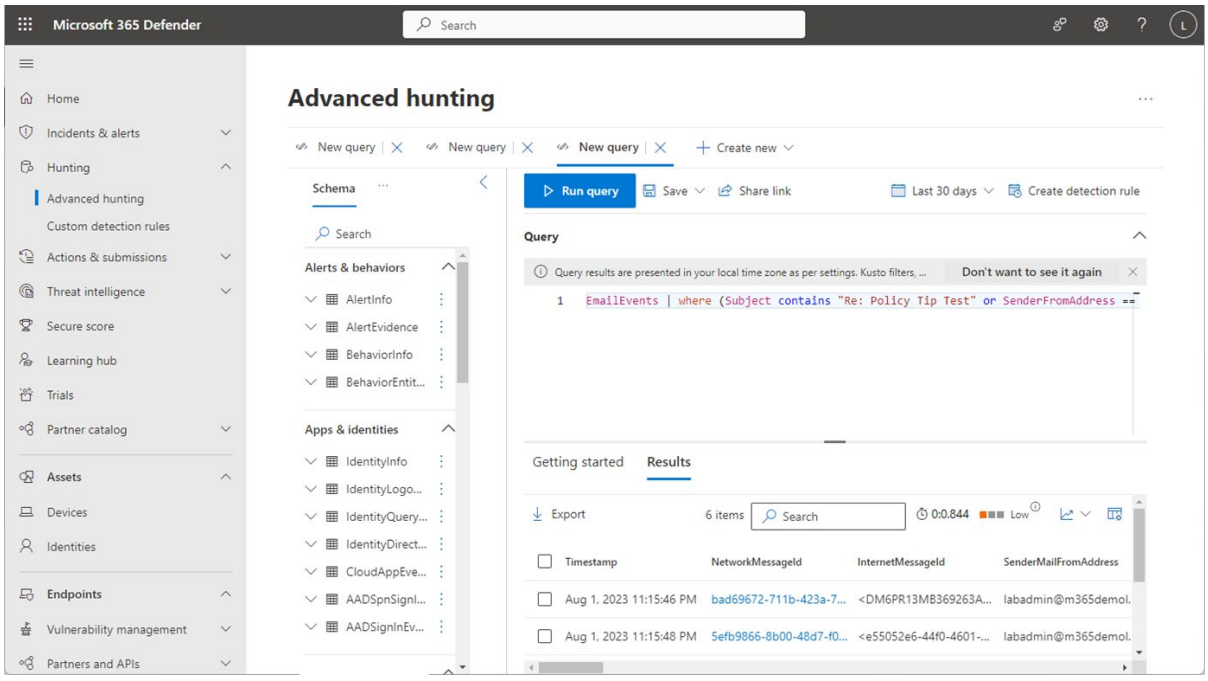

Figure 11.37 – Advanced hunting results

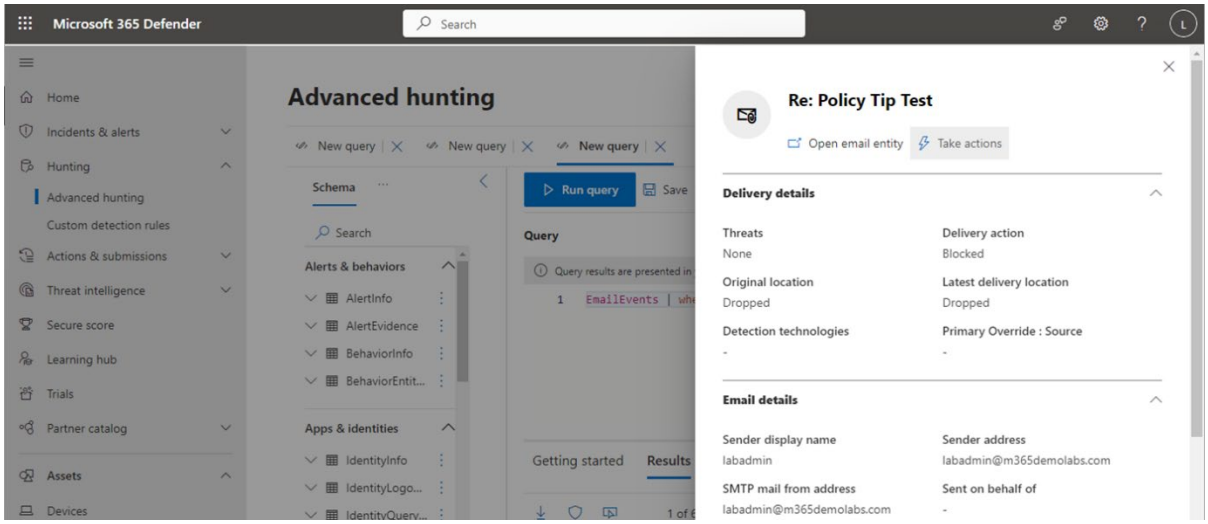

Figure 11.38: Advanced hunting item details

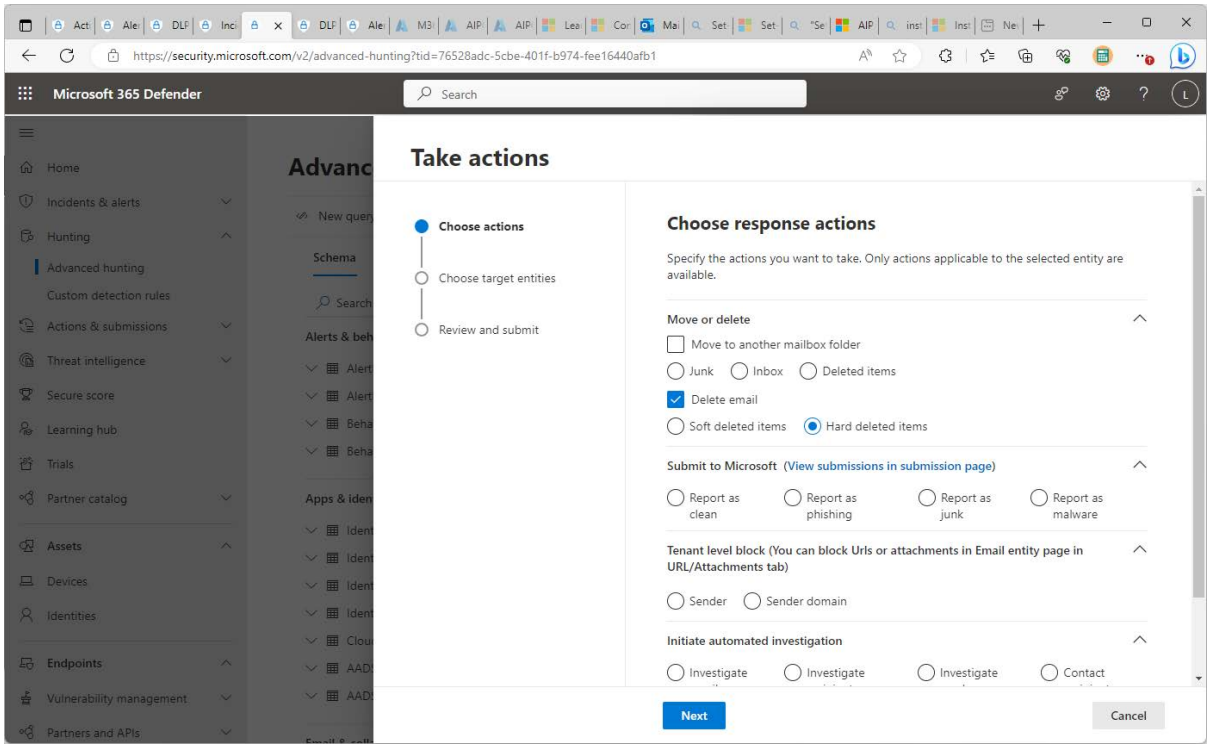

Figure 11.39 – Initiating remediation tasks

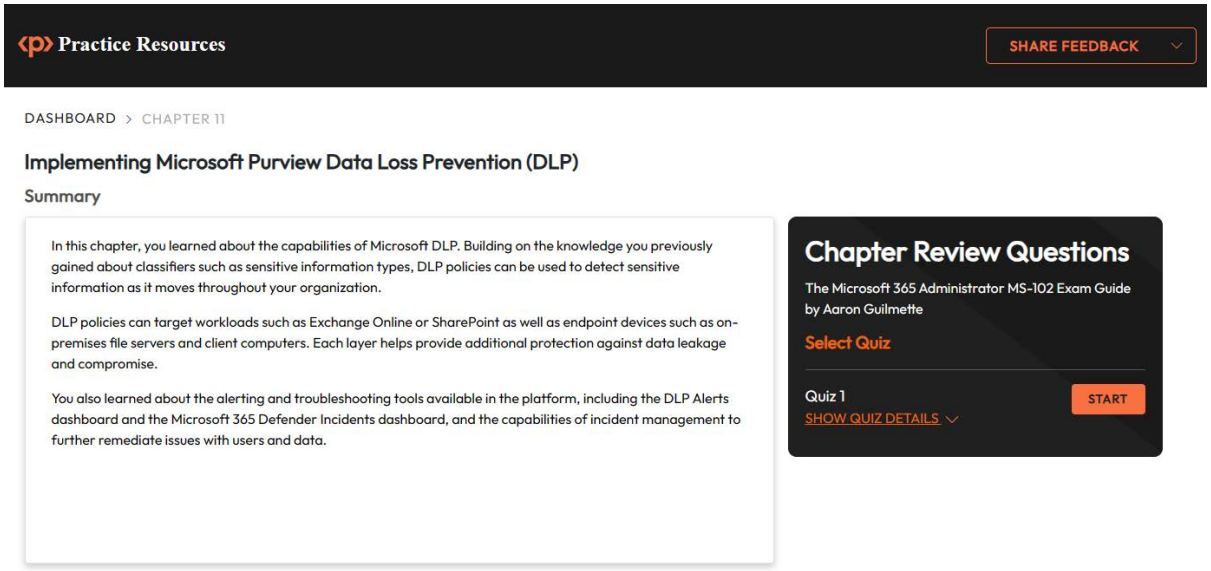

Figure 11.40 – Chapter Review Questions for Chapter 11