

Microsoft Security Operations Analyst

SECOND EDITION

Exam Ref SC-200

Yuri Diogenes
Sarah Young

FREE SAMPLE CHAPTER |



Microsoft

Exam Ref SC-200 Microsoft Security Operations Analyst, Second Edition

Yuri Diogenes and Sarah Young

Exam Ref SC-200 Microsoft Security Operations Analyst, Second Edition

Published with the authorization of Microsoft Corporation by:
Pearson Education, Inc.

Copyright © 2026 by Pearson Education, Inc.

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit *www.pearson.com/global-permission-granting.html*.

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein. Please contact us with concerns about any potential bias at *https://www.pearson.com/report-bias.html*.

ISBN-13: 978-0-13-559078-2
ISBN-10: 0-13-559078-7

Library of Congress Control Number: 2026937251

$PrintCode

TRADEMARKS

Microsoft and the trademarks listed at *http://www.microsoft.com* on the "Trademarks" webpage are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

WARNING AND DISCLAIMER

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author, the publisher, and Microsoft Corporation shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the programs accompanying it.

EDITOR-IN-CHIEF
Julie Phifer

EXECUTIVE EDITOR
Loretta Yates

ACQUISITIONS EDITOR
Shourav Bose

DEVELOPMENT EDITOR
Rick Kughen

MANAGING EDITOR
Sandra Schroeder

SENIOR PROJECT EDITOR
Tracey Croom

COPY EDITOR
Rick Kughen

INDEXER
Brad Herriman

PROOFREADER
Jennifer Hinchliffe

TECHNICAL EDITOR
Javier Soriano

COVER DESIGNER
Twist Creative, Seattle

COMPOSITOR
codeMantra

GRAPHICS
codeMantra

Contents at a glance

	Introduction	*xii*
CHAPTER 1	**Manage a security operations environment**	**1**
CHAPTER 2	**Configure protections and detections**	**83**
CHAPTER 3	**Manage incident response**	**153**
CHAPTER 4	**Manage security threats**	**229**
CHAPTER 5	**SC-200 Microsoft Security Operations Analyst exam updates**	**291**
	Index	*295*

This page intentionally left blank

Contents

Introduction **xii**

Organization of this book *xii*

Preparing for the exam *xii*

Microsoft certifications *xiii*

Access the Exam Updates chapter and online references *xiii*

Errata, updates, & book support *xiv*

Chapter 1 Manage a security operations environment **1**

Skill 1.1: Configure settings in Microsoft Defender XDR 2

Configure alert and vulnerability notification rules 2

Configure Microsoft Defender for Endpoint advanced features 5

Configure endpoint rules settings 8

Manage automated investigation and response capabilities in Microsoft Defender XDR 14

Configure automatic attack disruption in Microsoft Defender XDR 19

Skill 1.2: Manage assets and environments 23

Configure and manage device groups, permissions, and automation levels in Microsoft Defender for Endpoint 23

Identify unmanaged devices in Microsoft Defender for Endpoint 27

Discover unprotected resources by using Defender for Cloud 31

Identify and remediate devices at risk by using Microsoft Defender Vulnerability Management 37

Mitigate risk by using Exposure Management in Microsoft Defender XDR 42

Skill 1.3: Design and configure a Microsoft Sentinel workspace 48

Plan a Microsoft Sentinel workspace 48

Configure Microsoft Sentinel roles 53

Specify Azure RBAC roles for Microsoft Sentinel configuration 55

Design and configure Microsoft Sentinel data storage, including log types and log retention 56

Skill 1.4: Ingest data sources in Microsoft Sentinel 59
Identify data sources to be ingested into Microsoft Sentinel 59
Implement and use Content hub solutions 63
Configure and use Microsoft connectors for Azure resources, including Azure Policy and diagnostic settings 65
Configure bidirectional synchronization between Microsoft Sentinel and Microsoft Defender XDR 68
Plan and configure Syslog and Common Event Format (CEF) event collections 70
Plan and configure the collection of Windows Security events by using data collection rules, including Windows Event Forwarding (WEF) 73
Create custom log tables in the workspace to store ingested data 76
Monitor and optimize data ingestion 79
Thought experiment. 79
Thought experiment answers 80
Chapter summary 81

Chapter 2 Configure protections and detections 83

Skill 2.1: Configure protections in Microsoft Defender security technologies 83
Configure policies for Microsoft Defender for Cloud Apps 84
Configure policies for Microsoft Defender for Office 365 88
Configure security policies for Microsoft Defender for Endpoint, including attack surface reduction (ASR) rules 97
Configure cloud workload protections in Microsoft Defender for Cloud 106
Skill 2.2: Configure detections in Microsoft Defender XDR 110
Configure and manage custom detection rules 110
Manage alerts, including tuning, suppression, and correlation 115
Configure deception rules in Microsoft Defender XDR 118
Skill 2.3: Configure detections in Microsoft Sentinel 122
Classify and analyze data by using entities 123
Configure and manage analytics rules 125

Query Microsoft Sentinel data by using ASIM parsers 135
Implement behavioral analytics 142
Thought experiment . . . 148
Thought experiment answers . . . 149
Chapter summary . . . 150

Chapter 3 Manage incident response 153

Skill 3.1: Respond to alerts and incidents in the Microsoft Defender portal . . . 153
Investigate and remediate threats by using Microsoft Defender for Office 365 154
Investigate and remediate ransomware and business email compromise incidents identified by automatic attack disruption 156
Investigate and remediate compromised entities identified by Microsoft Purview Data Loss Prevention (DLP) policies 158
Investigate and remediate threats identified by Microsoft Purview insider risk policies 161
Investigate and remediate alerts and incidents identified by Microsoft Defender for Cloud workload protections 163
Investigate and remediate security risks identified by Microsoft Defender for Cloud Apps 166
Investigate and remediate compromised identities that are identified by Microsoft Entra ID 168
Investigate and remediate security alerts from Microsoft Defender for Identity 169
Skill 3.2: Respond to alerts and incidents identified by Microsoft Defender for Endpoint . . . 171
Investigate device timelines 172
Perform actions on the device, including live response and collecting investigation packages 174
Perform evidence and entity investigation 177
Skill 3.3: Investigate Microsoft 365 activities . . . 179
Investigate threats by using the unified audit log 180
Investigate threats by using Content Search 181
Investigate threats by using Microsoft Graph activity logs 182

Skill 3.4: Respond to incidents in Microsoft Sentinel 182
Investigate and remediate incidents in Microsoft Sentinel 183
Configure Security Orchestration, Automation, and Response (SOAR) in Microsoft Sentinel 195
Create and configure automation rules 196
Create and configure Microsoft Sentinel playbooks 199
Run playbooks on on-premises resources 204
Skill 3.5: Implement and use Microsoft Security Copilot 207
Create and use promptbooks 207
Manage plugins for Security Copilot 210
Integrate Security Copilot by implementing connectors 211
Manage permissions and roles in Security Copilot 214
Monitor Security Copilot capacity and cost 216
Identify threats and risks by using Security Copilot 218
Investigate incidents by using Security Copilot 222
Thought experiment 225
Thought experiment answers 226
Chapter summary 226

Chapter 4 Manage security threats 229

Skill 4.1: Hunt for threats by using Microsoft Defender XDR 229
Interpret threat analytics in the Microsoft Defender portal 235
Create custom hunting queries by using KQL 239
Skill 4.2: Hunt for threats by using Microsoft Sentinel 242
Analyze attack vector coverage by using the MITRE ATT&CK matrix 242
Manage and use threat indicators 244
Create and manage hunts 251
Create and monitor hunting queries 253
Use hunting bookmarks for data investigations 261
Retrieve and manage archived log data 275
Create and manage search jobs 277

Skill 4.3: Create and configure Microsoft Sentinel workbooks 279
Activate and customize Microsoft Sentinel workbook templates 279
Create custom workbooks that include KQL 282
Configure visualizations 286
Thought experiment 288
Thought experiment answers 288
Chapter summary 289

Chapter 5 SC-200 Microsoft Security Operations Analyst exam updates 291

The purpose of this chapter 291
About possible exam updates 291
Impact on you and your study plan 292
Exam objective updates 292
Updated technical content 292
Objective mapping 292

Index *295*

Acknowledgments

The authors would like to thank Loretta Yates and the entire Microsoft Press/Pearson team for their support in this project, and Javier Soriano for reviewing the book.

Yuri would also like to thank: my wife and daughters for their endless support; my great God for giving me strength and guiding my path on each step of the way; my great friend and co-author, Sarah Young, for this amazing partnership. I dedicate this book to my mother, who passed away in September 2025. Thank you for giving me my education and your unconditional love.

Sarah would like to thank: Grayson and Minako, who drive me to do better so I can fund their expensive lifestyle; my amazing co-author and friend Yuri for being a role model and advocate for so many. I'd also like to thank my Microsoft colleagues who have championed me, supported me, and given me a shoulder to cry on when needed: there are many, but in particular Ryan, Hilary, Orin, Macca, Matt, Michael, Mark, Jen, Seth, and Joey. My most special thanks are saved for my parents, who gave so much for my education, taught me the value of hard work and integrity, and continue to support me in every way possible.

About the authors

YURI DIOGENES has a PhD in cybersecurity leadership and a Master of Science in cybersecurity intelligence and forensics investigation. Yuri has been working at Microsoft since 2006, and currently he is a Principal PM Manager at Microsoft CxE, where he manages the Defender for Cloud and Azure Network Security Teams. Yuri is also a Professor at the University of Texas at Dallas, Trine University, and EC-Council University. Yuri has published more than 30 books, mostly around information security and Microsoft technologies. Yuri also holds an MBA and many IT/Security industry certifications, such as CISSP, E|CND, E|CEH, E|CSA, E|CHFI, E|CTI, CompTIA Security+, CySA+, CASP, and MITRE ATT&CK Cyber Threat Intelligence. You can follow Yuri on X at *@yuridiogenes* and watch his Defender for Cloud in the Field show at *aka.ms/MDCInTheField*.

SARAH YOUNG is the Director of Security for the Microsoft Innovation Hub. Having worked with Microsoft Security products for a good portion of her security career, Sarah has extensive knowledge of the platform and has helped it develop and grow in various roles at Microsoft over the years. Sarah is an experienced public speaker and has presented on a range of IT security and technology topics at global industry events and holds numerous IT security qualifications (some expired, some still going!). She is an active supporter of security and cloud native communities around the world and is a co-host of the Microsoft Azure Security Podcast. You can follow Sarah on the socials *@_sarahyo* and listen to her podcast at *aka.ms/azsecpod*.

Introduction

The SC-200 exam deals with technologies that are relevant to Microsoft Security Operations Analysts who collaborate with organizational stakeholders to secure information technology systems for the organizations. This exam covers topics that will help to reduce organizational risk by rapidly remediating active attacks in the environment, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders. The exam also covers topics such as investigation and response to threats using Microsoft Sentinel, Security Copilot, Microsoft Defender XDR, and third-party security products.

This book covers every major topic area found on the exam, but it does not cover every exam question. Only the Microsoft exam team has access to the exam questions, and Microsoft regularly adds new questions to the exam, making it impossible to cover specific questions.

You should consider this book a supplement to your relevant real-world experience and other study materials. If you encounter a topic in this book that you do not feel completely comfortable with, use the Need More Review links, which provide additional information. Great information is available on *docs.microsoft.com*, at MS Learn, and in blogs and forums.

Organization of this book

This book is organized by the "Skills measured" list published for the exam. The "Skills measured" list is available for each exam on the Microsoft Learning website: *microsoft.com/learn*. Each chapter in this book corresponds to a major topic area in the list, and the technical tasks in each topic area determine a chapter's organization. If an exam covers six major topic areas, for example, the book will contain six chapters.

Preparing for the exam

Microsoft certification exams are a great way to build your résumé and let the world know about your level of expertise. Certification exams validate your on-the-job experience and product knowledge. Although there is no substitute for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam. This book is not designed to teach you new skills.

We recommend that you augment your exam preparation plan by using a combination of available study materials and courses. For example, you might use this *Exam Ref* and another study guide for your "at home" preparation and take a Microsoft Official Curriculum course for

the classroom experience. Choose the combination that you think works best for you. Learn more about available classroom training and find free online courses and live events at *microsoft.com/learn*.

Note that this *Exam Ref* is based on publicly available information about the exam and the author's experience. To safeguard the integrity of the exam, authors do not have access to the live exam.

Microsoft certifications

Microsoft certifications distinguish you by proving your command of a broad set of skills and experience with current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies, both on-premises and in the cloud. Certification brings a variety of benefits to the individual and to employers and organizations.

MORE INFO **ALL MICROSOFT CERTIFICATIONS**

For information about Microsoft certifications, including a full list of available certifications, go to *microsoft.com/learn*.

Access the Exam Updates chapter and online references

The final chapter of this book, "SC-200 Microsoft Security Operations Analyst exam updates," will be used to provide information about new content per new exam topics, content that has been removed from the exam objectives, and revised mapping of exam objectives to chapter content. The chapter will be made available from the link below as exam updates are released.

Throughout this book are addresses to webpages that the author has recommended you visit for more information. Some of these links can be very long and painstaking to type, so we've shortened them for you to make them easier to visit. We've also compiled them into a single list that readers of the print edition can refer to while they read.

The URLs are organized by chapter and heading. Every time you come across a URL in the book, find the hyperlink in the list to go directly to the webpage.

Download the Exam Updates chapter and the URL list at *MicrosoftPressStore.com/ERSC2002e/downloads*

Errata, updates, & book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

MicrosoftPressStore.com/ERSC2002e/errata

If you discover an error that is not already listed, please submit it to us on the same page.

If you need additional support, email Microsoft Press Book Support at *MicrosoftPressStore.com/Support*.

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to *support.microsoft.com*.

CHAPTER 2

Configure protections and detections

One critical component of any Security Operations Center (SOC) is the quality of the alert that is received from a given data source. The quality of the alert can be measured by the relevance of the information contained in the alert, how that alert reflects the threat vectors of a cloud workload, and how these indications can help Security Operations Analysts investigate and respond to that alert. The products within the Defender security technologies provide tailored threat detection that can empower the SOC to have more accurate and relevant information to perform investigations. These alerts are also streamed to Microsoft Defender XDR and Microsoft Sentinel, which will enhance SOC Analysts' experience by bringing all these insights together in a single dashboard.

Skills covered in this chapter:

- Configure protections in Microsoft Defender security technologies
- Configure detections in Microsoft Defender XDR
- Configure detections in Microsoft Sentinel

Skill 2.1: Configure protections in Microsoft Defender security technologies

Before the SOC consumes the alert, the posture management team needs to ensure that protection is in place to reduce the likelihood of potential compromise. This means improving the security posture by implementing policies that enhance the workload's protection. This section of the chapter covers the skills necessary to configure protections in Microsoft Defender security technologies according to the Exam SC-200 outline.

This skill covers:

- Configure policies for Microsoft Defender for Cloud Apps
- Configure policies for Microsoft Defender for Office 365
- Configure security policies for Microsoft Defender for Endpoints, including attack surface reduction (ASR) rules
- Configure cloud workload protections in Microsoft Defender for Cloud

Configure policies for Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud Apps (formerly Microsoft Cloud App Security) is a Cloud Access Security Broker (CASB) solution that helps organizations enhance visibility, manage security, and enforce compliance across their cloud environments. It integrates seamlessly with other Microsoft Security solutions and provides deep insights into cloud app usage while protecting sensitive data.

In Microsoft Defender for Cloud Apps, app policies can be used to establish guidelines for user behavior in the cloud, helping you identify risky actions, policy violations, or unusual activities within your cloud environment. These policies can also incorporate remediation workflows to facilitate comprehensive risk mitigation when needed. Various policy types are available, tailored to the specific information you want to monitor in your cloud environment, and the remediation measures you may need to implement. Table 2-1 describes the different types of policies.

TABLE 2-1 Policy type and use case scenario

Activity policy	Threat detection	Enables you to implement a variety of automated processes by leveraging the app provider's APIs. These policies allow you to track specific user activities or monitor unusually high occurrences of particular types of actions.
Anomaly detection policy	Threat detection	Helps identify unusual activities within your cloud environment. These policies use the risk factors you define to notify you of actions that deviate from your organization's baseline or a user's typical behavior.
OAuth app policy	Threat detection	Allows you to review the permissions requested by each OAuth application and automatically approve or revoke them. These are preconfigured policies included with Defender for Cloud Apps and cannot be manually created.
Malware detection policy	Threat detection	Helps detect malicious files stored in your cloud environment and allows for their automatic approval or revocation. This is a preconfigured policy included with Defender for Cloud Apps and cannot be manually created.
File policy	Information protection	Allows you to scan your cloud applications for specific files or file types (such as those shared or shared with external domains) and detect various types of data, including proprietary information, personal data, credit card details, and more. These policies also enable you to apply governance actions, which vary depending on the specific cloud application.
Access policy	Conditional Access	Leverages Conditional Access app control to offer real-time oversight and management of access to cloud applications. These policies regulate access based on factors such as user identity, location, device, and application, and they are compatible with any device.
Session policy	Conditional Access	Provides detailed visibility into cloud applications through real-time, session-level monitoring. These policies enable you to define actions based on the conditions of a user session. Unlike access policies, which fully grant or deny access, session policies permit access while actively monitoring the session. By integrating the Conditional Access app control, you can restrict specific activities during the session.
App discovery policy	Shadow IT	Enables you to have visibility and receive an alert when new apps are detected.

After identifying the type of policy you want to create, you can go to the same Microsoft Defender XDR portal to configure policies in Microsoft Defender for Cloud Apps. You can either create a policy from a template or a query. Follow the steps below to create a policy from a template:

1. Sign in to *https://security.microsoft.com*.
2. In the left navigation pane, click **Cloud apps** > **Policies** > **Policy templates**. The **Policy templates** page appears, as shown in Figure 2-1.

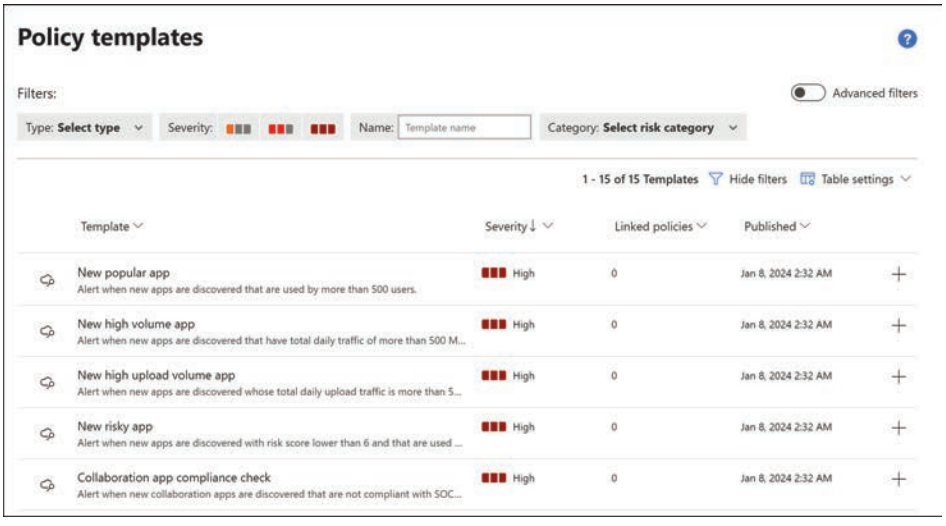


FIGURE 2-1 Policy templates page

3. This page lists all the templates available, the default severity level of the policy, whether the template is already linked to an existing policy, and the last time that was published. To create a policy based on one of those templates, click the plus sign (**+**) next to the template. For this example, click the plus sign (**+**) next to the **New popular app** template; the **Create app discovery policy** page appears. The first part of this page is shown in Figure 2-2.
4. As you can see, the policy template dropdown is automatically populated with the template that was selected. In the **Policy name** field, type the name for this policy. Under **Policy severity**, you can either leave the default selection, which is high severity, or you can change to medium or low. The **Category** field is also automatically populated since it inherits from the template. In the **Description** field, type more information about this policy and its purpose.
5. The second part of this page, shown in Figure 2-3, has the matching variables for this app.

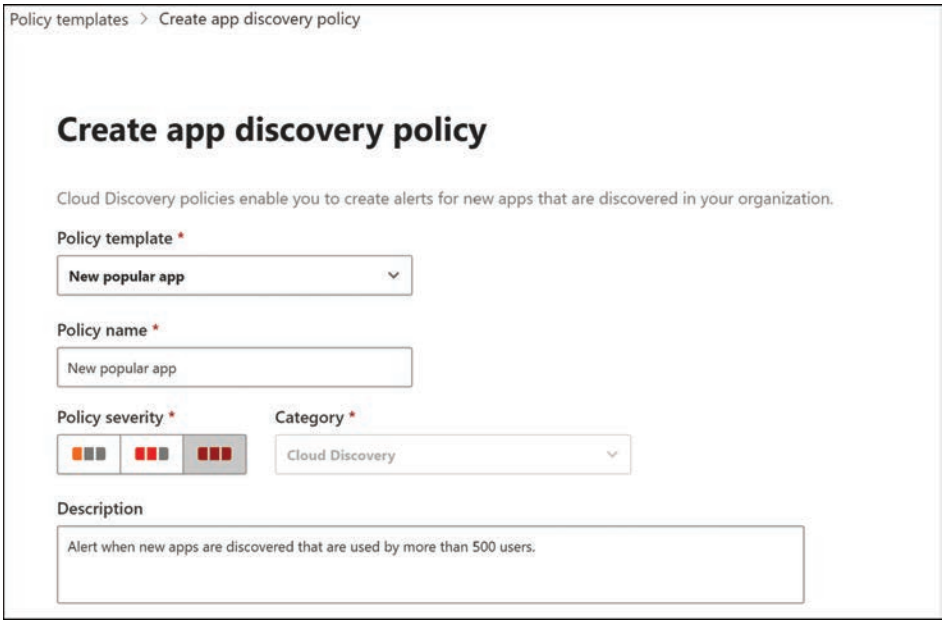


FIGURE 2-2 Create app discovery policy page

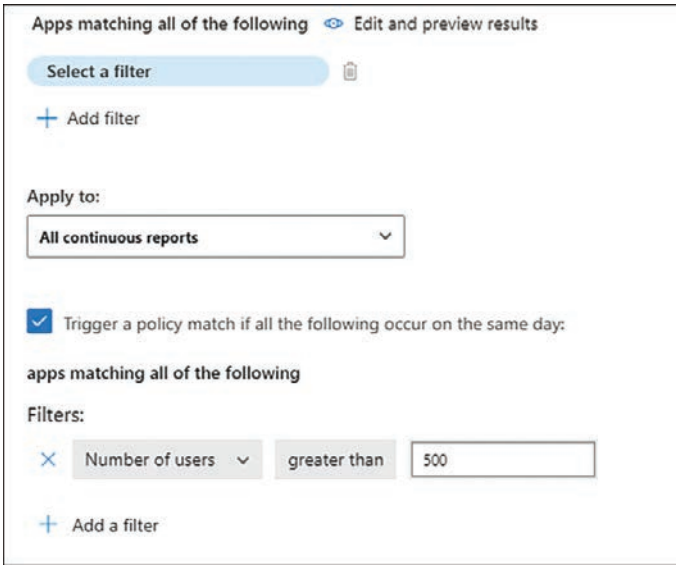


FIGURE 2-3 Matching criteria for the apps

6. Under the first **Select a filter** dropdown, you can select the first criterion that the app needs to match. For example, you can select **Apps and domains** and type the domain name, as shown in Figure 2-4.



FIGURE 2-4 Matching criteria for the apps

7. By default, the second criterion for this template is already set up for the **Number of users**, but you could add a filter for daily traffic, downloaded data, the number of IP addresses, the number of transactions, the number of users, and uploaded data.
8. The last part of the page, shown in Figure 2-5, has the alert and governance settings.

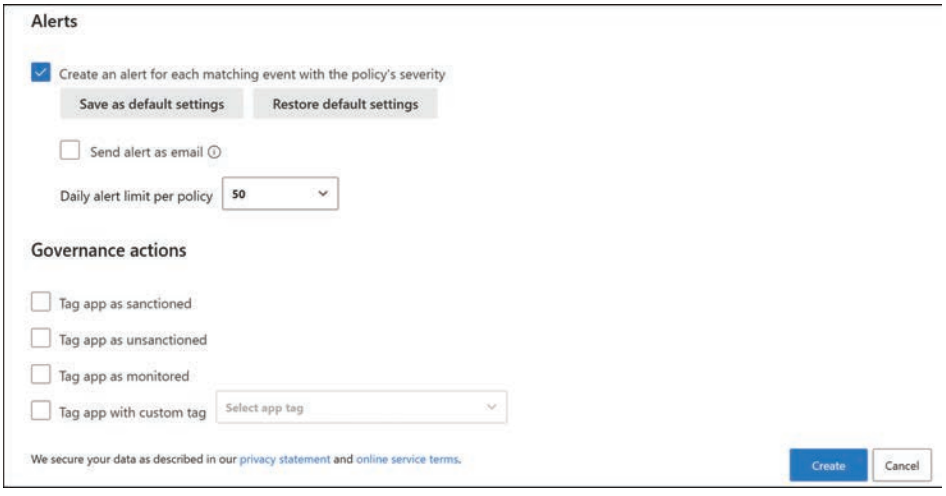


FIGURE 2-5 Alert and governance settings

9. By default, this template already has the checkbox to create an alert for each matching selected. Optionally, you can also select the **Send alert as email** checkbox and specify an email address to which you want an alert to be sent. Lastly, you have the **Daily alert limit per policy**, which, for this template, is configured to **50** alerts.
10. The **Governance actions** section has the tags that you may want to enable for the apps. Keep in mind that unsanctioned apps will not be blocked. You can also create a custom tag if necessary. When you are finished making selections, click the **Create** button. The policy will appear on the **Policies** page, as shown in Figure 2-6.
11. Notice that the **Count** shown in Figure 2-6 appears as **Loading**, which means that it is still matching the variables that were established in the policy creation with the apps available in the environment. Also, notice that there are two tabs, **Shadow IT** and **All policies**. That's because this policy that you just created is part of the **Shadow IT** category (see all categories in Table 2-1). Once you create policies that are part of other categories, you will see more tabs on this page.

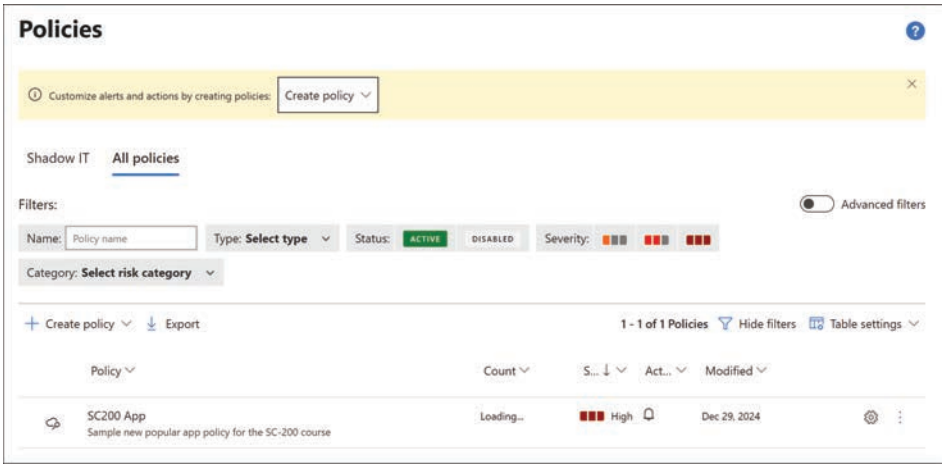


FIGURE 2-6 Policies page

MORE INFO **OTHER POLICIES**

While the main steps to create policies are the same, each policy has different variables. Use the table in this article as an index to navigate to the pages for each category: *https://learn.microsoft.com/en-us/defender-cloud-apps/control-cloud-apps-with-policies*.

Configure policies for Microsoft Defender for Office 365

Microsoft Defender for Office 365 provides various policy types to help organizations protect against threats, enforce compliance, and manage security for email and collaboration tools. While Microsoft 365 subscriptions include built-in security and protection features, different plans will provide different sets of features. The plans are as follows:

- **Exchange Online Protection (EOP)** This plan is included in all subscriptions that have an Exchange Online mailbox but is also available as a stand-alone plan for on-premises email servers.
- **Defender for Office 365 Plan 1** This plan focuses on small and medium-sized businesses, with a focus on protection for email and collaboration. Include features from zero-day malware, phishing, and business email compromise.
- **Defender for Office 365 Plan 2** This is the enterprise-level plan that has everything that Plan 1 has, plus phishing simulations, post-breach investigation, hunting/response, and automation.

Once you determine the plan that best fits your organization's needs, you can start thinking about the configuration policies that you want to apply to your users. Policies are categorized to address specific security needs. There are three basic types of protection policies:

- **Default policies** These policies are automatically implemented when the organization is set up. They apply to all recipients within the organization and cannot be disabled or adjusted for specific users. However, you can modify the security settings within these policies in the same way you would for custom policies.
- **Preset security policies** This type of policy offers an easy way to apply recommended spam, malware, and phishing policies to all users within your organization. As Microsoft introduces new threat protection features, your organization will automatically update to reflect the latest recommended settings. It ensures that your organization remains aligned with evolving recommendations as the threat landscape changes, reducing the effort needed to manage security policies.
- **Custom policies** Enables you to customize the policies to fit your environment better.

Within these types of protection policies, you have individual policies that are either native to Exchange Online Protection (EOP) or Defender for Office 365 (MDO) policies. The list of policies is shown in Table 2-2.

TABLE 2-2 Policy name and category

Policy name*	Policy Category		
	Default	Preset	Custom
Anti-malware [EOL]	X	X	X
Anti-spam [EOL]	X	X	X
Anti-phishing/spoofing protection [EOL]	X	X	X
Outbound spam [EOL]	X		X
Connection filtering [EOL]	X		
Anti-phishing (spoofing protection) plus Impersonation protection and Advanced phishing thresholds [MDO]	X	X	X
Safe links [MDO]	Partially**	X	X
Safe attachments [MDO]	Partially**	X	X

* Since Microsoft is dynamically adding more policies, make sure to visit the following page for the latest set of policies: *https://learn.microsoft.com/en-us/defender-office-365/eop-about#features-in-the-default-email-protections-for-cloud-mailboxes*.

** Even though there are no default Safe Attachments or Safe Links policies in Defender for Office 365, the built-in protection has Safe Attachments and Safe Links protection enabled by default.

MORE INFO **ORDER OF PRECEDENCE**

When configuring security settings for users, it is crucial to consider how protection policies are implemented. To learn more details about the precedence order, visit *https://learn.microsoft.com/en-us/defender-office-365/how-policies-and-protections-are-combined*.

To configure preset security policies in Microsoft Defender for Office 365, you need to be a member of the **Organization Management** or **Security Administrator** role groups. You can also leverage Microsoft Defender XDR Unified role-based access control (RBAC) and grant **Core Security settings (manage)** or **Authorization and Settings** (**Security Settings** > **Core Security Settings (Read)**). Once you grant the proper permissions, follow the steps below to configure the preset security policies:

1. Sign in to *https://security.microsoft.com*.
2. In the left navigation pane, click **Email & collaboration**, click the **Policies & rules** option; the **Policies & rules** page appears, as shown in Figure 2-7.



FIGURE 2-7 Policies & rules page

3. Click **Threat policies**; the **Threat policies** page appears, as shown in Figure 2-8.
4. This page has three major sections:
   - **Template policies** Provides ready-to-use, prebuilt templates that serve as starting points for creating your own policies. These templates encapsulate Microsoft's recommended filters and logic for common scenarios, so you don't need to build policies from scratch.
   - **Policies** Lists all the active policies currently in use in your tenant—whether created from templates, manually built, or automatically generated. This is your operational view of enforcement and monitoring logic.
   - **Rules** Defines fine-grained conditions and response logic that can be reused across multiple policies or govern how policies behave—essentially automated response and correlation logic within Defender for Cloud Apps.

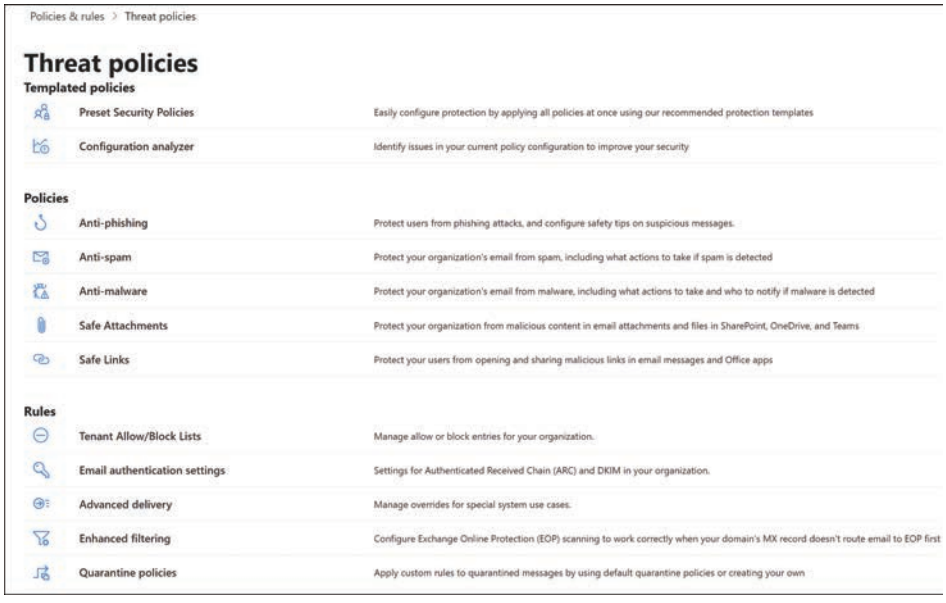


FIGURE 2-8 Threat policies page

5. Under **Templated policies**, click **Preset Security Policies**; the **Preset security policies** page appears, as shown in Figure 2-9.

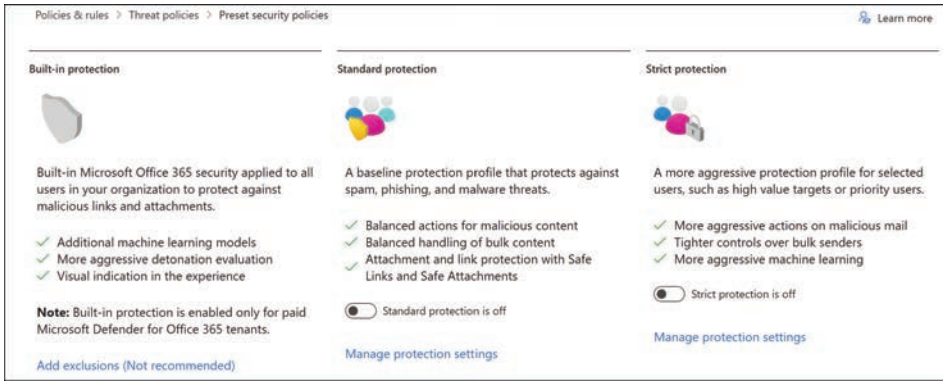


FIGURE 2-9 Preset security policies options

6. Three options are summarized on this page. For this example, click **Manage protection settings** in the **Standard protection** column. The **Apply standard protection** wizard appears with the **Apply Exchange Online Protection** page selected, as shown in Figure 2-10.
7. Click the **All recipients** option to ensure that all recipients are protected with EOP capabilities, and then click the **Next** button. The **Defender for Office 365 protection** page appears, as shown in Figure 2-11.

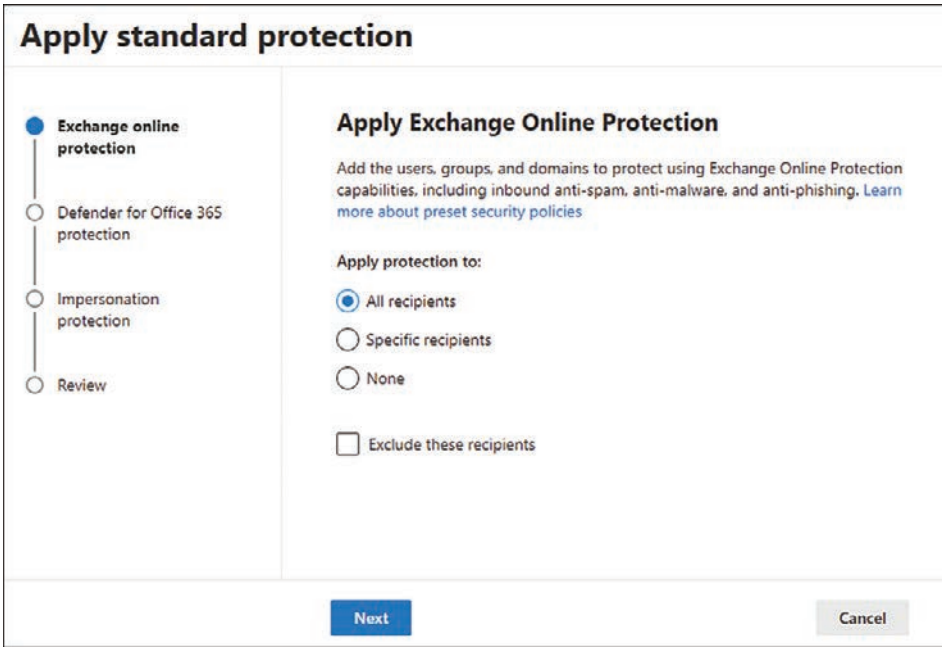


FIGURE 2-10 Apply standard protection page

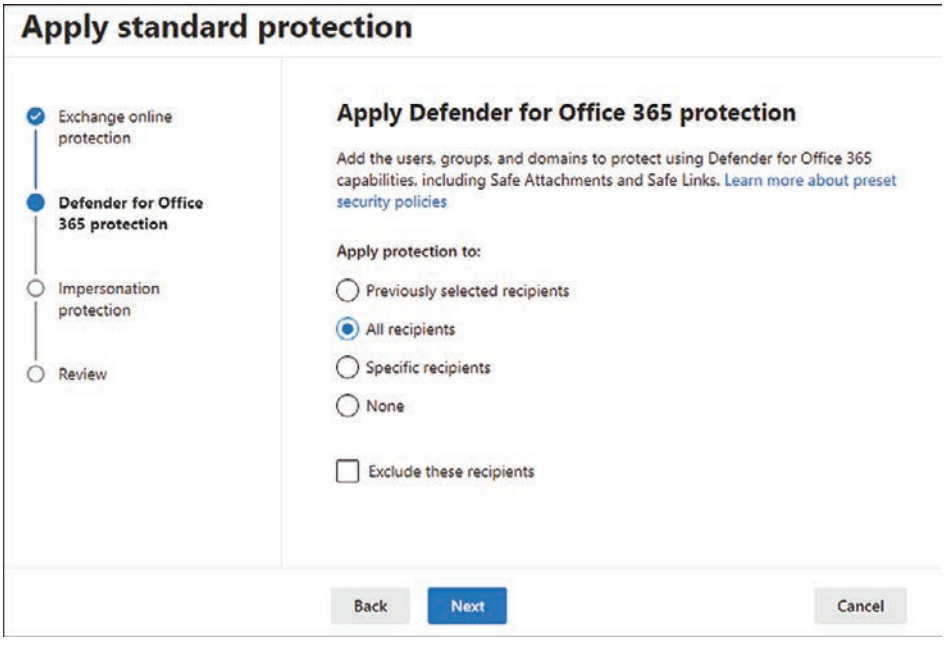


FIGURE 2-11 Apply Defender for Office 365 protection page

8. Click the **All recipients** option and click the **Next** button; the **Impersonation protection** page appears, as shown in Figure 2-12.

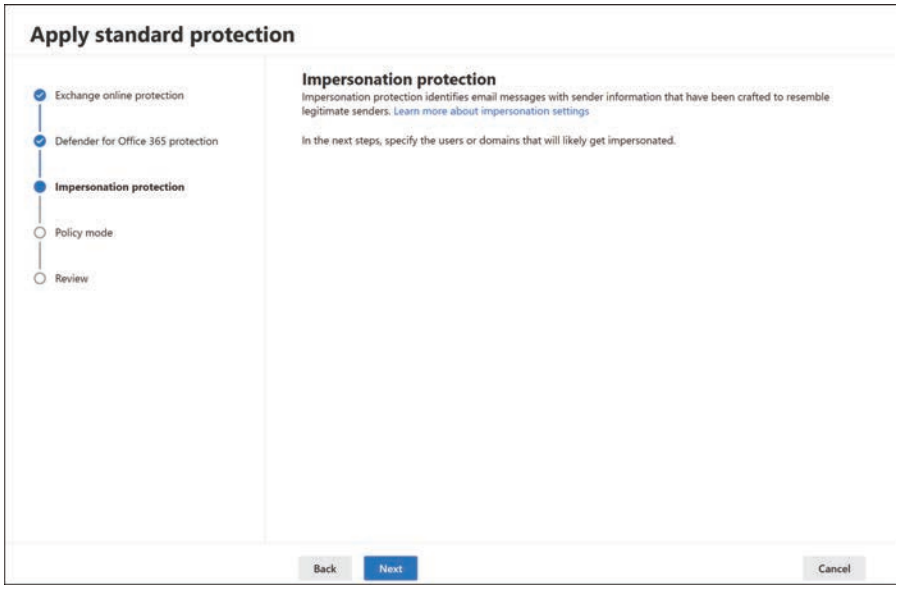


FIGURE 2-12 Impersonation protection page

9. The goal of this feature is to detect where the sender or the sender's email domain in a message looks like a real one. For example, *ćóntoso.com* (notice the accents) could be an impersonation of the *contoso.com* domain. Click the **Next** button; the **Add email addresses to flag when impersonated by attackers** subpage appears, as shown in Figure 2-13.

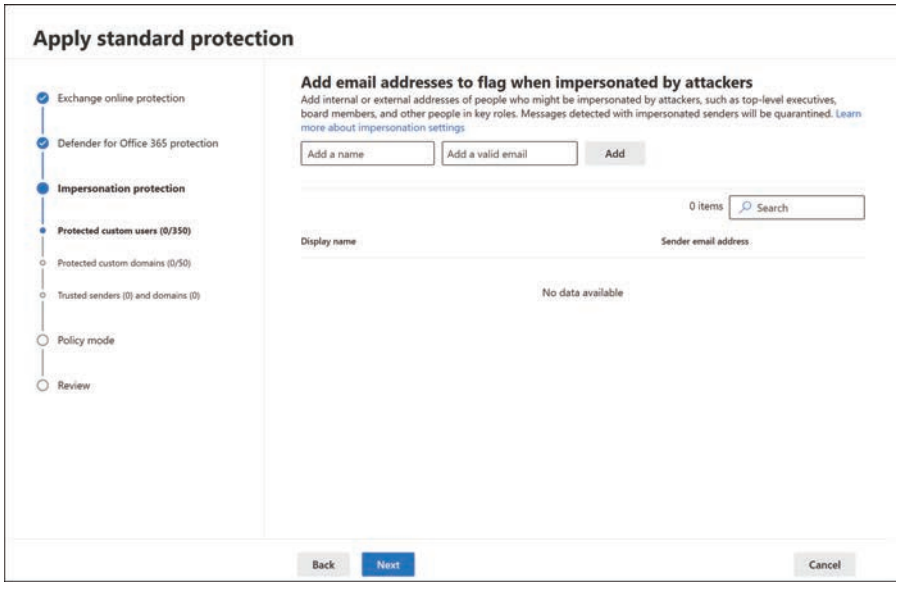


FIGURE 2-13 Customizing the email address to flag for impersonation

10. If you have specific users that you want to ensure will be flagged for potential impersonation, you should add their names in the **Add a name** field, add their email addresses in the **Add a valid email** field, and click the **Add** button. When you are finished adding email addresses, click **Next**. (If you don't have any email addresses to add, just click the **Next** button.) The **Add domains to flag when impersonated by attackers** subpage appears, as shown in Figure 2-14.

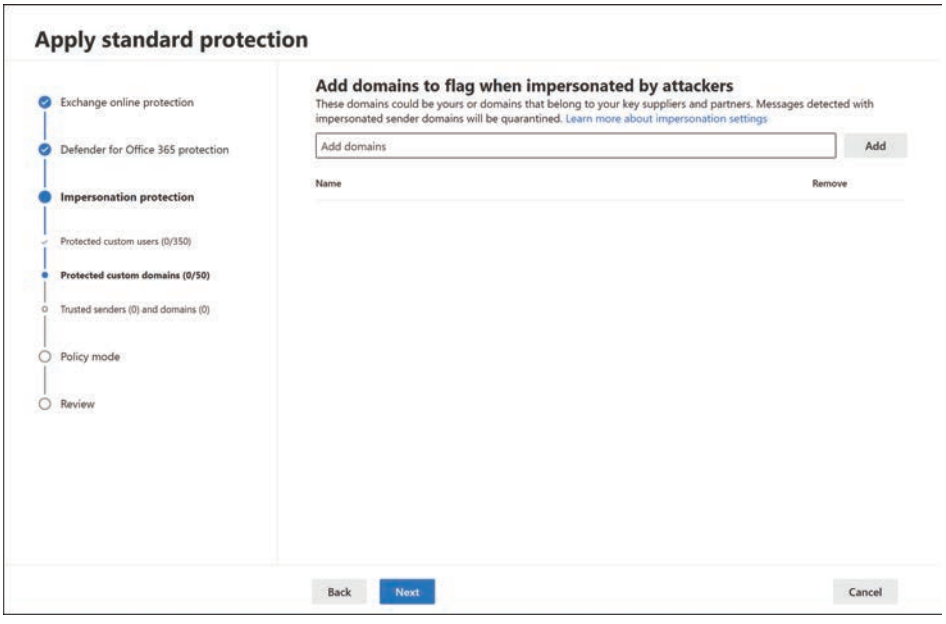


FIGURE 2-14 Customizing the email address to flag for impersonation

11. On this page, you can add the domains that belong to your organization in the **Add domains** field and click the **Add** button. Although this is an optional step, it is recommended that you add at least the domains that your organization owns. After you are done adding domains, click the **Next** button. The **Add trusted email addresses and domains to not flag as impersonation** page appears, as shown in Figure 2-15.
12. If you are certain of users or domains you trust to be exempt from being flagged as impersonation, you can add them to this list. Type the email address or domain in the **Add domains** field and click the **Add** button. Click **Next**; the **Review and confirm your changes** page appears, as shown in Figure 2-16.

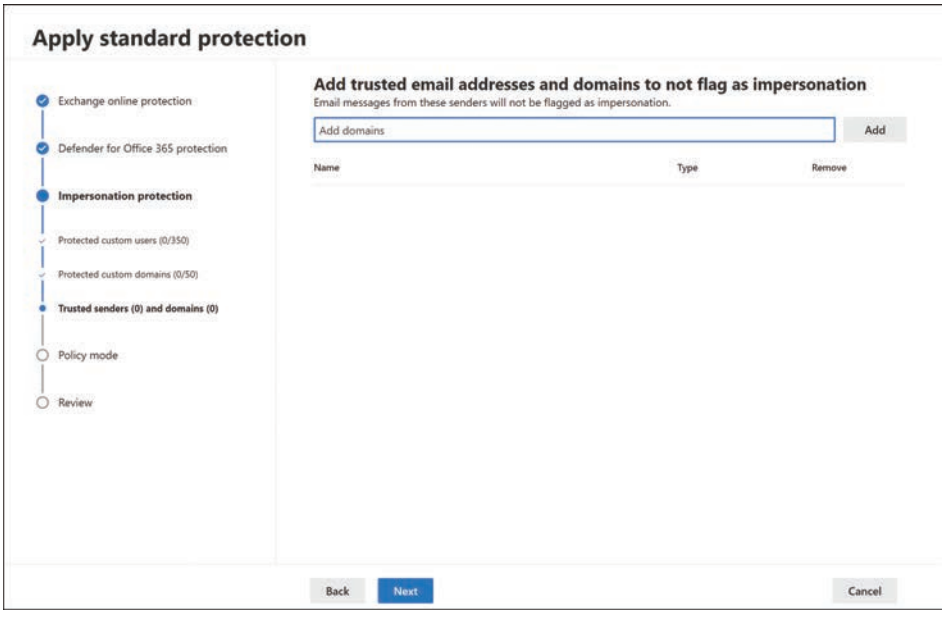


FIGURE 2-15 Adding trusted email address

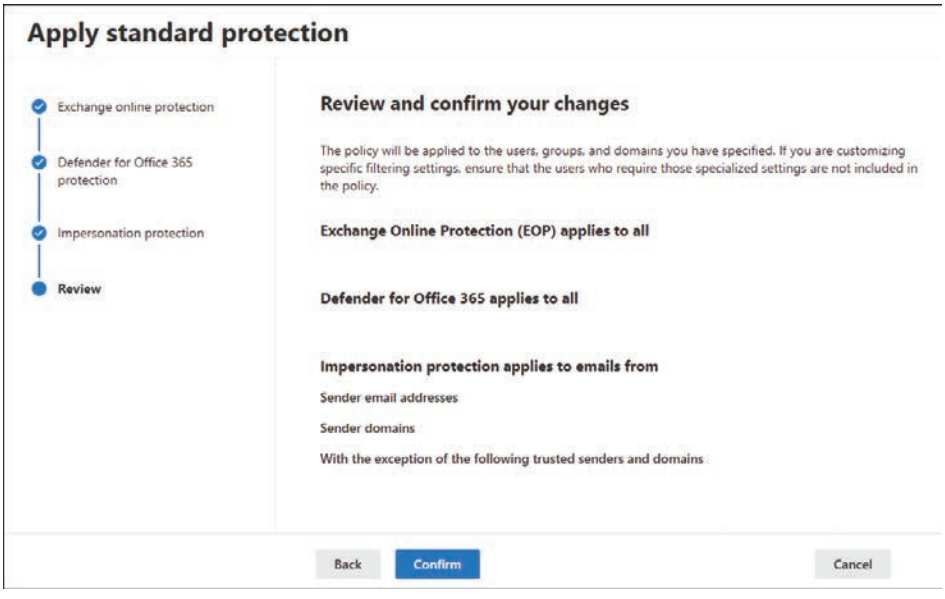


FIGURE 2-16 Review and confirm your changes page

13. Click the **Confirm** button; the **Standard protection updated** page appears, as shown in Figure 2-17.

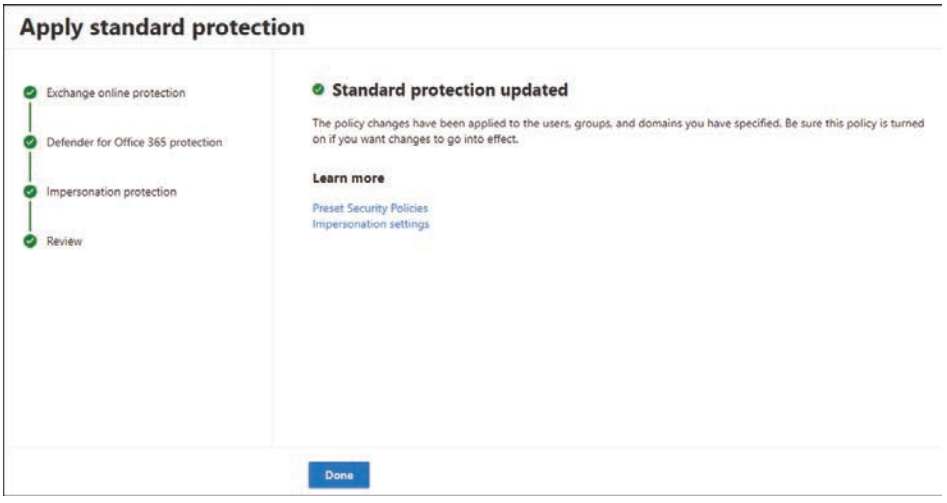


FIGURE 2-17 Standard protection updated page

14. Click the **Done** button to conclude. Return to the **Preset security policies** page; this page shows the **Standard protection is on** toggle (see Figure 2-18).

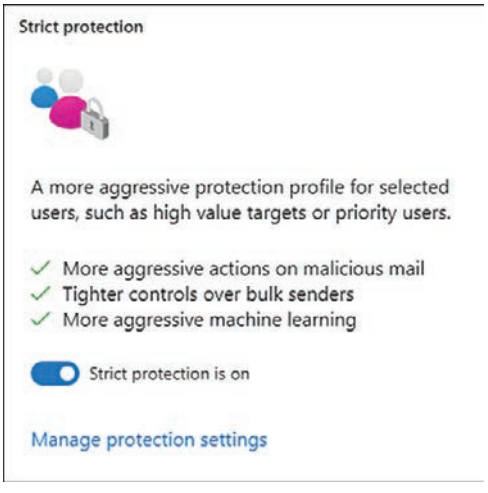


FIGURE 2-18 Standard protection toggle

After finishing configuring preset security policies, you can use the Configuration Analyzer to identify and address security policies with settings that are less secure than those defined by the Standard protection and Strict protection profiles in preset security policies. Click **Threat policies** to return to the **Threat policies** page. Then, click **Configuration analyzer** (see Figure 2-8); the **Configuration analyzer** page appears, as shown in Figure 2-19.



FIGURE 2-19 Configuration analyzer page

By default, the Configuration Analyzer will open, showing the **Standard recommendation** tab. The Standard recommendation evaluates your current security policies against the standard recommendations and adjusts your settings to align with the recommended security level. If you need a stricter set of recommendations, you can switch to the **Strict recommendation** tab and make the changes there. The **Configuration drift analysis and history** tab can be used to audit and track changes in policy.

To apply a recommendation, you just need to select the recommendation from the list (for example, **Change 15 to 30**) and click the **Apply recommendation** button that appears, as shown in Figure 2-20.

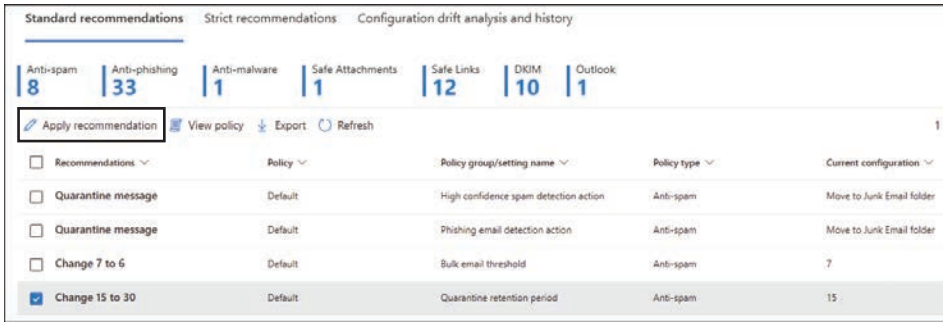


FIGURE 2-20 Applying a recommendation

You will receive a pop-up message asking if you are sure that you want to make the change; click the **OK** button to commit the change.

Configure security policies for Microsoft Defender for Endpoint, including attack surface reduction (ASR) rules

Endpoint security policies are configurations designed to enhance the protection, detection, and response capabilities of devices within an organization. These policies allow administrators

to define and enforce security settings across endpoints to protect against threats, reduce vulnerabilities, and maintain compliance.

It allows administrators to manage security settings for endpoints across the organization from a unified interface, and it applies security settings in real time to ensure endpoints are continuously protected. There are different types of endpoint security policies, as shown in the list below:

- **Antivirus** Can be used to configure and manage antivirus settings for endpoints, including real-time protection, cloud-delivered protection, and scheduled scans.
- **Endpoint Detection and Response (EDR)** Can be used to enable advanced threat detection and response capabilities, allowing you to monitor and investigate suspicious activities on endpoints.
- **Attack Surface Reduction (ASR)** Use this policy to mitigate potential attack vectors by limiting risky behaviors, such as executing scripts or macros from untrusted sources and running unsigned or vulnerable applications.
- **Firewall** Use this policy to configure firewall rules and settings to control incoming and outgoing traffic. It helps to protect endpoints from unauthorized access and external threats.
- **Disk encryption** This policy allows you to manage BitLocker encryption settings to ensure data on endpoints is encrypted and protected from unauthorized access.

Policies can be deployed using the Microsoft Defender portal or Microsoft Intune. By default, Microsoft Defender for Endpoint is already integrated with Intune. You can validate this configuration by choosing **System** > **Settings** > **Endpoint** > **Advanced Features**. After doing so, you will see that the Microsoft Intune connection toggle is on. This integration allows the sharing of device information and enhanced policy enforcement with Microsoft Intune.

Follow the steps below to create an endpoint security policy using Microsoft Defender Portal:

1. Sign in to *https://security.microsoft.com*.
2. In the left navigation pane, click **Endpoint** > **Configuration management** > **Endpoint Security Policies**. The **Endpoint Security Policies** page appears, as shown in Figure 2-21.

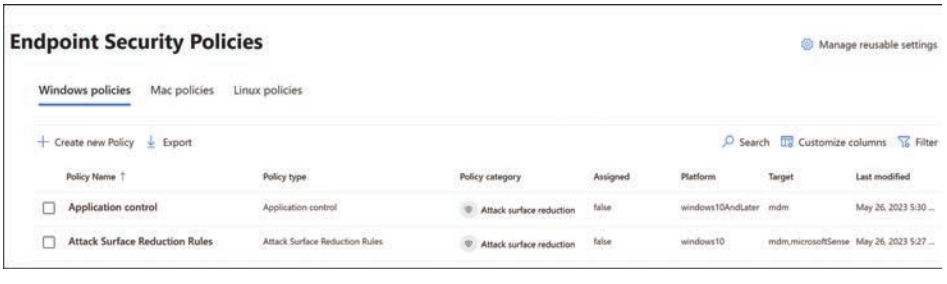


FIGURE 2-21 Endpoint security policies

3. Click the **Create a new Policy** button, and in the **Create a new Policy** blade, select the proper platform, such as **Windows 10**, **Windows 11**, or **Windows Server**.
4. Click the **Select Template** dropdown, and you will see the options shown in Figure 2-22.

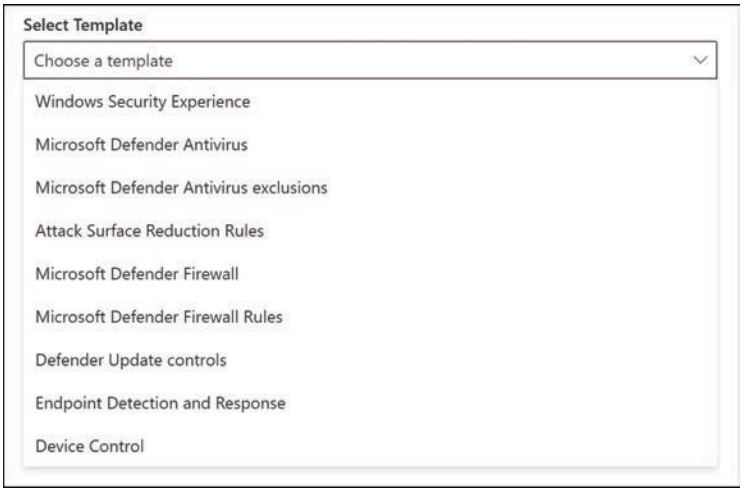


FIGURE 2-22 Templates available

5. For this example, select the **Endpoint Detection and Response** option and click the **Create policy** button; the **Create new policy** wizard appears, as shown in Figure 2-23.

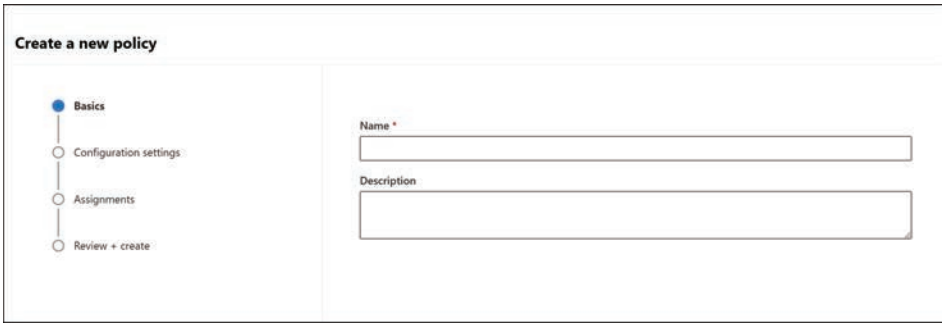


FIGURE 2-23 Create a new policy wizard

6. Type a name for the policy in the **Name** field, type a brief explanation about this policy in the **Description** field, and click the **Next** button; the **Configuration settings** page appears, as shown in Figure 2-24.

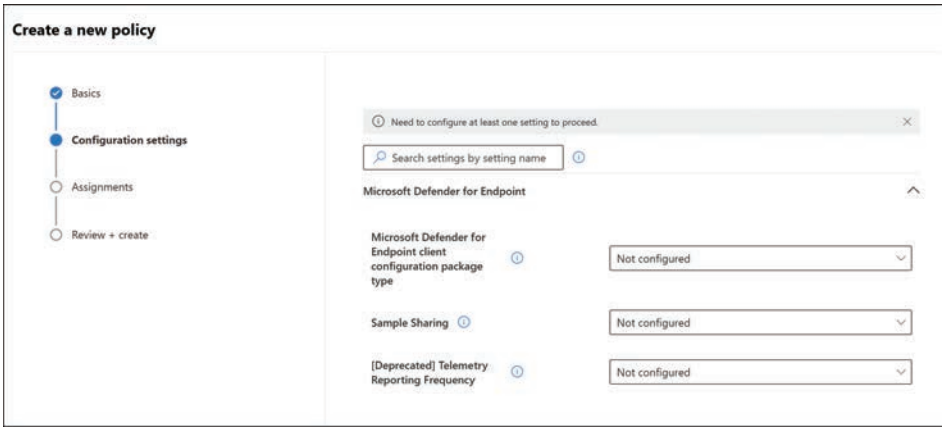


FIGURE 2-24 Configuration settings page

7. Click the dropdown next to the **Microsoft Defender for Endpoint client configuration package type** option. If you are integrating it with Microsoft Intune, you should select the **Auto from connector** option (the **Onboarding blob from Connector** option will automatically appear). With this option, the onboarding policy automatically uses the onboarding blob that Intune received from Microsoft Defender. Leave the other options set to their defaults and click the **Next** button. The **Assignments** page appears, as shown in Figure 2-25.

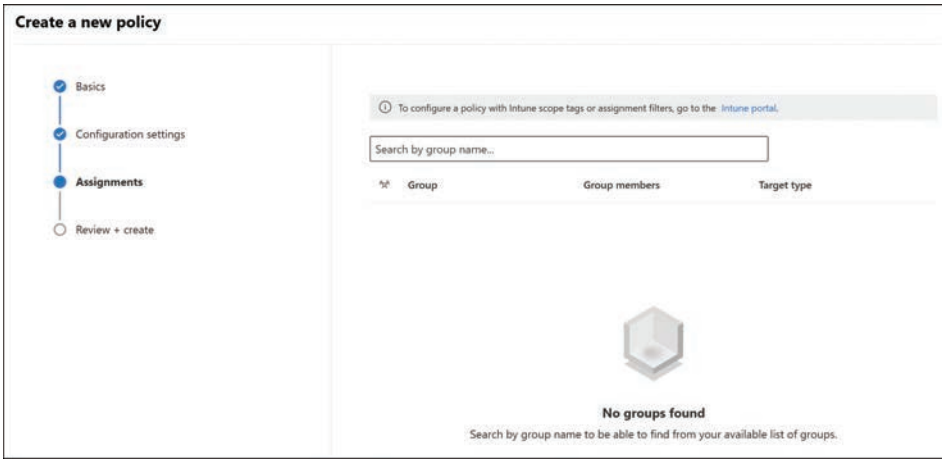


FIGURE 2-25 Assignments page

8. On the **Assignments** page, select the groups (device or user groups) that will receive this profile. After making the selection, click **Next**, and then click **Save**.

Attack surface reduction (ASR)

An organization's attack surface consists of all potential points where attackers could exploit devices or networks. Minimizing the attack surface strengthens the protection of your organization's devices and network, limiting opportunities for attackers to launch attacks.

Implementing Attack Surface Reduction (ASR) rules in Microsoft Defender for Endpoint helps you do this proactively by blocking risky behaviors before malware fully executes, rather than reacting after the fact. In practice, ASR rules target common attacker techniques such as:

- Office apps spawning child processes (often used to launch PowerShell or CMD)
- Scripts or executables that download and run content from the internet
- Abuse of WMI and JavaScript/VBScript engines
- Credential-stealing attempts (for example, suspicious access to Local Security Authority Subsystem Service [LSASS])
- Code execution from unusual locations, like temporary or email cache folders

Because these techniques are heavily reused across phishing, ransomware, and hands-on-keyboard intrusions, reducing them measurably lowers incident frequency and blast radius.

ASR also complements other MDE layers (next-gen AV, EDR, and endpoint firewall/network protection): AV detects known threats, EDR helps you investigate and respond, while ASR removes entire classes of high-risk behaviors, starving attackers of their usual footholds. Rules can be deployed with Microsoft Intune, Group Policy, or PowerShell; scoped to device groups; and tuned with per-rule exclusions (by file hash, path, certificate, or process) to accommodate legitimate business software without weakening your global security posture.

You can initially use Audit mode to assess the potential impact of enabling ASR rules on your organization. Testing all rules in audit mode first allows you to evaluate their effects on line-of-business (LOB) applications and to separate genuine business workflows from look-alike malicious behavior. This is important because many LOB tools were designed for functionality, not least-privilege execution; they may, for example, update via scripts from web locations or spawn helper processes that resemble attacker tradecraft. During this phase, use the Microsoft Defender portal (and Advanced Hunting queries) to review audit events, identify noisy rules, and add narrow, evidence-based exclusions. Once validated, move rules to Block mode for pilot groups, then broaden rollout.

In 2024, Microsoft added Warn mode as a middle ground: users see a notification when content is blocked and can choose to unblock once to complete their task; the allow lasts 24 hours and then enforcement resumes, giving security teams time to monitor what users felt they needed to bypass. Warn mode is particularly useful for field, executive, or developer devices where productivity impact is sensitive, and it creates teachable moments that raise security awareness. Warn mode requires Windows 10 version 1809 or later, Windows 11, or Windows Server version 1809 or later, and Microsoft Defender Antivirus running with real-time

protection in Active mode. Also, make sure Microsoft Defender Antivirus and anti-malware updates are installed, which include the following:

- Minimum platform release requirement: 4.18.2008.9
- Minimum engine release requirement: 1.1.17400.5

For ongoing governance, track ASR coverage and efficacy with the built-in reports, review exception drift quarterly, and align rule posture with your threat model (such as stricter Office and script rules for phishing-exposed cohorts, stricter credential-theft rules for admin workstations).

MORE INFO **PLANNING**

Before implementing ASR it is important to plan the adoption and the overall deployment phases. To learn more details about these processes, visit *https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-deployment*.

Follow the steps below to enable ASR rules using Microsoft Defender Portal:

1. Sign in to *https://security.microsoft.com*.
2. In the left navigation pane, click **Endpoints** > **Configuration management** > **Endpoint Security Policies**. The **Policy templates** page appears, as shown in Figure 2-21.
3. Click the **Create a new Policy** button, and in the **Create a new Policy** blade, select the proper platform, such as **Windows 10**, **Windows 11**, or **Windows Server**.
4. Click the **Select Template** dropdown, and you will see the options shown previously in Figure 2-22.
5. For this example, select the **Attack Surface Reduction Rules** option. Click the **Create policy** button; the **Create new policy** wizard appears, as shown previously in Figure 2-23.
6. Type a name for the policy in the **Name** field, type a brief explanation about this policy in the **Description** field, and click the **Next** button. The **Configuration settings** page appears, as shown in Figure 2-26.
7. While the name for each ASR rule is self-explanatory, you can learn more about each of these rules at *https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference*. For each rule, you can click the **Not configured** dropdown and change the mode to **Block**, **Audit**, or **Warn**. When you select the type of mode you want from the dropdown, you will also have the opportunity to add exclusions for the rule (optional). Figure 2-26 shows only the first part of the screen; the second part, shown in Figure 2-27, has additional settings that you can also enable.

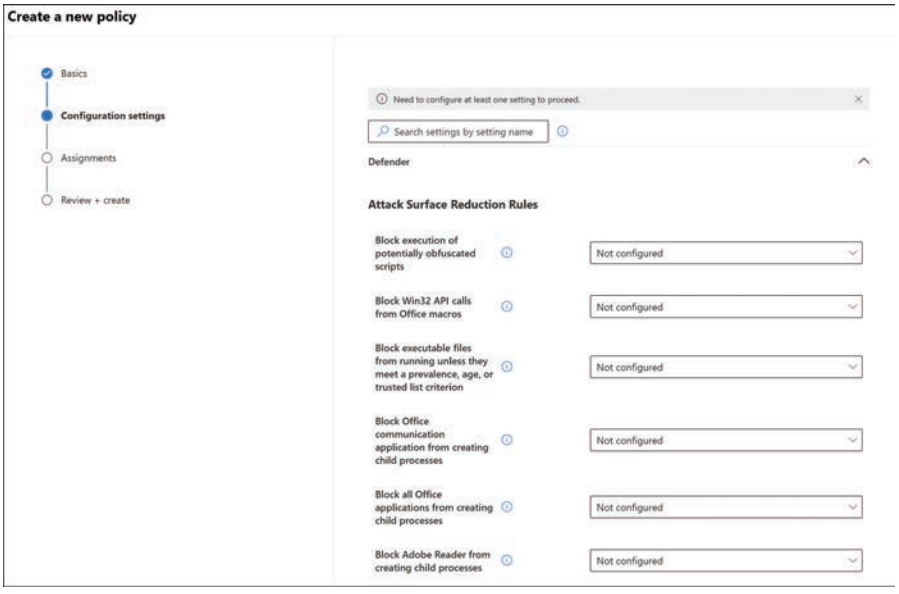


FIGURE 2-26 ASR rules

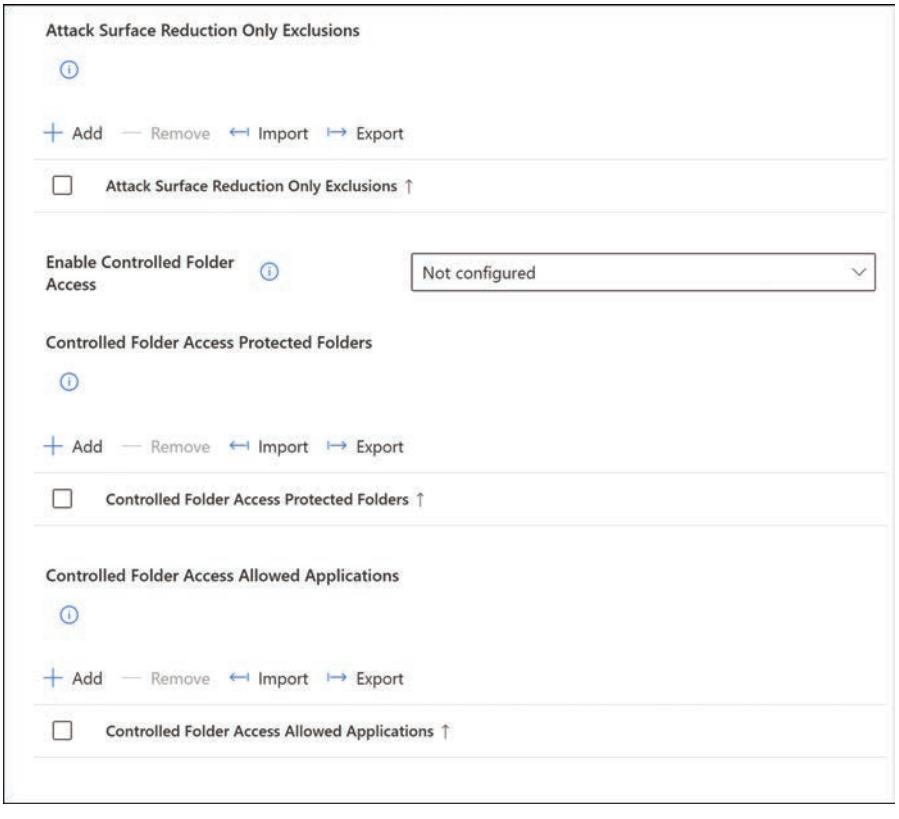


FIGURE 2-27 Second part of the ASR rules configuration

8. The ASR-only exclusion enables you to exclude specific files or fully qualified resources from being matched by ASR rules. To configure this, click the **Add** button and add the desired paths. Each entry should be formatted as a name–value pair, where the name represents a string specifying a path or a fully qualified resource name. For instance, you could use a path like `C:\Windows` to exclude all files within that directory or a fully qualified resource name like `C:\Windows\calc.exe` to exclude a specific file. The type for this value is `string`.
9. The **Enable Controlled Folder Access** option allows you to configure the state (**On**, **Off**, or **Audit**) for the controlled folder access feature. Controlled folder access restricts untrusted applications from modifying or deleting files in specific folders. The value type is an integer with a range of `0` to `2`.
10. The **Controlled Folder Access Protected Folders** option allows you to specify additional folder locations for inclusion in the controlled folder access feature. These user-defined folders will supplement system-defined folders, such as My Documents and My Pictures. The value type is a `string`.
11. The **Controlled Folder Access Allowed Applications** option enables you to specify applications for inclusion in the controlled folder access feature. Adding an application as allowed permits it to modify or delete content in protected folders. The value type is a `string`.
12. After making the selections that are appropriate for your deployment, click the **Next** button; the **Assignments** page appears, as previously shown in Figure 2-25. On the **Assignments** page, you select the groups (device or user groups) that will receive this profile. After making the selection, click **Next**, and then click **Save**.

After configuring the rules—and those rules are in effect—you can use the **Attack surface reduction rules** reporting page in the Microsoft Defender portal to see the status of matching rules. This report is available from the **Reports** option, located at the bottom of the left navigation pane, and then click the **Attack surface reduction rules** option in the **Endpoints** section. The report's page appears with the first tab selected by default (**Detections**), as shown in Figure 2-28.

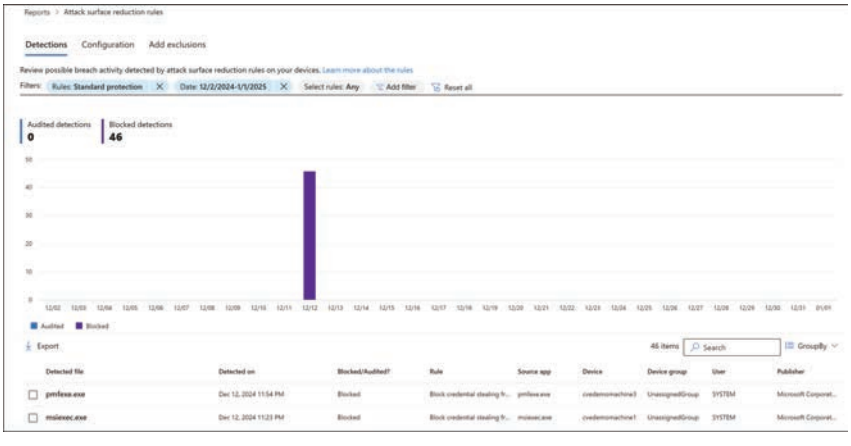


FIGURE 2-28 Detections report

Index

A

Access policy (Microsoft Defender XDR), 84
Action Center, alerts and policies, 18
activities, Microsoft 365, investigating, 179–182
Activity policy (Microsoft Defender XDR), 84
Advanced Hunting, Microsoft Defender XDR, 232–235
Aggregated Reporting feature (Microsoft Defender for Endpoint), 7
AIR (Automated Investigation and Response), 154–156
alert notification rules, Microsoft Defender XDR, configuring, 2–5
AlertEvidence table, 231
AlertInfo table, 231
alerts, managing, SOC (security operations center), 115–118
Allow or block file feature (Microsoft Defender for Endpoint), 6
analytic rules
    versus hunting queries, 253
    Microsoft Sentinel, configuring, 125–135
anomaly detection analytic rules, configuring, 133–135
Anomaly detection policy (Microsoft Defender XDR), 84
Apply streamlined connectivity feature (Microsoft Defender for Endpoint), 7
archived log data, retrieving and managing, Microsoft Sentinel, 275–277
ASIM (Advanced Security Information Model), Microsoft Sentinel, parsers, 135–138
ASR (attack surface reduction), Microsoft Defender for Endpoint, configuring, 97–106
at-risk devices, identifying and remediating, 37–41
attack disruption, Microsoft Defender XDR, configuring, 19–23
Attack surface & metrics page (MSEM), 45–46
attack vector coverage analysis, MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Matrix, 242–244
Authenticated telemetry feature (Microsoft Defender for Endpoint), 8
authentication events, querying, 138
automated investigation and response, Microsoft Defender XDR, 13–19
Automated Investigation and Response (AIR), 154–156
automatic attack disruption
    business email compromise incidents, investigating and remediating, 156–157
    Microsoft Defender XDR, configuring, 19–23
    ransomware, investigating and remediating, 156–157
Automatically resolve alerts feature (Microsoft Defender for Endpoint), 6
automation levels, Microsoft Defender for Endpoint, configuring, 23–27
Azure RBAC roles, Microsoft Sentinel, configuring, 55–59

B

behavioral analytics, UEBA (user entity behavior analytics), 142–148
bidirectional synchronization between, Microsoft Sentinel, Microsoft Defender XDR, 68–69
bookmarks, hunting for data investigations, Microsoft Sentinel, 261–275
bulk actions, TI (threat intelligence), 246
business email compromise incidents, investigating and remediating, automatic attack disruption, 156–157

C

capabilities log (Sentinel), 59
capacity, Microsoft Security Copilot, monitoring, 216–218
CEF (Common Event Format), 70–73
CIS Microsoft 365 Foundations Benchmark (MSEM), 45
cloud, unprotected resources, discovering, 31–36

cloud workload protections, configuring, 106–109
Common Event Format (CEF), 70–73
comprised identities, investigating and remediating, Microsoft Extra ID, 168–169
configuring
  Microsoft Defender for Cloud, cloud workload protections, 106–109
  Microsoft Defender for Endpoint
    advanced features, 5–8
    automation levels, 23–27
    device groups, 23–27
    permissions, 23–27
    policies, 97–106
    rules settings, 8–13
  Microsoft Defender XDR, 2
    alert notification rules, 2–5
    automatic attack disruption, 19–23
    deception rules, 118–122
    detection, 110–115
    protections, 83–88
    vulnerability notification rules, 2–5
  Microsoft Sentinel
    analytic rules, 125–135
    Azure RBAC roles, 55–59
    bidirectional synchronization between Microsoft Defender XDR, 68–69
    data connectors, 65–68
    detections, 122–125
    playbooks, 199–204
    roles, 53–55
    SOAR (Security Orchestration, Automation, and Response), 195–199
connecting data sources permission (Sentinel), 56
connectors, Microsoft Security Copilot, 211–214
contain user attack disruption leverage response action, 20
Content Hub (Sentinel), 63–65, 205
  analytics rules, managing, 132–133
Content Search, Microsoft 365, 181–182
correlation, managing, SOC (security operations center), 115–118
costs, Microsoft Security Copilot, monitoring, 216–218
creating and deleting workbooks permission (Sentinel), 56
cross-workspace analytics rules, Microsoft Sentinel, 195
Cryptographic Assessment (MSEM), 44
Custom network indicators feature (Microsoft Defender for Endpoint), 6

D

data connectors, Microsoft Sentinel, configuring, 65–68
data ingestion, monitoring and optimizing, 79
data sources, ingesting, Microsoft Sentinel, 59–62
DCU (Digital Crimes Unit), 163
Deception feature (Microsoft Defender for Endpoint), 7
deception rules, Microsoft Defender XDR, configuring, 118–122
Default to streamlined connectivity feature (Microsoft Defender for Endpoint), 7
Defender for Cloud. *see* Microsoft Defender for Cloud
Defender for Endpoint. *see* Microsoft Defender for Endpoint
Defender for Identity. *see* Microsoft Defender for Identity
Defender Threat Intelligence, 218
Defender XDR. *see* Microsoft Defender XDR
  configuring, 2
    alert notification rules, 2–5
    vulnerability notification rules, 2–5
detection
  Microsoft Defender XDR, configuring, 110–115
  Microsoft Sentinel, configuring, 122–125
device contain attack disruption leverage response action, 20
Device discovery feature (Microsoft Defender for Endpoint), 7
device groups, Microsoft Defender for Endpoint, configuring, 23–27
device timelines, investigating, Microsoft Defender Portal, 172–174
DeviceEvents table, 230
DeviceFileEvents table, 231
DeviceProcessEvents table, 231
Digital Crimes Unit (DCU), 163
disable user attack disruption leverage response action, 20
DLP (Data Loss Prevention), Microsoft Purview, 158–163
DNS events, querying, 138
Download quarantined files feature (Microsoft Defender for Endpoint), 7

E

EDR in Block Mode feature (Microsoft Defender for Endpoint), 6
email connectors, 203

EmailAttachmentInfo table, 231
EmailEvents table, 231
Endpoint attack notification feature (Microsoft Defender for Endpoint), 8
entity investigation, Microsoft Defender for Endpoint, 177–179
Event IDs, 75
events
  authentication, querying, 138
  DNS, querying, 138

F

File policy Email Events (Microsoft Defender XDR), 84

G

give Microsoft Sentinel permission to run playbooks permission (Sentinel), 56
Graph Security API, 61
guest user assigning incidents permission (Sentinel), 56

H

Hide potential duplicate device records feature (Microsoft Defender for Endpoint), 6
hunt management, threats, Microsoft Sentinel, 251–260
hunting queries
  versus analytics rules, 253
  logic, 270
  monitoring, Livestream, 257–260

I

identities, comprised, Microsoft Extra ID, 168–169
Identity Security (MSEM), 44
IdentityLogonEvents table, 231
incident logic, 138
incident response, 153
  Microsoft Defender for Cloud, 163–166
  Microsoft Defender for Endpoint, 171–179
  Microsoft Defender Portal, 153–171
  Microsoft Security Copilot, 222–225
  Microsoft Sentinel, 182–195
incidents, adding bookmarks, 264–275
indicators, Microsoft Defender for Endpoint, 8–11
ingestion rules, TI (threat intelligence), 246
ingestion_time() function, 132
Insider Risk Management, Microsoft Purview, 161
investigation and response, Microsoft Defender XDR, 13–19
investigation packages, Microsoft Defender Portal, 174–177
IoCs, 247–249
Isolation Exclusion Rules feature (Microsoft Defender for Endpoint), 7

J

Jupyter Project, 270–271

K

KQL (Kusto Query Language), 138–142, 231
  configuring, 126–135
  threat identification, 229–235, 239–242
  workbooks, creating, 282–286

L

live response, Microsoft Defender Portal, 174–177
Live Response & Live Response for Servers feature (Microsoft Defender for Endpoint), 7
Live Response unsigned script execution feature (Microsoft Defender for Endpoint), 7
Livestream, monitoring hunting queries, 257–260
Log Analytics, 56–59
log tables, workspaces, creating custom, 76–79
logic, hunting queries, 270
logs, Microsoft Sentinel, 59
Logs Ingestion API, 79

M

Malware detection policy (Microsoft Defender XDR), 84
MDTI (Microsoft Defender Threat Intelligence), 218
MDVM (Microsoft Defender Vulnerability Management), 37–41

Microsoft 365
Content Search, 181–182
investigating activities, 179–182
Microsoft Defender XDR policies, configuring, 88–97
Microsoft Graph activity logs, 182
Unified Audit Log, 180–181
Microsoft Defender for Cloud
configuring, cloud workload protections, 106–109
discovering unprotected resources, 31–36
workload protections, 163–166
Microsoft Defender for Cloud Apps, 7
security risks, investigating and remediating, 166–167
Microsoft Defender for Endpoint
configuring
advanced features, 5–8
automation levels, 23–27
device groups, 23–27
permissions, 23–27
rules settings, 8–13
evidence and entity investigation, 177–179
identifying unmanaged devices, 27–31
incident response, 171–179
indicators, 8–11
policies, configuring, 97–106
web content filtering, 12–13
Microsoft Defender for Identity, security alerts, investigating and remediating, 169–171
Microsoft Defender for Office 365, threats, investigating and remediating, 154–156
Microsoft Defender Portal
incident response, 153–171
investigating device timelines, 172–174
investigation packages, 174–177
live response, 174–177
threat identification, 235–239
Microsoft Defender Threat Intelligence (MDTI), 218
Microsoft Defender Vulnerability Management (MDVM). *see* MDVM (Microsoft Defender Vulnerability Management)
Microsoft Defender XDR
Advanced Hunting, 232–235
automated investigation and response, 13–19
behavioral analytics, 147–148
configuring, 2
automatic attack disruption, 19–23
bidirectional synchronization between Microsoft Sentinel, 68–69
deception rules, configuring, 118–122
detection, configuring, 110–115
MSEM (Microsoft Security Exposure Management), 42–48
permissions, 231–232
policies, 83–88
configuring, 88–97
protections, configuring, 83–88
threat identification, 229
KQL (Kusto Query Language), 229–235, 239–242
Microsoft Defender Portal, 235–239
Microsoft Extra ID, comprised identities, investigating and remediating, 168–169
Microsoft Graph, activity logs, 182
Microsoft Graph Security API, 61
Microsoft Intune Connection feature (Microsoft Defender for Endpoint), 8
Microsoft Learn, 292
Microsoft Press, 292
Microsoft Purview
DLP (Data Loss Prevention), 158–163
Insider Risk Management, 161
Microsoft Security Copilot, 207
connectors, 211–214
identifying threats and risks, 218–221
incident response, 222–225
monitoring capacity and cost, 216–218
permissions, 214–215
plugins, 210–211
promptbooks, creating, 207–210
roles, 214–215
Microsoft Security Exposure Management (MSEM). *see* MSEM (Microsoft Security Exposure Management)
Microsoft Security Response Center (MSRC), 163
Microsoft Sentinel
archived log data, retrieving and managing, 275–277
ASIM (Advanced Security Information Model), parsers, 135–142
bookmarks, hunting for data investigations, 261–275
CEF (Common Event Format), 70–73
configuring
analytic rules, 125–135
Azure RBAC roles, 55–59
bidirectional synchronization between Microsoft Defender XDR, 68–69
data connectors, 65–68
roles, 53–55
Content Hub, 63–65, 205
cross-workspace analytics rules, 195
detections, configuring, 122–125
free data sources, 62

incident response, 182–195
ingesting data sources, 59–62
Log Analytics, 56–59
logs, 59
MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Matrix, 242–244
permissions, 55–56
playbooks
creating and configuring, 199–204
managing incidents, 205–206
remediating threats, 204–205
running on on-premises resources, 204–206
pricing calculator, 57
remediating incidents, 191–195
search jobs, creating and managing, 277–279
SOAR (Security Orchestration, Automation, and Response), configuring, 195–199
Syslog (System Logging Protocol), 70–73
threat identification, 242
attack vector coverage analysis, 242–244
hunt management, 251–260
TI (threat intelligence), 244–250
triaging incidents, 191
UEBA (user entity behavior analytics), 142–148
WEF (Windows Event Forwarding), 73–76
workbooks
creating and configuring, 279–287
creating with KQL, 282–286
templates, 279–282
visualizations, 286–287
workspace planning, 47–52
Microsoft XDR, 1
MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Matrix, 240
attack vector coverage analysis, 242–244
MSEM (Microsoft Security Exposure Management), Microsoft Defender XDR, 42–48
MSRC (Microsoft Security Response Center), 163

N

network sessions, querying, 138
notebooks, advanced hunting, 270–275
notification rules, Microsoft Defender XDR, configuring, 2–5
NRT (near-real-time) query rules, configuring, 130–132

O

OAuth app policy (Microsoft Defender XDR), 84
objective mapping, 292–295
onboard devices discovery, 27

P

parsers, ASIM (Advanced Security Information Model), 135–142
permissions
Microsoft Defender for Endpoint, configuring, 23–27
Microsoft Defender XDR, 231–232
Microsoft Security Copilot, 214–215
Microsoft Sentinel, 55–56
playbooks
Microsoft Sentinel
creating and configuring, 199–204
managing incidents, 205–206
remediating threats, 204–205
running on on-premises resources, 204–206
plugins, Microsoft Security Copilot, 210–211
policies
Microsoft Defender for Endpoint, configuring, 97–106
Microsoft Defender XDR, 83–88
configuring, 88–97
Preview features feature (Microsoft Defender for Endpoint), 8
promptbooks, Microsoft Security Copilot, creating, 207–210
purpose log (Sentinel), 59

Q

queries
authentication events, 138
DNS events, 138
KQL (Kusto Query Language), 138–142
configuring, 126–135
network sessions, 138
parsers, ASIM (Advanced Security Information Model), 135–142
underlying data, 141

R

ransomware, investigating and remediating, automatic attack disruption, 156–157
references, time ranges, 255
remediation, at-risk devices, 37–41
Restrict correlation to within scoped device groups feature (Microsoft Defender for Endpoint), 6
risks, identifying, Microsoft Security Copilot, 218–221
roles
    Microsoft Security Copilot, 214–215
    Microsoft Sentinel, configuring, 53–59
rules settings, Microsoft Defender for Endpoint, configuring, 8–13

S

SC-200 Microsoft Security Operations Analyst exam, updates, 291–295
scheduled query rules, configuring, 126–131
SCUs (Security Compute Units), 216
search jobs, creating and managing, Microsoft Sentinel, 277–279
Security Compute Units (SCUs), 216
Security Copilot. *see* Microsoft Security Copilot
security information and event management (SIEM), 1
security operations center (SOC), 1, 79
Sentinel. *see* Microsoft Sentinel
Session policy network (Microsoft Defender XDR), 84
Share endpoint alerts with Microsoft Compliance Center feature (Microsoft Defender for Endpoint), 8
Show user details feature (Microsoft Defender for Endpoint), 7
SIEM (security information and event management), 1
    Microsoft Graph Security API, 61
Skype user details feature (Microsoft Defender for Endpoint), 7
SOA (Security Operations Analyst), 153
SOC (security operations center), 1, 79
    alerts, managing, 115–118
    Microsoft Sentinel, configuring, 195–199
STIX/TAXII, 247–249
storage tiers, Log Analytics, 57
suppression, managing, SOC (security operations center), 115–118
Syslog (System Logging Protocol), 70–73

T

Tamper protection feature (Microsoft Defender for Endpoint), 7
TAXII, 245–246
templates, workbooks, Microsoft Sentinel, 279–282
threats, 229
    identifying
        hunt management, 251–260
        KQL (Kusto Query Language), 229–235, 239–242
        Microsoft Defender Portal, 235–239
        Microsoft Defender XDR, 229–242
        Microsoft Security Copilot, 218–221
        Microsoft Sentinel, 242–279
        MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Matrix, 242–244
        TI (threat intelligence), 244–250
    investigating and remediating, Microsoft Defender for Office 365, 154–156
TI (threat intelligence), 244–250
    connectors, 249–250
time ranges, references, 255
triaging incidents, Microsoft Sentinel, 191
tuning, managing, SOC (security operations center), 115–118

U

UEBA (user entity behavior analytics), 142–148
Unified Audit Log, Microsoft 365, 180–181
Unify audit log feature (Microsoft Defender for Endpoint), 7
unmanaged devices, identifying, Microsoft Defender for Endpoint, 27–31
unprotected resources, discovering, Microsoft Defender for Cloud, 31–36
updates, SC-200 Microsoft Security Operations Analyst exam, 291–295
usage log (Sentinel), 59
using playbooks for autmation permission (Sentinel), 56

V

visualizations, Microsoft Sentinel workbooks, 286–287
vulnerability notification rules, Microsoft Defender XDR, configuring, 2–5

W

web content filtering, Microsoft Defender for Endpoint, 12–13
Web content filtering feature (Microsoft Defender for Endpoint), 7
WEF (Windows Event Forwarding), 73–76
Windows Event Forwarding (WEF), 73–76
workbooks
    Microsoft Sentinel
        creating and configuring, 279–287
        creating with KQL, 282–286
        templates, 279–282
        visualizations, 286–287
workloads
    cloud protection, configuring, 106–109
    Microsoft Defender for Cloud, protections, 163–166
workspaces
    log tables, creating custom, 76–79
    Microsoft Sentinel, planning, 47–52

X

XDR. *see* Microsoft XDR

Z

Zero Trust (MSEM), 45