Microsoft

Microsoft 365 Mobility and Security

SECOND EDITION

Exam Ref MS-101

Brian Svidergol
Robert D. Clements
Charles Pluta

FREE SAMPLE CHAPTER

Microsoft

Exam Ref MS-101 Microsoft 365 Mobility and Security

Second Edition

Brian Svidergol
Bob Clements
Charles Pluta

Exam Ref MS-101 Microsoft 365 Mobility and Security, Second Edition

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

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.

ISBN-13: 978-0-13-747177-5
ISBN-10: 0-13-747177-7

Library of Congress Control Number: 2021944465

ScoutAutomatedPrintCode

TRADEMARKS

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.

SPECIAL SALES

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

EDITOR-IN-CHIEF
Brett Bartow

EXECUTIVE EDITOR
Loretta Yates

DEVELOPMENT EDITOR
Rick Kughen

SPONSORING EDITOR
Charvi Arora

MANAGING EDITOR
Sandra Schroeder

SENIOR PROJECT EDITOR
Tracey Croom

COPY EDITOR
Rick Kughen

INDEXER
Valerie Haynes Perry

PROOFREADER
Scout Festa

TECHNICAL EDITOR
Boyd Nolan

EDITORIAL ASSISTANT
Cindy Teeters

COVER DESIGNER
Twist Creative, Seattle

COMPOSITOR
Danielle Foster

Contents at a glance

Introduction *xiii*

CHAPTER 1 **Implement modern device services** **1**

CHAPTER 2 **Implement Microsoft 365 security and threat management** **81**

CHAPTER 3 **Manage Microsoft 365 governance and compliance** **147**

Index *231*

Contents

Introduction xiii

Organization of this book xiii

Preparing for the exam xiii

Microsoft certifications xiv

Quick access to online references. xiv

Errata, updates & book support xv

Stay in touch xv

Chapter 1 Implement modern device services **1**

Skill 1.1: Plan device management. 2

Plan device monitoring 2

Plan Microsoft Endpoint Manager implementation 4

Plan for configuration profiles 6

Skill 1.2: Manage device compliance 8

Plan for device compliance 9

Plan for attack surface reduction 18

Configure security baselines 21

Configure device-compliance policy 22

Skill 1.3: Plan for apps 24

Create and configure Microsoft Store for Business 25

Plan app deployment 34

Plan for mobile application management 40

Skill 1.4: Plan Windows 10 deployment 45

Plan for Windows as a service (WaaS) 45

Plan the appropriate Windows 10 Enterprise deployment method 51

Evaluate and deploy additional Windows 10 Enterprise security features 68

Skill 1.5: Enroll devices. 70

Plan for device join to Azure Active Directory (Azure AD) and plan for device enrollment 70

Enable device enrollment 71

Thought experiment. 77

Thought experiment answers 78

Chapter summary 78

Chapter 2 Implement Microsoft 365 security and threat management 81

Skill 2.1: Manage security reports and alerts 81

Evaluate and manage Microsoft Office 365 tenant security by using Secure Score 82

Manage incident investigation 88

Manage and review security alerts 94

Skill 2.2: Plan and implement threat protection with Microsoft Defender. 97

Plan Microsoft Defender for Endpoint 97

Design Microsoft Defender for Office 365 policies 103

Implement Microsoft Defender for Identity 116

Skill 2.3: Plan Microsoft Cloud App Security 119

Plan information protection by using Cloud App Security 119

Plan for application connectors 124

Configure Cloud App Security policies 127

Review and respond to Cloud App Security alerts 137

Monitor for unauthorized cloud applications 139

Thought experiment. 143

Thought experiment answers 144

Chapter summary 144

Chapter 3 Manage Microsoft 365 governance and compliance 147

Skill 3.1: Plan for compliance requirements 147

Plan compliance solutions 148

Assess compliance 149

Plan for legislative and regional or industry requirements and drive implementation 152

Skill 3.2: Manage information governance 154

Plan for data classification and labeling 155

Plan for restoring deleted content 158

Configure information retention 171

Design data retention labels 173

Skill 3.3: Implement Azure Information Protection. 176

Plan information protection solution 177

Implement Azure Information Protection policies 179

Monitor label alerts and analytics 183

Deploy Azure Information Protection unified labeling client 185

Configure Information Rights Management (IRM) for workloads 186

Plan for Windows Information Protection (WIP) implementation 187

Skill 3.4: Plan and implement data loss prevention (DLP) 193

Plan for DLP 194

Configure DLP policies 201

Monitor DLP policy matches 205

Skill 3.5: Manage search and investigation 208

Plan for auditing 209

Design Content Search solution 212

Plan for eDiscovery 214

Implement insider risk management 223

Thought experiment. 226

Thought experiment answers 227

Chapter summary 228

Index 231

Acknowledgments

I would like to thank my wife, Jennifer, for being supportive and putting up with the odd hours getting this book finished. To Elias Mereb and Brian Svidergol, thank you for the years of friendship, conferences, dinners, and everything else. And to my friends and colleagues Ed Gale, Joshua Waddell, and Aaron Lines, thank you for your friendship, mentorship, and advice the last couple of years. Finally, to all the IT professionals and readers of this book, thank you for taking the time to read, explore, learn, test, and "play around" with these technologies while you are learning. Keep it up, and good luck!

About the Authors

BRIAN SVIDERGOL designs and builds infrastructure, cloud, and hybrid solutions. He holds many industry certifications, including Microsoft Certified Solutions Expert (MCSE) – Cloud Platform and Infrastructure. Brian is the author of several books covering everything from on-premises infrastructure technologies to hybrid cloud environments. He has extensive real-world experience from startup organizations to large Fortune 500 companies on design, implementation, and migration projects.

BOB CLEMENTS specializes in enterprise device management. He holds industry certifications relating to client manageability and administration for Windows, Mac, and Linux. Bob has an extensive background in designing, implementing, and supporting device-management solutions for private- and public-sector companies. In his free time, he enjoys spending time with his family, writing, and exploring new technologies.

CHARLES PLUTA is a technical consultant and Microsoft Certified Trainer who has authored several certification exams, lab guides, and learner guides for various technology vendors. As a technical consultant, Charles has assisted small, medium, and large organizations in deploying and maintaining their IT infrastructure. He is also a speaker, staff member, or trainer at several large industry conferences every year. Charles has a degree in computer networking and holds over 25 industry certifications. He makes it a point to leave the United States to travel to a different country once every year. When not working on training or traveling, he plays pool in Augusta, Georgia.

Introduction

The MS-101 exam focuses on common tasks and concepts that an administrator needs to understand to plan, migrate to, deploy, and manage Microsoft 365 services. A majority of these services are included as part of the Enterprise Mobility + Security suite, with some optional compliance add-ons.

As an enterprise administrator responsible for the Microsoft 365 services in your organization, you will need to understand identities, security, policies, and industry and regulatory compliance as they relate to the organization to be successful.

This book assumes you already have a working knowledge of some Microsoft 365 services, including Exchange, SharePoint, Teams, or Windows 10. To complete some of the step-by-step guides, or to use some of the features that are outlined, you'll also need a supported device, or even a virtual machine, to be able to join and manage from your tenant.

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 you'll find in the text to find more information and take the time to research and study the topic. Great information is also available on MSDN, on TechNet, 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 Learn website: *http://aka.ms/examlist*. 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 the 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 *http://microsoft.com/learn*. Microsoft Official Practice Tests are available for many exams at *http://aka.ms/practicetests*.

Note that this Exam Ref is based on publicly available information about the exam and the authors' 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.

NEED MORE REVIEW? **ALL MICROSOFT CERTIFICATIONS**

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

Quick access to online references

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.

Download the list at *https://MicrosoftPressStore.com/ExamRefMS1012e/downloads*.

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.

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/ExamRefMS1012e/errata

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

For additional book support and information, please visit *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 *http://support.microsoft.com*.

Stay in touch

Let's keep the conversation going! We're on Twitter: *http://twitter.com/MicrosoftPress*.

CHAPTER 2

Implement Microsoft 365 security and threat management

In a traditional environment, applications and services are hosted and managed from an organization's on-premises data center. Intellectual property, employee data, and other sensitive information are contained within the confines of that organization. In the modern workplace, applications and services are hosted in cloud environments, such as Office 365, reducing overhead for IT and providing greater flexibility to the end user. This transition requires IT administrators to address new challenges around information protection and application security.

In this chapter we cover cloud-based security services for Microsoft 365. This includes a deep dive into Cloud App Security, Advanced Threat Analytics, and Windows Defender Advanced Threat Protection. With these services we walk through the various reports and alerts provided in each solution.

Skills covered in this chapter:

- 2.1: Manage security reports and alerts
- 2.2: Plan and implement thread protection with Microsoft Defender
- 2.3: Plan Microsoft Cloud App Security

Skill 2.1: Manage security reports and alerts

Microsoft 365 includes several cloud services under its umbrella, each one enabled with security controls. As an Azure cloud administrator, it is important that you know what these controls are, how to configure alerts, and how to generate reports so that you can keep informed when an event occurs. In this chapter we are going to be working with a few different technologies dealing with Microsoft 365 security. This will include an introduction to service assurance and the various security assessment reports that Microsoft is making available to customers. We will also be onboarding Azure AD Identity Protection and exploring its capabilities. Finally, we will be exploring the event-based alerts available in the Office 365 Security & Compliance center.

This skill covers how to:

- Evaluate and manage Microsoft Office 365 tenant security by using Secure Score
- Manage incident investigation
- Manage and review security alerts

Evaluate and manage Microsoft Office 365 tenant security by using Secure Score

In this skill section we review the Microsoft Secure Score. The Microsoft Secure Score is a numerical value based on the current configuration of the Microsoft 365 tenant. Every tenant has a different possible number of points, and the Secure Score is represented as a percentage of the possible points. By configuring or deploying the recommended best practices, an organization can increase their Secure Score points and percentage. A higher percentage then indicates an increased security posture based on the settings and policies defined by the organization.

Secure Score overview

The Microsoft Secure Score is segmented into different groups:

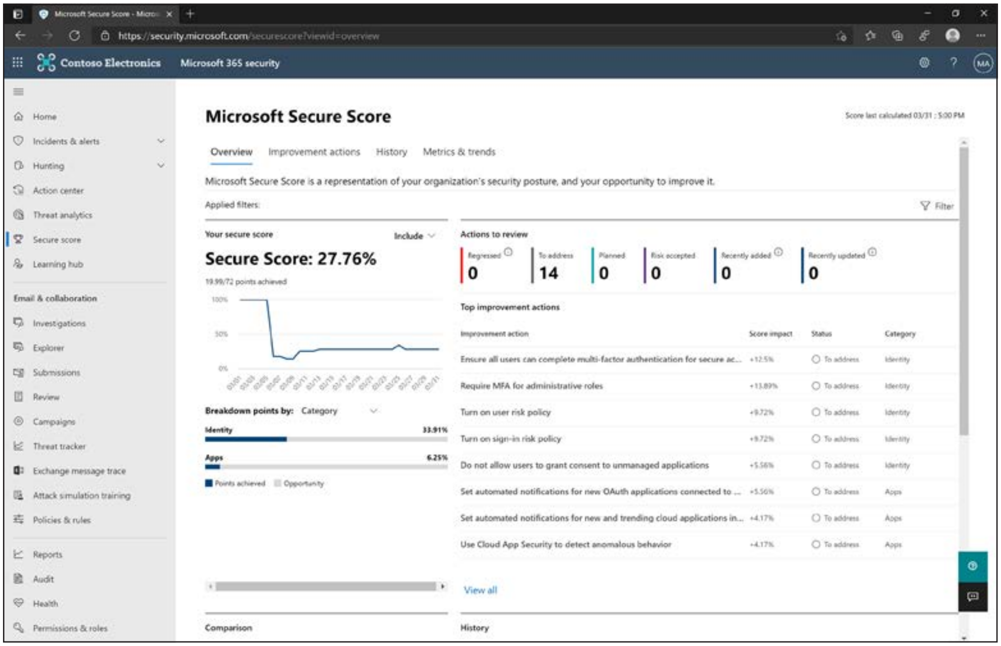
- **Identity** Actions to take with Azure Active Directory accounts and roles
- **Device** Actions to take with Microsoft Defender for Endpoint
- **App** Actions to take with email and cloud apps, including Office 365 and Microsoft Cloud App Security

To view the Secure Score for your organization, follow these steps.

1. Sign in to the Microsoft 365 security center at *https://security.microsoft.com*.
2. From the Navigation bar on the left, click **Secure score**.

The Secure Score for the organization is displayed on the Overview tab, as shown in Figure 2-1. By default, the Secure Score only includes the currently settings that have already been configured in the tenant. You can change the display to include theoretical possabilities, including:

- **Planned score** A projected score based on improvement actions that have been marked as ‘Planned’
- **Current license score** The total possible score that can be achieved with the current licensed features
- **Achievable score** The total score that can be achieved with both current licenses and risk acceptance



Microsoft Secure Score

Score last calculated 03/31 ; 5:00 PM

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Applied filters:

Your secure score

Secure Score: 27.76%

19.99/72 points achieved

Breakdown points by: Category

Identity 33.91%

Apps 6.25%

■ Points achieved ▨ Opportunity

Actions to review

Regressed	To address	Planned	Risk accepted	Recently added	Recently updated
0	14	0	0	0	0

Top improvement actions

Improvement action	Score impact	Status	Category
Ensure all users can complete multi-factor authentication for secure ac...	+12.5%	○ To address	Identity
Require MFA for administrative roles	+13.89%	○ To address	Identity
Turn on user risk policy	+9.72%	○ To address	Identity
Turn on sign-in risk policy	+9.72%	○ To address	Identity
Do not allow users to grant consent to unmanaged applications	+5.56%	○ To address	Identity
Set automated notifications for new OAuth applications connected to ...	+5.56%	○ To address	Apps
Set automated notifications for new and trending cloud applications in...	+4.17%	○ To address	Apps
Use Cloud App Security to detect anomalous behavior	+4.17%	○ To address	Apps

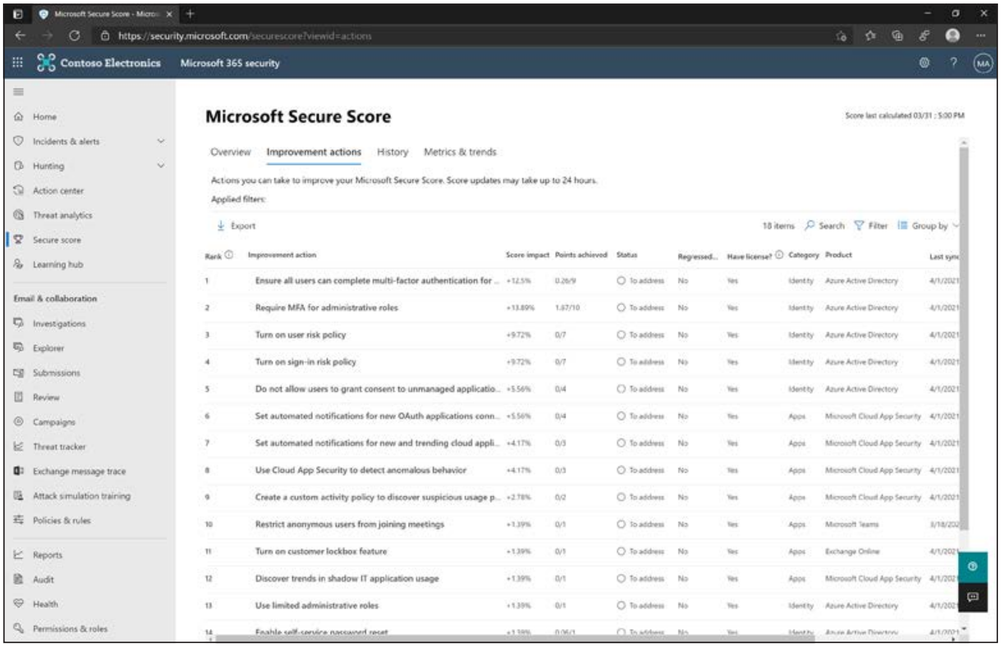
FIGURE 2-1 Microsoft Secure Score overview

Managing improvement actions

To increase the Secure Score in the tenant, you must take additional action for the various settings or features in identity, device, or apps. To see the list of improvement actions for your organization specifically, check the **Improvement actions** tab of Secure Score. Figure 2-2 shows the improvement actions that are available for the Contoso Electronics organization.

A variety of information is displayed for each improvement action that you can take in the organization. Some of the relevant columns for identifying how the improvement action changes the Secure Score are noted in these columns:

- **Score impact** The percentage that the Secure Score will increase upon completing the action
- **Points achieved** The numerical points that are added to your Secure Score by completing the action
- **Status** The status of the action. Possible values are *Alternate mitigation*, *Completed*, *Planned*, *Risk accepted*, *Third party*, or *To address*
- **Regressed in last 90 days** Whether the improvement action has been negatively impacted in the last 90 days by a configuration change
- **Have license?** Displays if the organization already has the required license to make the recommended change



Microsoft Secure Score

Score last calculated 03/31 ; 5:00 PM

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Applied filters:

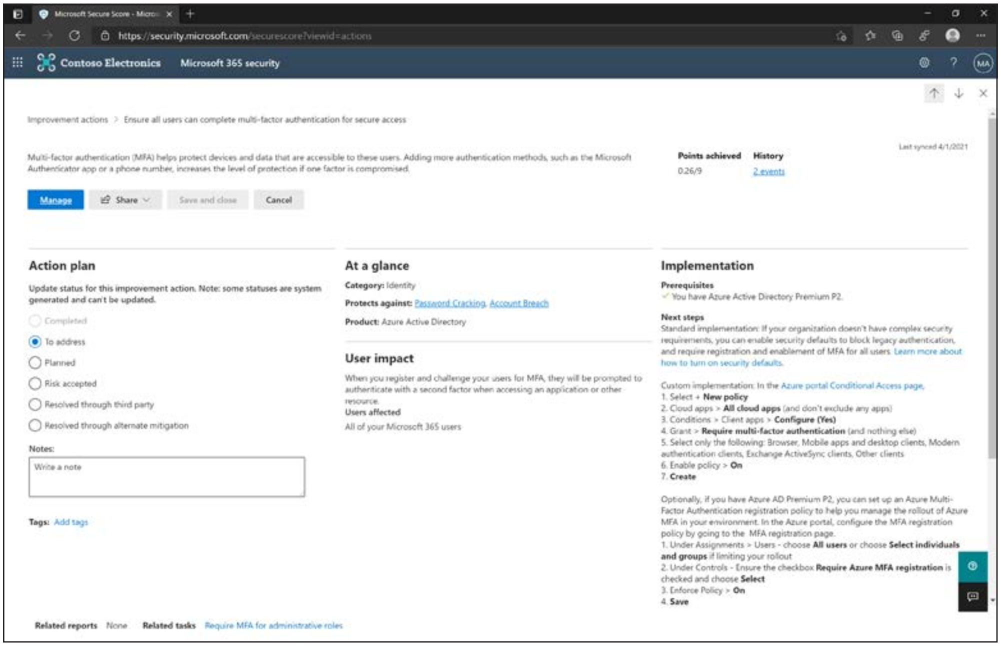
Rank	Improvement action	Score impact	Points achieved	Status	Regressed...	Have license?	Category	Product	Last sync
1	Ensure all users can complete multi-factor authentication for ...	+12.5%	0.26/9	○ To address	No	Yes	Identity	Azure Active Directory	4/1/2021
2	Require MFA for administrative roles	+13.89%	1.87/10	○ To address	No	Yes	Identity	Azure Active Directory	4/1/2021
3	Turn on user risk policy	+9.72%	0/7	○ To address	No	Yes	Identity	Azure Active Directory	4/1/2021
4	Turn on sign-in risk policy	+9.72%	0/7	○ To address	No	Yes	Identity	Azure Active Directory	4/1/2021
5	Do not allow users to grant consent to unmanaged applicatio...	+5.56%	0/4	○ To address	No	Yes	Identity	Azure Active Directory	4/1/2021
6	Set automated notifications for new OAuth applications conn...	+5.56%	0/4	○ To address	No	Yes	Apps	Microsoft Cloud App Security	4/1/2021
7	Set automated notifications for new and trending cloud appli...	+4.17%	0/3	○ To address	No	Yes	Apps	Microsoft Cloud App Security	4/1/2021
8	Use Cloud App Security to detect anomalous behavior	+4.17%	0/3	○ To address	No	Yes	Apps	Microsoft Cloud App Security	4/1/2021
9	Create a custom activity policy to discover suspicious usage p...	+2.78%	0/2	○ To address	No	Yes	Apps	Microsoft Cloud App Security	4/1/2021
10	Restrict anonymous users from joining meetings	+1.39%	0/1	○ To address	No	Yes	Apps	Microsoft Teams	3/18/202
11	Turn on customer lockbox feature	+1.39%	0/1	○ To address	No	Yes	Apps	Exchange Online	4/1/202
12	Discover trends in shadow IT application usage	+1.39%	0/1	○ To address	No	Yes	Apps	Microsoft Cloud App Security	4/1/202
13	Use limited administrative roles	+1.39%	0/1	○ To address	No	Yes	Identity	Azure Active Directory	4/1/202
14	Enable self-service password reset	+1.39%	0.06/1	○ To address	No	Yes	Identity	Azure Active Directory	4/1/2021

FIGURE 2-2 Microsoft Secure Score improvement actions

To manage an individual improvement action, click the action from the improvement actions tab. Each action has similar information that is displayed on the main tab. From the individual action, you can configure an **Action plan**, which changes the *Status* column on the previous page. The available settings for Action plan are *To address*, *Planned*, *Risk accepted*, *Resolved through third party*, and *Resolved through alternate mitigation*.

The Implementation section of the improvement action lists any prerequisites, such as licensing, as well as the general steps to customize and configure the desired state for that action. Figure 2-3 shows the management screen of an individual improvement action.

On the main Secure Score page, the History tab displays a line chart with the Secure Score history of the tenant. The History tab also shows a list of changes that have been made in the tenant with the resulting positive or negative point score change. You can also filter or search through the list of recent changes on the History tab. By default, the results show the past 90 days, but can be changed to 7 days, 30 days, or a custom date range. Other filter options include whether the change was an increase, regression, or no points change; the category of the change, the product the change was made in, the type of update that was made, and any tags that might have been associated with the change. Figure 2-4 shows the History tab with the default filtering options.


Microsoft Secure Score - Micro
https://security.microsoft.com/securescore?viewid=actions
Contoso Electronics
Microsoft 365 security
MA
Manage
Share
Save and close
Cancel

Improvement actions > Ensure all users can complete multi-factor authentication for secure access

Multi-factor authentication (MFA) helps protect devices and data that are accessible to these users. Adding more authentication methods, such as the Microsoft Authenticator app or a phone number, increases the level of protection if one factor is compromised.

Points achieved	History
0.26/9	2 events

Last synced 4/1/2021

Action plan

Update status for this improvement action. Note: some statuses are system generated and can't be updated.

○ Completed
● To address
○ Planned
○ Risk accepted
○ Resolved through third party
○ Resolved through alternate mitigation

Notes:
Write a note

Tags: Add tags

At a glance

Category: Identity

Protects against: Password Cracking, Account Breach

Product: Azure Active Directory

User impact

When you register and challenge your users for MFA, they will be prompted to authenticate with a second factor when accessing an application or other resource.

Users affected

All of your Microsoft 365 users

Implementation

Prerequisites
✓ You have Azure Active Directory Premium P2.

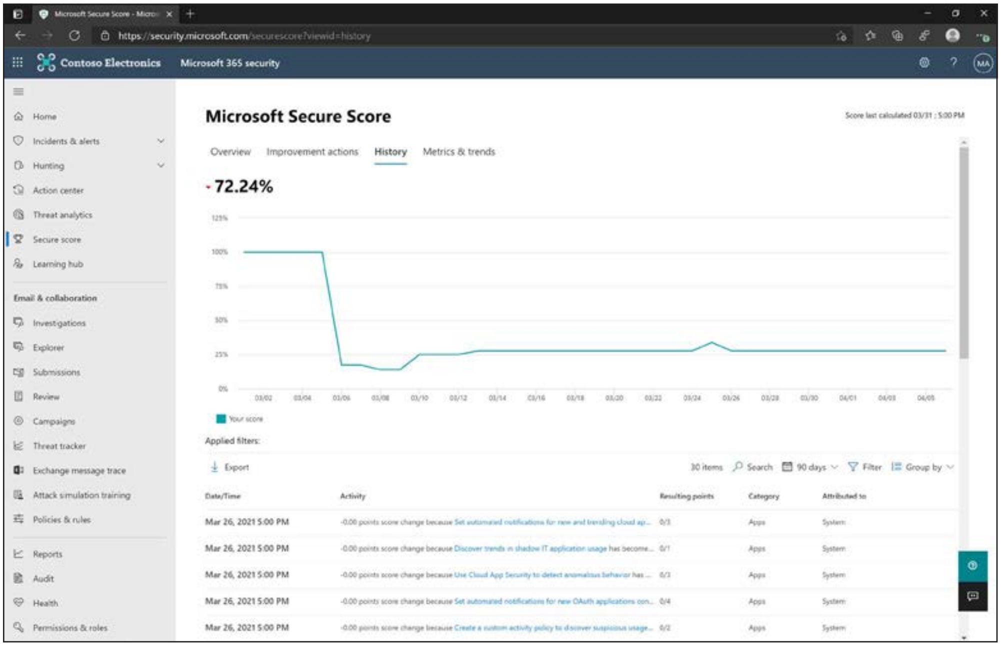
Next steps
Standard implementation: If your organization doesn't have complex security requirements, you can enable security defaults to block legacy authentication, and require registration and enablement of MFA for all users. Learn more about how to turn on security defaults.

Custom implementation: In the Azure portal Conditional Access page,
1. Select + **New policy**
2. Cloud apps > **All cloud apps** (and don't exclude any apps)
3. Conditions > Client apps > **Configure (Yes)**
4. Grant > **Require multi-factor authentication** (and nothing else)
5. Select only the following: Browser, Mobile apps and desktop clients, Modern authentication clients, Exchange ActiveSync clients, Other clients
6. Enable policy > **On**
7. **Create**

Optionally, if you have Azure AD Premium P2, you can set up an Azure Multi-Factor Authentication registration policy to help you manage the rollout of Azure MFA in your environment. In the Azure portal, configure the MFA registration policy by going to the MFA registration page.
1. Under Assignments > Users - choose **All users** or choose **Select individuals and groups** if limiting your rollout
2. Under Controls - Ensure the checkbox **Require Azure MFA registration** is checked and choose **Select**
3. Enforce Policy > **On**
4. **Save**

Related reports None **Related tasks** Require MFA for administrative roles

FIGURE 2-3 Microsoft Secure Score improvement action management



Microsoft Secure Score

Score last calculated 03/31 : 5:00 PM

72.24%

Applied filters:

Date/Time	Activity	Resulting points	Category	Attributed to
Mar 26, 2021 5:00 PM	-0.00 points score change because Set automated notifications for new and trending cloud ap...	0/3	Apps	System
Mar 26, 2021 5:00 PM	-0.00 points score change because Discover trends in shadow IT application usage has become...	0/1	Apps	System
Mar 26, 2021 5:00 PM	-0.00 points score change because Use Cloud App Security to detect anomalous behavior has ...	0/3	Apps	System
Mar 26, 2021 5:00 PM	-0.00 points score change because Set automated notifications for new OAuth applications con...	0/4	Apps	System
Mar 26, 2021 5:00 PM	-0.00 points score change because Create a custom activity policy to discover suspicious usage...	0/2	Apps	System

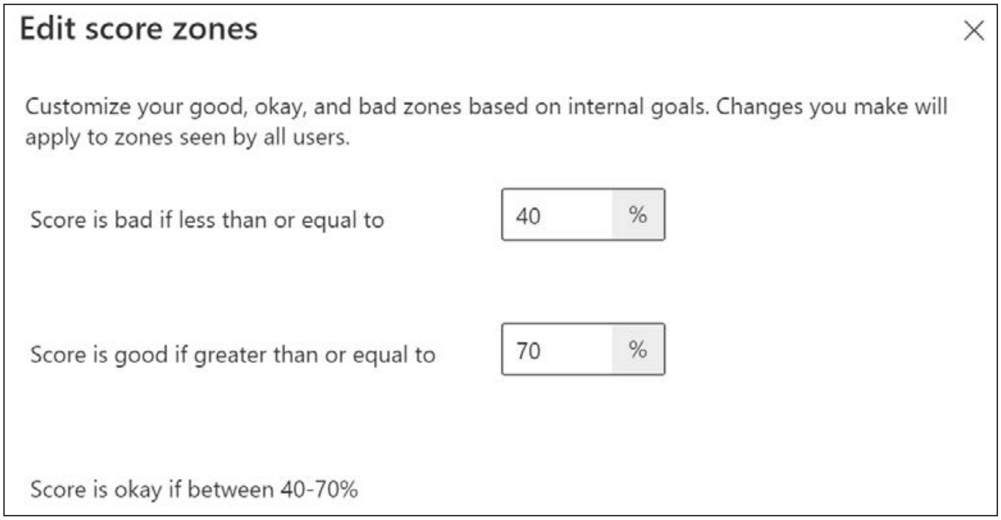
FIGURE 2-4 Microsoft Secure Score History

The final tab that is available with Secure Score is the Metrics & trends tab, which displays Secure Score changes, custom Secure Score zones, and trends in the environment for regression, risk acceptance, and a comparison to other organizations that are similar in size, industry, and the products that are licensed.

The Secure Score zones are a minimum and maximum percentage that you can set to display a chart that displays your score as bad, okay, or good relative to your current score. To create a custom zone, use the following steps.

1. Sign in to the Microsoft 365 security center at *https://security.microsoft.com*.
2. From the Navigation bar on the left, click **Secure score**.
3. On the Secure Score page, click **Metrics & trends**.
4. On the Metrics & trends tab, click **Add score zones**.
5. In the flyout window, customize the **Score is bad if less than or equal to and Score is good if greater than or equal to** fields, and then click **Save and close**.

Figure 2-5 shows the fields set to 40% and 70% respectively. This means that a bad score would be less than or equal to 40%, an okay score is in the 41% to 69% range, and a good score is greater than or equal to 70%.



Edit score zones

Customize your good, okay, and bad zones based on internal goals. Changes you make will apply to zones seen by all users.

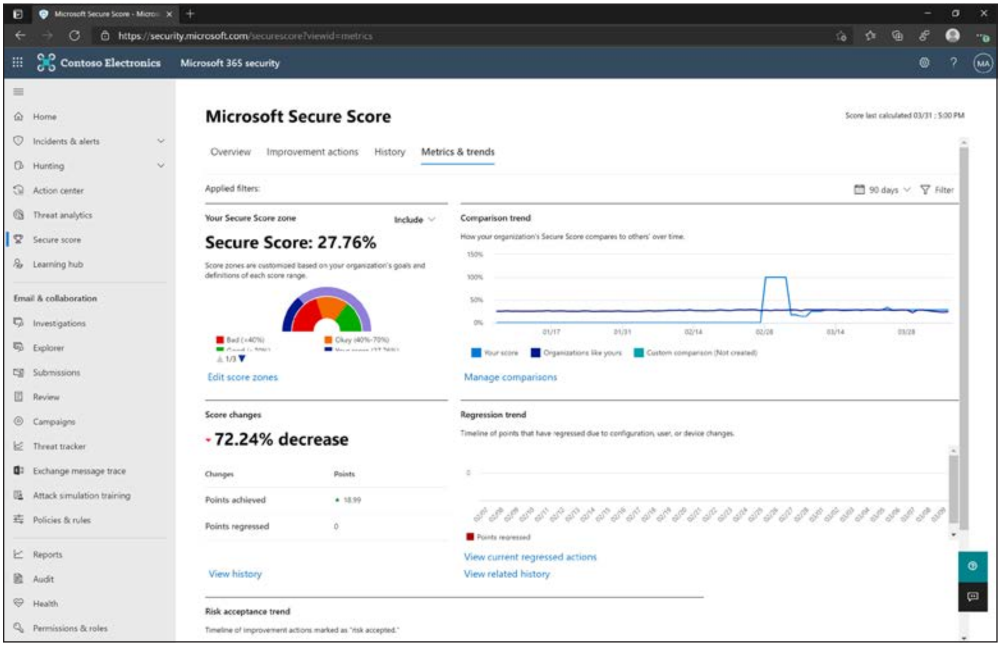
Score is bad if less than or equal to 40 %

Score is good if greater than or equal to 70 %

Score is okay if between 40-70%

FIGURE 2-5 Custom Secure Score zones

After you save the custom zone, the Metrics & trends page will update with a chart displaying where your tenant is on the scale that you created. Figure 2-6 shows the Metrics & trends page with a custom zone created, Secure Score changes, and the comparison and regression trends.



Microsoft Secure Score

Score last calculated 03/31 : 5:00 PM

Applied filters:

Your Secure Score zone

Secure Score: 27.76%

Score zones are customized based on your organization's goals and definitions of each score range.

Comparison trend

How your organization's Secure Score compares to others' over time.

Score changes

72.24% decrease

Changes	Points
Points achieved	18.99
Points regressed	0

Regression trend

Timeline of points that have regressed due to configuration, user, or device changes.

Risk acceptance trend

Timeline of improvement actions marked as "risk accepted."

FIGURE 2-6 Secure Score Metrics & trends

To manage the comparison chart, click Manage comparisons on the Metrics & trends page. This will open another flyout window where you can set a custom comparison. The fields for a custom comparison are:

- **Industries** The industries that you would like to compare with, for example, Manufacturing or Healthcare.
- **Organization size** The size of the organization relative to the number of users being managed.
- **Licenses** The licenses that are included in the organization.
- **Regions** The geographic region of other organizations to compare with.

If you configure these options and click Save and close, the line chart on the Metrics & trends page will update with your custom settings. The line chart displays three lines, for Your score, organizations like yours, and your custom comparison.

The other charges that are displayed on the Metrics & trends for regression and risk acceptance are relative to the actions that have been taken in your specific environment. Actions that have resulted in a negative change to your Secure Score are displayed in the Regression trend chart. Improvement actions that have been marked as *Risk accepted* are displayed in the Risk Acceptance trend. You can also view the individual actions that were taken in either scenario if you need to review or report on when and why those actions were taken.

Required permissions

To have permissions to manage improvement actions, create custom score zones, or edit the custom comparisons, you must have a role that includes read and write access to Secure Score. The built-in roles that include read and write access are:

- **Global administrator**
- **Security administrator**
- **Exchange administrator**
- **SharePoint administrator**
- **Account administrator**

For accounts that only need read access to the Secure Score and the customizations that an administrator has made, you can assign any of the following roles:

- **Helpdesk administrator**
- **User administrator**
- **Service administrator**
- **Security reader**
- **Security operator**
- **Global reader**

It is also important to note that the Secure Score is simply a numerical value that represents the security posture of the current configuration in the organization. It is not guaranteed measure of how secure the organization might be. No online service is completely protected from security breaches, and a high or even 100% completion of Secure Score should not be interpreted as such.

Manage incident investigation

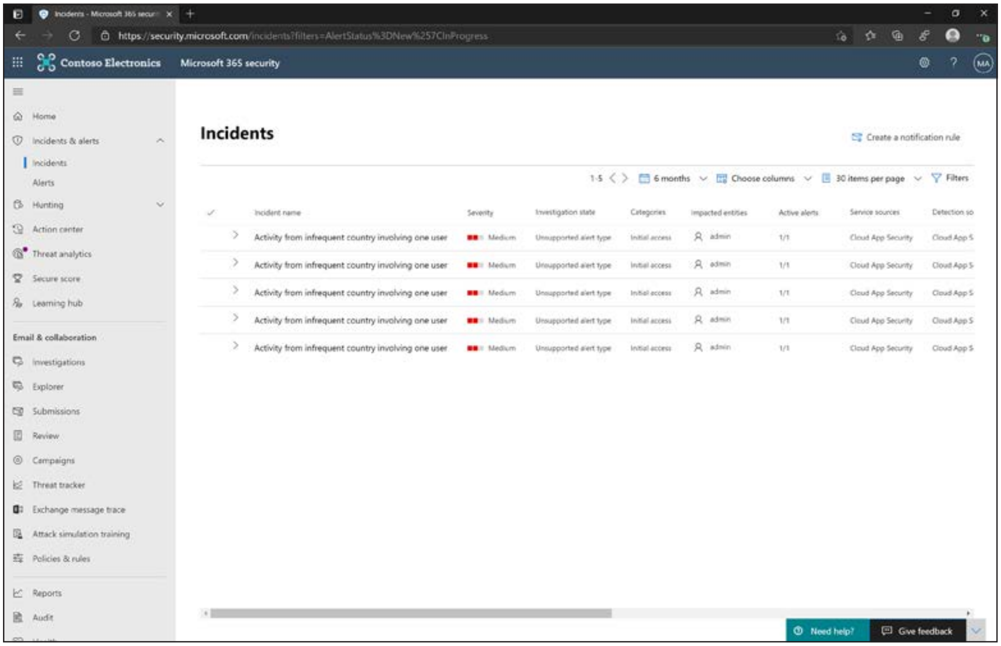
Incidents are triggered by alerts that correspond to a suspicious or malicious event that has occurred in the organization. We can look at incident response with two categories: manual investigation and automated investigation. In a large organization, there could be thousands of alerts at any given time that might require additional investigation. Some might be handled automatically, and others might require additional administrative input. In this section, we'll look at both investigation types.

Manual incident investigations

The Microsoft 365 security center includes an incidents queue, which displays any incidents that have occurred in the organization. The incidents queue can help you sort, filter, and prioritie the alerts and incidents that require additional actions to review and resolve the incident as either a *False alert* or a *True alert*. To open the incident queue, follow these steps.

1. Sign in to the Microsoft 365 security center at *https://security.microsoft.com*.
2. From the Navigation bar on the left, expand **Incidents & alerts**, and then click **Incidents**.

Figure 2-7 displays the incidents that have been identified in the Contoso Electronics organization.



Incidents

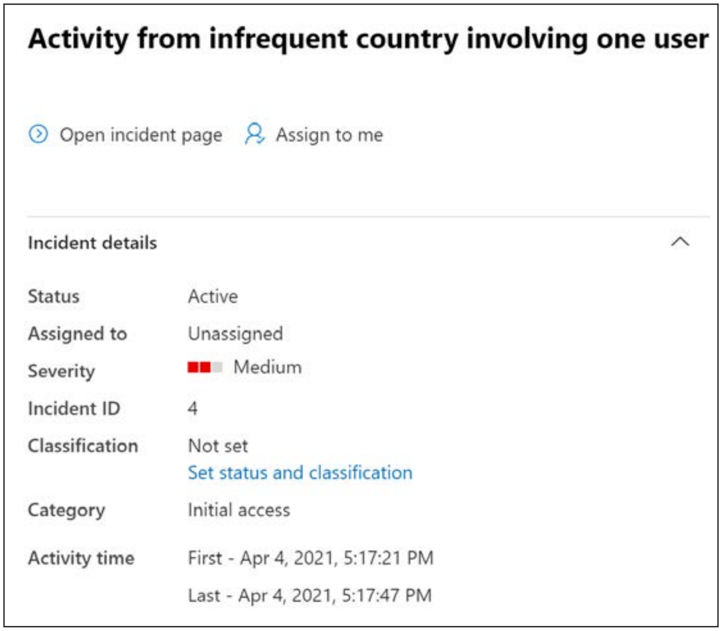
Incident name	Severity	Investigation state	Categories	Impacted entities	Active alerts	Service sources	Detection so
Activity from infrequent country involving one user	Medium	Unsupported alert type	Initial access	admin	1/1	Cloud App Security	Cloud App S
Activity from infrequent country involving one user	Medium	Unsupported alert type	Initial access	admin	1/1	Cloud App Security	Cloud App S
Activity from infrequent country involving one user	Medium	Unsupported alert type	Initial access	admin	1/1	Cloud App Security	Cloud App S
Activity from infrequent country involving one user	Medium	Unsupported alert type	Initial access	admin	1/1	Cloud App Security	Cloud App S
Activity from infrequent country involving one user	Medium	Unsupported alert type	Initial access	admin	1/1	Cloud App Security	Cloud App S

FIGURE 2-7 Microsoft 365 security center incident queue

The incident queue has a variety of columns that display relevant information for each incident that has outstanding actions. Some of these columns include:

- **Severity** The severity of the incident, categorized as informational, low, medium, or high.
- **Investigation state** Displays the alert type that the incident relates to.
- **Categories** The category that the incident relates to.
- **Impacted entities** The user accounts, devices, or other entity that the alert corresponds to.
- **Active alerts** The number of alerts that are still active that correspond to the incident. One incident could have multiple alerts that correspond to the same event.
- **Service sources** The Microsoft 365 service that the incident has potentially impacted.

To view more information about the incident, click the checkmark next to the name of the incident, without clicking the name itself. This will open a flyout window that displays more information about the incident, including the classification, activity times, and buttons to open the full incident page or assign the incident to your user account. Figure 2-8 displays a portion of the information from the flyout window.



Activity from infrequent country involving one user

Incident details

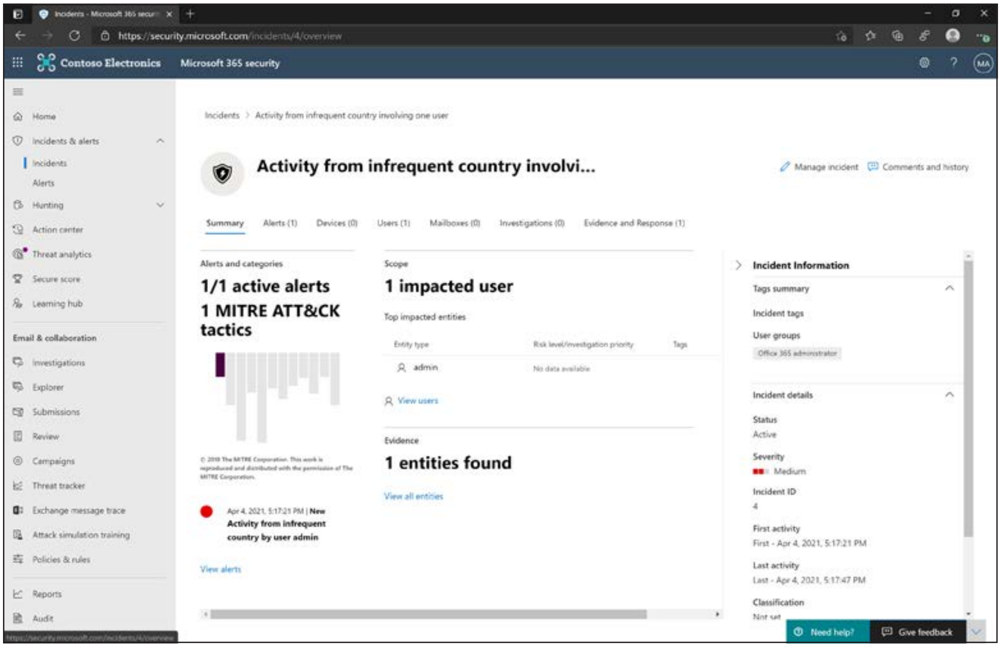
Status	Active
Assigned to	Unassigned
Severity	■■□ Medium
Incident ID	4
Classification	Not set Set status and classification
Category	Initial access
Activity time	First - Apr 4, 2021, 5:17:21 PM Last - Apr 4, 2021, 5:17:47 PM

FIGURE 2-8 Incident information

To view even more information, or to begin managing the properties of the incident, click the name of the incident or the **Open incident page** link. Every incident can be managed individually, and has a variety of tabs that display more information around the incident and alert. These tabs include

- **Summary** Displays the basic information about the incident and alert, including the MITRE ATT&CK tactics, impacted user accounts, and incident information.
- **Alerts** The alert(s) that was generated from the services as they relate to the overall incident.
- **Devices** Any impacted devices if the alert or incident occurred on a device that is being managed by the organization.
- **Users** The impacted user accounts that have been associated with the incident.
- **Mailboxes** Any Exchange Online mailboxes that might also be associated with the incident.
- **Investigations** Any automated investigation that occurred with the incident.
- **Evidence and response.** A summary of the evidence that relates to the alerts that were generated.

Depending on the incident and alert type, not all of these tabs might have information as it relates to the incident. Figure 2-9 shows the incident summary page for an alert related to user activity, but was not associated with a device or investigated automatically.



Activity from infrequent country involvi...

Alerts and categories

1/1 active alerts

1 MITRE ATT&CK tactics

© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

Apr 4, 2021, 5:17:21 PM | **New**
Activity from infrequent country by user admin

Scope

1 impacted user

Top impacted entities

Entity type	Risk level/investigation priority	Tags
admin	No data available	

Evidence

1 entities found

Incident Information

Tags summary

Incident tags

User groups

Office 365 administrator

Incident details

Status
Active

Severity
Medium

Incident ID
4

First activity
First - Apr 4, 2021, 5:17:21 PM

Last activity
Last - Apr 4, 2021, 5:17:47 PM

Classification
Not set

FIGURE 2-9 Incident summary

To manage the properties of the incident, click the **Manage incident** link from the summary tab. This will open a flyout window where you can change the properties of the incident, including:

- **Name** You can change the display name of the incident from the default provided.
- **Incident tags** Custom tags that can be assigned to the incident for reporting and tracking.
- **Assign to me** A toggle to assign the incident to your user account for further investigation or management.
- **Resolve incident** A toggle that marks whether the incident has been resolved and does not require further investigation.
- **Classification** The classification value for the incident, which could be *Not set*, *False alert*, or *True alert*.
- **Comment** A free text field that can be used to track investigation comments for later reporting or other administrators.

EXAM TIP

When you set the classification at the incident level, it will also be applied on the individual alerts that have been linked to the incident.

Automated incident investigations

If your organization is using Microsoft 365 Defender, you can take advantage of having a built-in analyst for the alerts and incidents that might occur in your environment. The automated investigation and remediation that is included with Microsoft 365 Defender provides some automated capabilities around for each alert, including:

- Determining if an alert requires additional actions
- Recommending or taking remeditation actions
- Determining if additional investigation should occur

When an alert is generated and creates an incident, the automated investigation can come to a vedict about the alert. The three verdicts of an investigation are:

- Malicious
- Suspicious
- No threats found

If an alert is found to be malicious or suspicious, some automatic remediation steps might be performed. Some of the more common actions include:

- Sending a file to quarantine
- Stopping a process on a managed device
- Isolating a device from the network
- Blocking a URL from being accessed

NEED MORE REVIEW? **REMEDIATION ACTIONS**

For more information on the possible remediation actions with Microsoft 365 Defender, visit *https://docs.microsoft.com/en-us/microsoft-365/security/defender/m365d-remediation-actions?view=o365-worldwide.*

To configure automated investigation and response, there are a few prerequisites that the organization must meet to enable this configuration. Table 2-1 explains the various requirements for the tenant.

After you have verified that your organization meets the requirements, you can set the automation level for device groups. To configure the automation level, follow these steps.

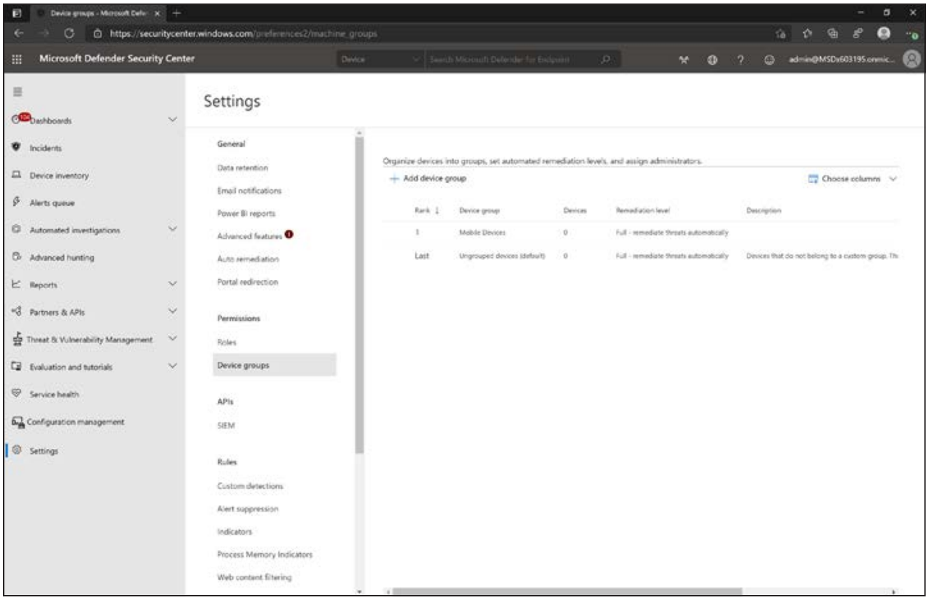
1. Sign in to the Microsoft 365 Defender security center at *https://securitycenter.windows.com.*
2. Go to **Settings**.

TABLE 2-1 Automated investigation and response requirements

Requirement	Details
Subscription and license type	One of the following subscription and license types: ■ Microsoft 365 A5 ■ Microsoft 365 E5 ■ Microsoft 365 A5 Security ■ Microsoft 365 E5 Security ■ Office 365 E5 with Enterprise Mobility + Security E5, and Windows E5
Network requirements	■ Microsoft Defender for Identity enabled ■ Microsoft Cloud App Security configured ■ Microsoft Defender for Identity integration configured
Windows device requirements	■ Windows 10, version 1709 or later ■ Microsoft Defender for Endpoint ■ Micosoft Defender Antivirus
Protection for email content and Office files	■ Microsoft Defender for Office 365 configured
Permissions	■ Global Administrator ■ Security Administrator

3. Under **Permissions**, click **Device groups**.

4. For each device group, set the desired *Remediation level*. For example, the recommended setting is *Full – remediate threads automatically*. Figure 2-10 shows the setting configured for the Mobile Devices device group.



Organize devices into groups, set automated remediation levels, and assign administrators.

Rank	Device group	Devices	Remediation level	Description
1	Mobile Devices	0	Full - remediate threats automatically	
Last	Ungrouped devices (default)	0	Full - remediate threats automatically	Devices that do not belong to a custom group. Th

FIGURE 2-10 Microsoft Defender Security Center remediation level

Automated investigations appear in the Investigations tab of the incident. From this tab, you can view the conclusions and actions that the investigation resulted in.

NEED MORE REVIEW? **AUTOMATED INVESTIGATION**

For more information and a video on automated investigation and self-healing, visit *https://docs.microsoft.com/en-us/microsoft-365/security/defender/m365d-autoir?view=o365-worldwide*.

Manage and review security alerts

In this section we work with alerts in the Office 365 Security & Compliance Center. The alerts available in this portal deal with user, administrator, and general Office 365 activity. These alerts are based on information contained in the Office 365 audit log. While you can review the audit logs to retrieve this information, creating an alert policy can ensure that you are notified about critical events. There are a handful of pre-defined alert policies that cover major events, such as a user account being elevated to Exchange administrator. New alert policies can also be created by an administrator to provide additional visibility around the Office 365 platform.

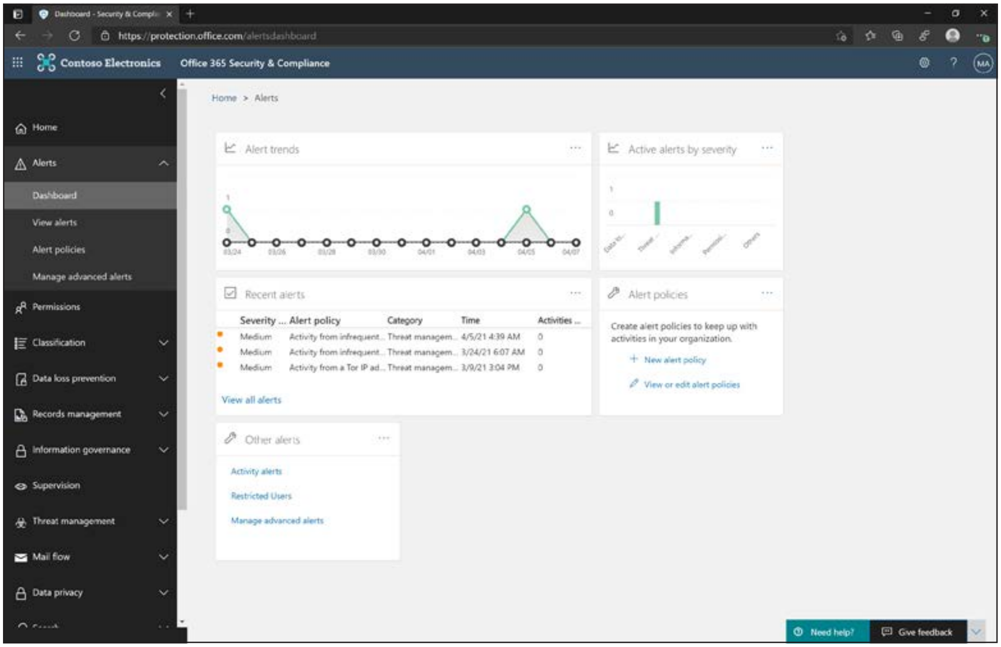
Plan for Office 365 alerts

Before you begin working with alerts in the Office 365 Security & Compliance Center, there are a few planning considerations that you need to be familiar with. These are the prerequisites for accessing managing Office 365 alerts.

- **Permissions** The administrator that will be creating managing alerts must be granted the Organization Configuration role in the Office 365 Security & Compliance Center. This role is automatically granted to members of the Compliance Administrator and Organization Management role groups.
- **Audit logging** Before you can start creating alerts, audit logging needs to be enabled for Office 365. Office 365 alerts are based on the information contained in the audit logs. To do this, navigate to the Office 365 Security & Compliance Center, select **Alerts**, then **Alert policies**. Select any one of the built-in alerts. On the alert policies settings you will be prompted to turn on auditing if it is not already enabled. Beyond these hard requirements, you should also create an action plan for implementation. This might include items such as who will be administering Office 365 alerts, who should be receiving notifications, and what items you need to create policies for.

Navigate Office 365 alerts

The alerts for Office 365 are visible in a few different formats, similar to the reports we saw with Azure AD Identity Protection. The first page we will look at is the Alerts dashboard. This can be accessed by signing in to the Office 365 Security & Compliance Center, clicking Alerts, and selecting Dashboard. Refer to Figure 2-11 for an example of what to expect when you access the dashboard. There are a few different resources available in this view.



Severity ...	Alert policy	Category	Time	Activities ...
Medium	Activity from infrequent...	Threat managem...	4/5/21 4:39 AM	0
Medium	Activity from infrequent...	Threat managem...	3/24/21 6:07 AM	0
Medium	Activity from a Tor IP ad...	Threat managem...	3/9/21 3:04 PM	0

FIGURE 2-11 Office 365 Alerts Dashboard

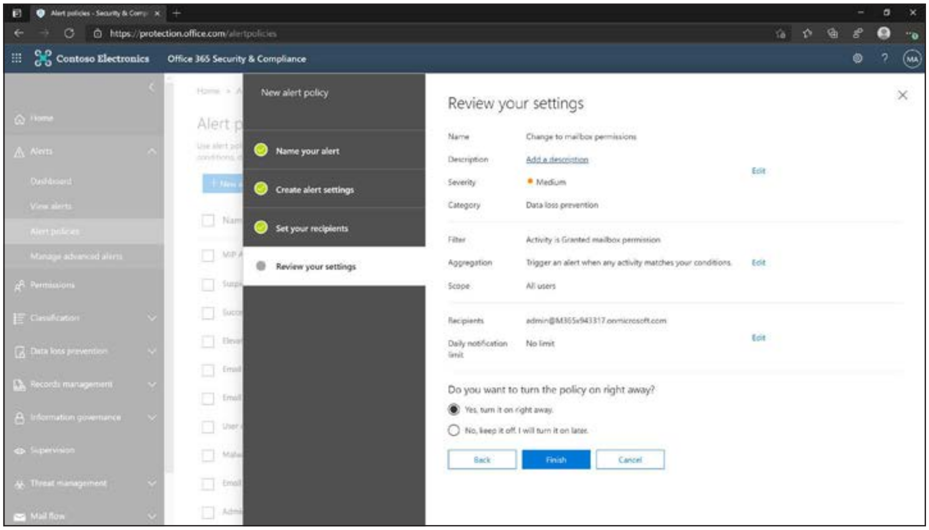
- **Alert Trends** The Alert Trends tile shows recent activity by count for each of the different alert categories. Hovering your mouse cursor over the report tile will summarize event accounts for each category. This tile does not have a drilldown view.
- **Active Alerts By Severity** The Active Alerts By Severity tile provides summarizes active alerts by category and severity (low, medium, high). Hovering your mouse cursor over the report tile will summarize the event counts by severity. This tile does not have a drilldown view.
- **Recent Alerts** The Recent Alerts tile provides a list of recent alerts, including Severity, Alert Policy, Category, Time, and Number Of Activities. Clicking any of the events on this tile will bring up a blade with additional details about the event. From there you can see additional information about that specific event. You also have controls to resolve, suppress, or notify users about the alert.
- **Alert Policies** The Alert Policies tile provides helpful links to quickly create a new alert policy or manage the existing policies.
- **Other Alerts** The Other Alerts tile provides helpful links to quickly create activity-based alerts, view restricted user accounts, and access advanced alert management.

It is worth noting that each of these tiles can also be pinned to the Office 365 Security & Compliance Center home page for quick reference. For situations where you need to browse all alerts, navigate to **Alerts**, then **View Alerts**. This page provides you with functionality to quickly filter all alerts, including those that have been resolved. Once you have isolated the alerts you need, you can also export them to CSV format from this page.

Configure Office 365 alert policies

The policy editor for Office 365 alerts enables you to create and manage additional custom alert policies. Through this interface you have access to all of the activities logged through auditing. In the following example we will walk through creating a policy that generates an alert when a user's mailbox permissions are modified.

1. Sign in to the Office 365 Security & Compliance Center at *https://protection.office.com*.
2. From the Navigation bar on the left, click **Alerts** and select **Alert Policies**.
3. On the Alert policies page, click **New Alert Policy**.
4. On the Name Your Alert page, fill in the following information and click **Next**.
   - **Name** Change to mailbox permissions.
   - **Description** Generate an alert when mailbox permissions are modified.
   - **Severity** Medium.
   - **Category** Data loss prevention.
5. On the Create alert settings page, fill in the following information and click **Next**.
   - **Activity Is** Granted mailbox permission.
   - **How Do You Want The Alert To Be Triggered?** Every time an activity matches the rule.
6. On the Set your recipients page, fill in the following information and click **Next**.
   - **Email Recipients** Your email address.
   - **Daily Notification Limit** No limit.
7. On the Review your settings page, review the proposed policy as shown in Figure 2-12. Select the option **Yes, Turn It On Right Away** and click **Finish**.



Review your settings

Name Change to mailbox permissions

Description Add a description

Severity ● Medium

Category Data loss prevention

Edit

Filter Activity is Granted mailbox permission

Aggregation Trigger an alert when any activity matches your conditions. Edit

Scope All users

Recipients admin@M365x943317.onmicrosoft.com

Daily notification limit No limit

Edit

Do you want to turn the policy on right away?

● Yes, turn it on right away.

○ No, keep it off. I will turn it on later.

Back | Finish | Cancel

FIGURE 2-12 Office 365 Alerts - Alert Policy

Index

NUMBERS

32-bit to 64-bit, Windows 10 Enterprise deployment, 54

A

access controls, device compliance, 14–15

Active Directory Rights Management Services (AD RMS), 176

AD RMS (Active Directory Rights Management Services), 176

AIP (Azure Information Protection)

- classification and labeling, 179
- deploying unified labeling client, 185
- features, 178
- implementing policies, 179–183
- IRM (Information Rights Management) for workloads, 186
- keys, 179
- label alerts and analytics, 183–186
- labeling client, 185
- licensing, 177–178
- overview, 176
- planning for, 178–179
- policies, 179–183
- prerequisites, 177
- reporting in, 184
- scanner, 182
- users and groups, 178
- WIP (Windows Information Protection), 187–192

alerts

- False versus True, 88
- managing and reviewing, 209–201
- managing by type, 139

Alerts Dashboard, 95

Amazon Web Services (AWS), Microsoft Cloud App Security, 124

Android

- device compliance use cases, 12
- Microsoft Defender for Endpoint, 99

anti-malware policies, Microsoft Defender for Endpoint, 111–114

anti-phishing policies, Microsoft Defender for Endpoint, 103–107

anti-spam policies, Microsoft Defender for Endpoint, 107–111

apps. *See also* Microsoft Cloud App Security; mobile application management

- assigning in Intune, 39–40
- Microsoft Store for Business (MSfB), 25–33
- planning deployment, 34–40
- planning for, 24–25
- protection policies, 40–44

assessment templates, 152–154

assignment controls, 40

assignments, device compliance, 13

attack surface reduction, device compliance, 18–20

audit logging and alerts, 94

auditing, planning for, 209–212

AWS (Amazon Web Services), Microsoft Cloud App Security, 124

Azure Active Directory (Azure AD)

- enrolling devices, 70–77
- Premium P2, 1
- subscription tier, 10

subscriptions, 15

Azure Information Protection (AIP)

- classification and labeling, 179
- deploying unified labeling client, 185
- features, 178
- implementing policies, 179–183
- IRM (Information Rights Management) for workloads, 186
- keys, 179
- label alerts and analytics, 183–186
- labeling client, 185
- licensing, 177–178
- overview, 176
- planning for, 178–179
- policies, 179–183
- prerequisites, 177
- reporting in, 184
- scanner, 182
- users and groups, 178
- WIP (Windows Information Protection), 187–192

B

backups

- capabilities and limitations, 165–167
- Exchange Online, 165–168
- OneDrive for Business, 166–171
- SharePoint Online, 166–171

BIOS and UEFI, 54

BitLocker, 69

Box app, Microsoft Cloud App Security, 124

C

CB (Current Branch) identifier, 47

Cisco Webex, Microsoft Cloud App Security, 125

client apps, approval of, 18

Cloud App Security. *See* Microsoft Cloud App Security

cloud applications, managing traffic logs, 139–143

cloud apps for actions, device compliance, 14

Cloud Discovery anomaly detection policies, 132–133

compliance. *See also* device compliance

- assessing, 149–152
- industry requirements, 152–154
- legislative requirements, 152–154
- planning solutions, 148–149
- regional requirements, 152–154
- scores, 149–150

conditional access policies, device compliance, 12–18

conditions, device compliance, 14

ConfigMgr (System Center Configuration Manager), 53, 55–56, 61–62

content holds, resource for, 218

Content Search solution, 212, 214. *See also* search and investigation

Current Branch (CB) identifier, 47

D

DAGs (database availability groups), 165

data classification and labeling, 155–158

data governance, 154

data loss prevention (DLP)

- configuring policies, 201–205
- creating policies, 196–201
- customizing rules, 202
- Incidents reports, 207–208
- managing exceptions, 203–205
- monitoring policy matches, 205–208
- overview, 193–194
- policy matches, 205–208
- policy sync process, 195–196
- policy tips, 206

Data Protection Baseline assessment template, 152

data retention labels, designing, 173–176

database availability groups (DAGs), 165

deleted content, restoring, 158–171

device compliance. *See also* compliance

- access controls, 14–15
- assignments, 13
- attack surface reduction, 18–20
- cloud apps for actions, 14
- conditional access policies, 12–18
- conditions, 14
- configuring policies, 22–24
- configuring security baselines, 21–22
- device exemption, 11
- device management, 16
- device platforms, 16
- device-compliance policy, 22–24
- email requirements, 16
- endpoint security profiles, 18–20
- Intune, 8
- Intune enrollment, 11
- permissions, 15
- planning for, 9–18
- platform support, 9–10
- policy assignment, 11
- prerequisites, 9–10
- process flow, 10–11
- requirements to be delivered, 16
- subscriptions, 9–10, 15
- use cases, 12
- users and groups, 13

device enrollment

- Azure Active Directory (Azure AD), 70–71
- deployment profiles, 71–72
- enabling, 71–77
- restrictions, 73–77

device exemption, device compliance, 11

device management, device compliance, 16

device platforms, device compliance, 16

device services. *See also* Windows 10

- app deployment, 34–40
- configuration profiles, 6–8
- Microsoft Endpoint Manager, 4–6
- mobile application management, 40–44
- planning for apps, 24–33
- planning monitoring, 2–3

devices
- Azure Active Directory (Azure AD) enrollment, 70–71
- deployment profiles, 71–72
- enabling enrollment, 71–77
- enrollment restrictions, 73–77

dictionary matches and DLP, 194

disk encryption, Windows 10 Enterprise deployment, 54

DKIM (DomainKeys Identified Mail), Microsoft Defender for Endpoint, 115–116

DLP (data loss prevention)
- configuring policies, 201–205
- creating policies, 196–201
- customizing rules, 202
- Incidents reports, 207–208
- managing exceptions, 203–205
- monitoring policy matches, 205–208
- overview, 193–194
- policy matches, 205–208
- policy sync process, 195–196
- policy tips, 206

Domain-based Message Authentication, Reporting, and Conformance (DMARC), 116

Dropbox, Microsoft Cloud App Security, 125

dual-boot, Windows 10 Enterprise deployment, 54

E

eDiscovery
- advanced features, 220–222
- configuring, 218
- express analysis, 222
- legal holds, 216–218
- licensing options, 214
- permissions, 215–216
- prerequisites, 214–216
- searching, 161
- working with cases, 219–222

EFS (Encrypting File System), 187, 193

Electronic Software Delivery (ESD), 52–53

email requirements, device compliance, 16

Encrypting File System (EFS), 187, 193

endpoint security profiles, device compliance, 18–20

Enterprise Mobility + Security 90-day trial, 1

ESD (Electronic Software Delivery), 52–53

EU GDPR assessment template, 152

Exam Tips
- Advanced eDiscovery, 215
- alerts and incident levels, 91
- assignment controls, 40
- audit logs, 210
- backups, 170
- configuring solutions, 5
- device compliance, 11
- DLP (data loss prevention), 194
- order of steps, 5
- Rights Management Adhoc license, 179

Exchange, Microsoft Cloud App Security, 125

Exchange Online
- backups, 165–168
- and IRM (Information Rights Management), 186
- legal holds, 216
- restoring deleted data in, 158–161

F

False alerts, 88

G

G Suite, Microsoft Cloud App Security, 125

Github, Microsoft Cloud App Security, 125

group policy, modern servicing with, 59–60

H

Historical reports, Microsoft Endpoint Manager, 3

holds, resource for, 217

I

identity and access management, 68

images, Windows 10 Enterprise deployment, 54

incident investigation, managing, 88–94

industry requirements, planning for, 152–154

information governance

- data classification and labeling, 155–158
- Labels tab, 174
- planning for backup, 164–171
- restoring deleted content, 158–164

information protection, 68

information retention, configuring, 171–173

In-Place Hold feature, 166

Insider program. *See* Windows Insider program

insider risk management

- global settings, 223–224
- policies, 224–226
- roles, 223

internal functions and DLP, 194

Intune

- assigning apps in, 39–40
- creating and deploying apps with, 36–40
- device compliance, 8, 11
- managing Store apps with, 36
- security policies, 18
- setting up, 4–6
- Windows 10 update rings, 58–62

investigation. *See* search and investigation

iOS

- device compliance use cases, 12
- Microsoft Defender for Endpoint, 99

ISO 27001:2013 assessment templates, 152

K

keyword matches and DLP, 194

L

labeling and data classification, 155–158

labels, resource for, 175

language packs, Windows 10 Enterprise deployment, 54

legal holds, eDiscovery, 217

legislative requirements, planning for, 152–154

Linux, Microsoft Defender for Endpoint, 99

log collector, deploying, 141

logs, reviewing, 3

Long-Term Servicing Branch (LTSB) identifier, 47–48

LTSB (Long-Term Servicing Branch) identifier, 47–48

M

macOS
  device compliance use cases, 12
  Microsoft Defender for Endpoint, 99
MBR2GPT, running, 54
MDM security baseline, 21
MDT (Microsoft Deployment Toolkit), 53
Microsoft, semi-annual release cycle, 68
Microsoft 365 Defender
  enabling, 2
  remediation actions, 92–93
Microsoft 365 security center, incident investigation, 88–94. *See also* security reports and alerts
Microsoft Cloud App Security. *See also* apps
  access policies, 127–128
  activity policies, 128–130
  alerts, 137–139
  app discovery policies, 130–132
  application connectors, 124–126
  AWS (Amazon Web Services), 124
  Box app, 124
  Cisco Webex, 125
  Cloud Discovery anomaly detection policies, 132–133
  configuring connected apps, 125–126
  configuring file policies, 133–134
  Dropbox, 125
  Exchange, 125
  G Suite, 125
  Github, 125
  information protection, 119–124
  Management Account, 124
  networking, 124
  OAuth (Open Authorization) app policies, 134–135
  Office 365, 125
  Okta, 125
  policies, 127–136
  Salesforce, 125
  ServiceNow, 125
  session policies, 135–136
  unauthorized cloud applications, 139–143
  Workday, 125
Microsoft Defender for Endpoint
  anti-malware policies, 111–114
  anti-phishing policies, 103–107
  anti-spam policies, 107–111
  baseline, 21
  deployment methods, 98–99
  deployment preparation, 99
  DKIM (DomainKeys Identified Mail), 115–116
  licenses, 100
  onboarding, 102–103
  planning, 97
  preferences, 101
  proxy configuration, 102
  requirements, 97
  setting up, 100–102
  Windows 10 security components, 69
Microsoft Defender for Identity, 116–118
Microsoft Defender for Office 365 policies
  anti-malware, 111–114
  anti-phishing, 103–107
  anti-spam, 107, 109–111
  DKIM (DomainKeys Identified Mail), 115–116
  settings, 107–109

Microsoft Deployment Toolkit (MDT), 53

Microsoft Edge baseline, 21

Microsoft Endpoint Manager

- admin center, 3
- configuration profiles, 6–8
- Historical reports, 3
- Intune setup, 4–5
- Operational reports, 3
- Organizations reports, 3
- Specialist reports, 3

Microsoft Office 365, tenant security and Secure Score, 82–88

Microsoft Store for Business (MSfB). *See also* apps; mobile application management

- Benefits page, 32
- Billing & Payments page, 32
- client app types, 35
- configuring, 31–33
- creating and deploying apps with Intune, 36–40
- customization controls, 32–33
- Devices page, 32
- first time sign-in, 29
- getting apps, 30
- Home page, 31
- licensing models, 26–27
- Order History page, 32
- overview, 25
- Partners page, 32
- Permissions page, 32
- prerequisites, 25–27
- private store, 27–30
- Products & Services page, 31–32
- Quotes page, 31
- Settings page, 32
- Support page, 32

mobile application management, 40–44. *See also* apps; MSfB (Microsoft Store for Business)

MSfB (Microsoft Store for Business). *See also* apps; mobile application management

- Benefits page, 32
- Billing & Payments page, 32
- client app types, 35
- configuring, 31–33
- creating and deploying apps with Intune, 36–40
- customization controls, 32–33
- Devices page, 32
- first time sign-in, 29
- getting apps, 30
- Home page, 31
- licensing models, 26–27
- Order History page, 32
- overview, 25
- Partners page, 32
- Permissions page, 32
- prerequisites, 25–27
- private store, 27–30
- Products & Services page, 31–32
- Quotes page, 31
- Settings page, 32
- Support page, 32

N

NIST assessment templates, 152

O

OAuth (Open Authorization) app policies, 134–135
Office 365 app suite, 38–39
Office 365 Business Premium 30-day trial, 1
Office 365, Microsoft Cloud App Security, 125
Okta, Microsoft Cloud App Security, 125
OneDrive for Business
    backups, 166–171
    and IRM (Information Rights Management), 186
    restoring deleted data in, 162–164
OneNote app, registering free copy of, 29–30
Open Authorization (OAuth) app policies, 134–135
operating system support, Windows 10 Enterprise deployment, 63
Operational reports, Microsoft Endpoint Manager, 3
Organizations reports, Microsoft Endpoint Manager, 3
Outlook, restoring deleted data in, 159

P

permissions
    and alerts, 94
    device compliance, 15
    Secure Score, 88
policy assignment, device compliance, 11
purged items, recovering, 159–161

R

recovering purged items, 159–161
regional requirements, planning for, 152–154
regular expression matches and DLP, 194
requirements to be delivered, device compliance, 16
restoring deleted content, 158–171
retention
    capabilities, 172
    labels, 171, 173–176
    limitations, 173
    policies, 171
    prerequisites, 172
reviewing logs, 3

S

Salesforce, Microsoft Cloud App Security, 125
search and investigation. *See also* Content Search solution
    Content Search solution, 212–213
    eDiscovery, 214–222
    insider risk management, 223–226
    overview, 208
    planning for auditing, 209–212
`Search-UnifiedAuditLog` command, 212
Secure Score
    History, 85
    improvement actions, 83–87
    Metrics & trends, 87
    overview, 82–83
    permissions, 88
    zones, 86
security alerts, managing and reviewing, 94–97
security baselines, device compliance, 21–22
security features, Windows 10 Enterprise deployment, 68–69

security reports and alerts, 81–82. *See also* Microsoft 365 security center

Sender Policy Framework (SPF), 116

sensitivity labeling, 155–158

ServiceNow, Microsoft Cloud App Security, 125

servicing plan, Windows 10 Enterprise deployment, 58–62

session policies, Microsoft Cloud App Security, 135–136

SetupDiag diagnostic tool, 58

SharePoint Online

- backups, 166–171
- and IRM (Information Rights Management), 186
- legal holds, 216
- restoring deleted data in, 161–162

snapshot reports, 139–143

Specialist reports, Microsoft Endpoint Manager, 3

SPF (Sender Policy Framework), 116

spoofing, preventing, 116

subscriptions, device compliance, 15

System Center Configuration Manager (ConfigMgr), 53, 55–56, 61–62

T

telemetry settings, Windows 10 Enterprise deployment, 63

threat protection, 68. *See also* Microsoft Defender for Endpoint

traffic logs, managing, 139–143

True alerts, 88

U

UEFI and BIOS, 54

unified audit logs, searching, 210–211

Universal Windows Platform (UWP), 25

upgrade readiness, Windows 10 Enterprise deployment, 62–67

users and groups, device compliance, 13

UWP (Universal Windows Platform), 25

V

VLSC (volume license service center), 55

W

WaaS (Windows as a Service)

- deployment rings, 47
- feature updates, 46
- LTSB (Long-Term Servicing Branch) identifier, 48
- overview, 45–46
- quality updates, 46
- semi-annual channel, 48
- servicing channels, 46–48
- Windows Insider, 47–50

WIM (Windows Imaging Format), 52–53

Windows, Microsoft Defender for Endpoint, 99

Windows 10. *See also* device services

- deployment, 45–51
- device compliance use cases, 12
- in S mode, 68
- WaaS (Windows as a Service), 45–51

Windows 10 Enterprise deployment
  data availability, 63
  offline servicing, 54
  operating system support, 63
  in-place upgrade, 55–58
  planning for, 51–54
  security features, 68–69
  servicing plans, 58–62
  setup command-line options, 55
  telemetry settings, 63
Windows 10 update rings, Intune, 58–62
Windows as a Service (Waas)
  deployment rings, 47
  feature updates, 46
  LTSB (Long-Term Servicing Branch) identifier, 48
  overview, 45–46
  quality updates, 46
  semi-annual channel, 48
  servicing channels, 46–48
  Windows Insider, 47–50
Windows Defender Antivirus, 69
Windows Defender Application Control, 69
Windows Defender Application Guard, 69
Windows Defender Credential Guard, 69
Windows Defender Exploit Guard, 69
Windows Hello for Business, 69
Windows Imaging Format (WIM), 52–53
Windows Information Protection, 69
Windows Insider program, 47–50
Windows Server Update Services (WSUS), 53
Windows to Go, Windows 10 Enterprise deployment, 54
Windows Update for Business (WUfB), 53
WIP (Windows Information Protection), 187–193
Workday, Microsoft Cloud App Security, 125
WSUS (Windows Server Update Services), 53
WUfB (Windows Update for Business), 53