EDUSUM

#1 Online Certification Guide

MICROSOFT MS-500

Microsoft 365 Security Administration Certification Questions & Answers

Exam Summary – Syllabus –Questions

MS-500

Microsoft 365 Certified - Security Administrator Associate

40-60 Questions Exam – 700/1000 Cut Score – Duration of 120 minutes

Table of Contents:

Know Your MS-500 Certification Well:

The MS-500 is best suitable for candidates who want to gain knowledge in the Microsoft 365. Before you start your MS-500 preparation you may struggle to get all the crucial Microsoft 365 Security Administration materials like MS-500 syllabus, sample questions, study guide.

But don't worry the MS-500 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the MS-500 syllabus?
- How many questions are there in the MS-500 exam?
- Which Practice test would help me to pass the MS-500 exam at the first attempt?

Passing the MS-500 exam makes you Microsoft 365 Certified - Security Administrator Associate. Having the Microsoft 365 Security Administration certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

Microsoft MS-500 Microsoft 365 Security Administration Certification Details:

Exam Name	Microsoft 365 Certified - Security Administrator Associate
Exam Code	MS-500
Exam Price	$165 (USD)
Duration	120 mins
Number of Questions	40-60
Passing Score	700 / 1000
Books / Training	**Course MS-500T00-A: Microsoft 365 Security Administration**
Schedule Exam	**Pearson VUE**
Sample Questions	**Microsoft 365 Security Administration Sample Questions**
Practice Exam	**Microsoft MS-500 Certification Practice Exam**

MS-500 Syllabus:

Topic	Details
Implement and manage identity and access (30-35%)	
Secure Microsoft 365 hybrid environments	- plan Azure AD authentication options - plan Azure AD synchronization options - monitor and troubleshoot Azure AD Connect events
Secure Identities	- implement Azure AD group membership - implement password management - configure and manage identity governance
Implement authentication methods	- plan sign-on security - implement multi-factor authentication (MFA) - manage and monitor MFA - plan and implement device authentication methods like Windows Hello - configure and Manage Azure AD user authentication options and self-service password management
Implement conditional access	- plan for compliance and conditional access policies - configure and manage device compliance for endpoint security - Implement and manage conditional access
Implement role-based access control (RBAC)	- plan for roles - configure roles - Audit roles
Implement Azure AD Privileged Identity Management (PIM)	- plan for Azure PIM - assign eligibility and activate admin roles - manage Azure PIM role requests and assignments - monitor PIM history and alerts
Implement Azure AD Identity Protection	- implement user risk policy - implement sign-in risk policy - configure Identity Protection alerts - review and respond to risk events
Implement and manage threat protection (20-25%)	
Implement an enterprise hybrid threat protection solution	- plan a Microsoft Defender for Identity solution - install and configure Microsoft Defender for Identity - monitor and manage Microsoft Defender for Identity
Implement device threat protection	- plan a Microsoft Defender for Endpoint solution - implement Microsoft Defender for Endpoint - manage and monitor Microsoft Defender for Endpoint

Topic	Details
Implement and manage device and application protection	- plan for device and application protection - configure and manage Microsoft Defender Application Guard - configure and manage Microsoft Defender Application Control - configure and manage exploit protection - configure Secure Boot - configure and manage Windows device encryption - configure and manage non-Windows device encryption - plan for securing applications data on devices - implement application protection policies
Implement and manage Microsoft Defender for Office 365	- configure Microsoft Defender for Office 365 - monitor Microsoft Defender for Office 365 - conduct simulated attacks using Attack Simulator
Monitor Microsoft 365 Security with Azure Sentinel	- Plan and implement Azure Sentinel - Configure playbooks in Azure Sentinel - Manage and monitor Azure Sentinel - Respond to threats in Azure Sentinel
Implement and manage information protection (15-20%)	
Secure data access within Office 365	- implement and manage Customer Lockbox - configure data access in Office 365 collaboration workloads - configure B2B sharing for external users
Manage sensitivity labels	- plan a sensitivity label solution - configure Sensitivity labels and policies - configure and use label analytics - use sensitivity labels with Teams, Sharepoint, OneDrive and Office apps
Manage Data Loss Prevention (DLP)	- plan a DLP solution - create and manage DLP policies - create and manage sensitive information types - monitor DLP reports - manage DLP notifications
Implement and manage Microsoft Cloud App Security	- plan Cloud App Security implementation - configure Microsoft Cloud App Security - manage cloud app discovery - manage entries in the Cloud app catalog - manage apps in Cloud App Security - manage Microsoft Cloud App Security - configure Cloud App Security connectors and Oauth apps - configure Cloud App Security policies and templates - review, interpret and respond to Cloud App Security alerts, reports, dashboards and logs

Topic	Details
Manage governance and compliance features in Microsoft 365 (25-30%)	
Configure and analyze security reporting	- monitor and manage device security status using Microsoft Endpoint Manager Admin Center - manage and monitor security and dashboards using Microsoft 365 Security Center - plan for custom security reporting with Graph Security API - use secure score dashboards to review actions and recommendations in the Microsoft 365 security center - configure alert policies
Manage and analyze audit logs and reports	- plan for auditing and reporting - perform audit log search - review and interpret compliance reports and dashboards - configure audit alert policy
Manage data governance and retention	- plan for data governance and retention - review and interpret data governance reports and dashboards - configure retention labels and policies - define data governance event types - define and manage communication compliance policies - configure Information holds - find and recover deleted Office 365 data - configure data archiving - manage inactive mailboxes
Manage search and investigation	- plan for content search and eDiscovery - delegate permissions to use search and discovery tools - use search and investigation tools to perform content searches - export content search results - manage eDiscovery cases
Manage data privacy regulation compliance	- plan for regulatory compliance in Microsoft 365 - review and interpret GDPR dashboards and reports - manage Data Subject Requests (DSRs) - Administer Compliance Manager in Microsoft 365 compliance security center - review Compliance Manager reports - create and perform Compliance Manager assessments and action items

Microsoft MS-500 Sample Questions:

Question: 1

How can you best ensure that your permanent break glass account is not targeted by user risk policy and sign-in risk policy?

a) Ensure your break glass account is synced with an on-premises AD
b) Ensure your break glass account is a cloud-only account
c) Ensure your break glass account has a complex password
d) Ensure your break glass account is excluded from the user risk policy and the sign-in risk policy

Answer: d

Question: 2

What is the minimum number of days that retention settings can be set in relation to Micarosoft Defender ATP?

a) 30 days
b) 60 days
c) 90 days
d) 120 days

Answer: a

Question: 3

You need to enable and configure Windows Defender ATP to meet the security requirements. What should you do?

a) Download and install the Microsoft Monitoring Agent
b) Create the ForceDefenderPassiveMode registry setting
c) Configure port mirroring
d) Run WindowsDefenderATPOnboardingScript.cmd

Answer: a

Question: 4

When enabling Litigation Hold for a user, what will happen if you do not specify a hold duration?

a) The hold will not be enabled.
b) The hold will be enabled with a hold duration of 365 days.
c) The hold will preserve content indefinitely.
d) The hold will be enabled, but will not apply.

Answer: c

Question: 5

You have a Microsoft 365 E5 subscription and 5,000 users. You create several alert policies that are triggered every time activities match rules.
You need to create an alert policy that is triggered when the volume of matched activities becomes unusual. What should you do first?

a) Enable Microsoft Office 365 auditing
b) Enable Microsoft Office 365 analytics
c) Enable Microsoft Office 365 Cloud App Security
d) Deploy a Microsoft Office 365 add-in to all the users

Answer: b

Question: 6

Other than the Security and Compliance Center, where can you also configure DLP policies?

a) Teams Admin Center
b) Exchange Admin Center
c) The Azure Portal
d) The Microsoft 365 Admin Center

Answer: b

Question: 7

Which of the following is not one of the built-in simulated attacks?

a) Spear phishing
b) Brute force password
c) Password spray
d) Whale phishing

Answer: d

Question: 8

How frequently does Azure AD Connect automatically synchronize on-premises AD changes to Azure AD?

a) Every 30 minutes
b) Once an hour
c) Every 20 minutes
d) Every 15 minutes

Answer: a

Question: 9

For up to how many days can the audit log can provide information?

a) 70
b) 30
c) 90
d) 60

Answer: c

Question: 10

After creating a hold in an eDiscovery case, how long will it take for the hold settings to take effect?

a) 48 hours
b) 12 hours
c) 24 hours
d) 96 hours

Answer: c

Study Guide to Crack Microsoft 365 Security Administration MS-500 Exam:

- Getting details of the MS-500 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the MS-500 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the Microsoft provided training for MS-500 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the MS-500 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on MS-500 practice tests is must. Continuous practice will make you an expert in all syllabus areas.