MICROSOFT MS-500

Microsoft 365 Security Administration Certification Questions & Answers

----

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

MS-500

Microsoft 365 Certified - Security Administrator Associate

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

----

Table of Contents:

Discover More about the MS-500 Certification

Are you interested in passing the Microsoft MS-500 exam? First discover, who benefits from the MS-500 certification. The MS-500 is suitable for a candidate if he wants to learn about Microsoft 365. Passing the MS-500 exam earns you the Microsoft 365 Certified - Security Administrator Associate title.

While preparing for the MS-500 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The MS-500 PDF contains some of the most valuable preparation tips and the details and instant access to useful **MS-500 study materials just at one click**.

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 (25-30%)	
Plan and implement identity and access for	- Choose an authentication method to connect to a hybrid environment

Topic	Details
Microsoft 365 hybrid environments	- Plan and implement pass-through authentication and password hash sync - Plan and implement Azure AD synchronization for hybrid environments - Monitor and troubleshoot Azure AD Connect events
Plan and implement identities in Azure AD	- Implement Azure AD group membership - Implement password management, including self-service password reset and Azure AD Password Protection - Manage external identities in Azure AD and Microsoft 365 workloads - Plan and implement roles and role groups - Audit Azure AD
Implement authentication methods	- Implement multi-factor authentication (MFA) by using conditional access policies - Manage and monitor MFA - Plan and implement Windows Hello for Business, FIDO, and passwordless authentication
Plan and implement conditional access	- Plan and implement conditional access policies - Plan and implement device compliance policies - Test and troubleshoot conditional access policies
Configure and manage identity governance	- Implement Azure AD Privileged Identity Management - Implement and manage entitlement management - Implement and manage access reviews
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 (30-35%)	
Secure identity by using Microsoft Defender for Identity	- Plan a Microsoft Defender for Identity solution - Install and configure Microsoft Defender for Identity - Manage and monitor Microsoft Defender for Identity - Secure score

Topic	Details
	- Analyze identity-related threats and risks identified in Microsoft 365 Defender
Secure endpoints by using Microsoft Defender for Endpoint	- Plan a Microsoft Defender for Endpoint solution - Implement Microsoft Defender for Endpoint - Manage and monitor Microsoft Defender for Endpoint - Analyze and remediate threats and risks to endpoints identified in Microsoft 365 Defender
Secure endpoints by using Microsoft Endpoint Manager	- Plan for device and application protection - configure and manage Microsoft Defender Application Guard - Configure and manage Windows Defender Application Control - configure and manage exploit protection - Configure and manage device encryption - Configure and manage application protection policies - Monitor and manage device security status using Microsoft Endpoint Manager admin center - Analyze and remediate threats and risks to endpoints identified in Microsoft Endpoint Manager
Secure collaboration by using Microsoft Defender for Office 365	- Plan a Microsoft Defender for Office 365 solution - Configure Microsoft Defender for Office 365 - Monitor for threats by using Microsoft Defender for Office 365 - Analyze and remediate threats and risks to collaboration workloads identified in Microsoft 365 Defender - Conduct simulated attacks by using Attack simulation training
Detect and respond to threats in Microsoft 365 by using Microsoft Sentinel	- Plan a Microsoft Sentinel solution for Microsoft 365 - Implement and configure Microsoft Sentinel for Microsoft 365 - Manage and monitor Microsoft 365 security by using Microsoft Sentinel - Respond to threats using built-in playbooks in Microsoft Sentinel

Topic	Details
Secure connections to cloud apps by using Microsoft Defender for Cloud Apps	- Plan Microsoft Defender for Cloud Apps implementation - Configure Microsoft Defender for Cloud Apps - Manage cloud app discovery - Manage entries in the Microsoft Defender for Cloud Apps catalog - Manage apps in Microsoft Defender for Cloud Apps - Configure Microsoft Defender for Cloud Apps connectors and OAuth apps - Configure Microsoft Defender for Cloud Apps policies and templates - Analyze and remediate threats and risks relating to cloud app connections identified in Microsoft 365 Defender - Manage App governance in Microsoft Defender for Cloud Apps
Implement and manage information protection (15-20%)	
Manage sensitive information	- Plan a sensitivity label solution - Create and manage sensitive information types - Configure Sensitivity labels and policies - Publish sensitivity labels to Microsoft 365 workloads - Monitor data classification and label usage by using Content explorer and Activity explorer - Apply labels to files and schematized data assets in Microsoft Purview Data Map
Implement and manage Microsoft Purview Data Loss Prevention (DLP)	- Plan a DLP solution - Create and manage DLP policies for Microsoft 365 workloads - Implement and manage Endpoint DLP - Monitor DLP - Respond to DLP alerts and notifications
Plan and implement Microsoft Purview Data lifecycle management	- Plan for data lifecycle management - Review and interpret data lifecycle management reports and dashboards - Configure retention labels, policies, and label policies

Topic	Details
	- Plan and implement adaptive scopes - Configure retention in Microsoft 365 workloads - Find and recover deleted Office 365 data
Manage compliance in Microsoft 365 (20-25%)	
Manage and analyze audit logs and reports in Microsoft Purview	- Plan for auditing and reporting - Investigate compliance activities by using audit logs - Review and interpret compliance reports and dashboards - Configure alert policies - Configure audit retention policies
Plan for, conduct, and manage eDiscovery cases	- Recommend eDiscovery Standard or Premium - Plan for content search and eDiscovery - Delegate permissions to use search and discovery tools - Use search and investigation tools to discover and respond - Manage eDiscovery cases
Manage regulatory and privacy requirements	- Plan for regulatory compliance in Microsoft 365 - Manage regulatory compliance in the Microsoft Purview Compliance Manager - Implement privacy risk management in Microsoft Priva - Implement and manage Subject Rights Requests in Microsoft Priva
Manage insider risk solutions in Microsoft 365	- Implement and manage Customer Lockbox - Implement and manage Communication compliance policies - Implement and manage Insider risk management policies - Implement and manage Information barrier policies - Implement and manage Privileged access management

Broaden Your Knowledge with Microsoft MS-500 Sample Questions:

Question: 1

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: 2

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: 3

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: 4

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

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

Answer: c

Question: 5

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: 6

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: 7

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

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

Answer: a

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

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

Question: 10

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

Avail the Study Guide to Pass Microsoft MS-500 Microsoft 365 Security Administration Exam:

- Find out about the MS-500 syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **MS-500 syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.
- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the MS-500 training. Joining the Microsoft provided training for MS-500 exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **MS-500 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. MS-500 practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

- Passing the MS-500 exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.

Here Is the Trusted Practice Test for the MS-500 Certification

EduSum.Com is here with all the necessary details regarding the MS-500 exam. We provide authentic practice tests for the MS-500 exam. What do you gain from these practice tests? You get to experience the real exam-like questions made by industry experts and get a scope to improve your performance in the actual exam. Rely on EduSum.Com for rigorous, unlimited two-month attempts on the **MS-500 practice tests**, and gradually build your confidence. Rigorous practice made many aspirants successful and made their journey easy towards grabbing the Microsoft 365 Certified - Security Administrator Associate.

Start Online Practice of MS-500 Exam by visiting URL

https://www.edusum.com/microsoft/ms-500-microsoft-365-security-administration