Microsoft 365 Certified: Security Administrator Associate – Skills Measured

This document contains the skills measured on the exams associated with this certification. It does not include any upcoming or recent changes that have been made to those skills. For more information about upcoming or recent changes, see the associated exam details page(s).

NOTE: The bullets that follow each of the skills measured are intended to illustrate how we are assessing that skill. This list is not definitive or exhaustive.

NOTE: Most questions cover features that are General Availability (GA). The exam may contain questions on Preview features if those features are commonly used.

Exam MS-500: Microsoft 365 Security Administration

Implement and manage identity and access (35-40%)

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
- manage external identities in Azure AD and Microsoft 365 workloads

Implement authentication methods

- implement multi-factor authentication (MFA) by using conditional access policy
- manage and monitor MFA
- plan and implement device authentication methods like Windows Hello

Implement conditional access

- plan for compliance and conditional access policies
- configure and manage device compliance for endpoint security
- implement and manage conditional access
- test and troubleshoot conditional access policies

Implement roles and role groups

- plan for roles and role groups
- configure roles and role groups
- audit roles for least privileged access

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 (25-30%)

Implement and manage Microsoft Defender for Identity

- 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

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 and manage Windows device encryption
- configure and manage non-Windows device encryption
- implement application protection policies
- configure and manage device compliance for endpoint security

Implement and manage Microsoft Defender for Office 365

- configure Microsoft Defender for Office 365
- monitor for and remediate threats using 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 using built-in playbooks in Azure Sentinel

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
- 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

Implement and manage information protection (10-15%)

Manage sensitive information

- plan a sensitivity label solution
- create and manage sensitive information types
- configure sensitivity labels and policies.
- configure and use Activity Explorer
- use sensitivity labels with Teams, SharePoint, OneDrive and Office apps

Manage Data Loss Prevention (DLP)

- plan a DLP solution
- create and manage DLP policies for Microsoft 365 workloads
- create and manage sensitive information types
- monitor DLP reports
- manage DLP notifications
- implement Endpoint DLP

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 and manage communication compliance policies
- configure retention in Microsoft 365 workloads
- find and recover deleted Office 365 data
- configure and use Microsoft 365 Records Management

Manage Governance and Compliance Features in Microsoft 365 (20-25%)

Configure and analyze security reporting

- monitor and manage device security status using Microsoft Endpoint Manager Admin Center.
- manage and monitor security reports and dashboards using Microsoft 365 Defender portal
- plan for custom security reporting with Graph Security API
- use secure score dashboards to review actions and recommendations
- configure alert policies in the Security & Compliance center

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

Discover and respond to compliance queries in Microsoft 365

- 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 compliance

- plan for regulatory compliance in Microsoft 365
- manage Data Subject Requests (DSRs)
- administer Compliance Manager in Microsoft 365 compliance center
- use Compliance Manager

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