

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).

Exam MS-500: Microsoft 365 Security Administration

Skills Measured

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

NOTE: In most cases, exams do NOT cover preview features, and some features will only be added to an exam when they are GA (General Availability).

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

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
- implement and configure Azure PIM roles
- manage Azure PIM role assignments

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 an Azure ATP solution
- install and configure Azure ATP
- monitor and manage Azure ATP

Implement device threat protection

- plan a Microsoft Defender ATP solution
- implement Microsoft Defender ATP
- manage and monitor Microsoft Defender ATP

Implement and manage device and application protection

- plan for device and application protection
- configure and manage Windows Defender Application Guard
- configure and manage Windows Defender Application Control
- configure and manage Windows Defender Exploit Guard
- 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 Office 365 ATP

- configure Office 365 ATP
- monitor Office 365 ATP
- conduct simulated attacks using Attack Simulator

Implement Azure Sentinel for Microsoft 365

- 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 Azure information Protection (AIP)

- plan an AIP solution
- configure Sensitivity labels and policies
- deploy the RMS connector
- manage tenant keys
- deploy the AIP client
- integrate AIP with Office 365 Services

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

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 reports 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
- configure alert policies in the Security & Compliance admin 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

Manage data governance and retention

- plan for data governance and retention
- review and interpret data governance reports and dashboards
- configure retention policies
- define data governance event types
- define data governance supervision 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
- search for personal data
- monitor for leaks of personal data
- 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
- review Compliance Manager reports
- create and perform Compliance Manager assessments and action items