

Study Guide

Exam AZ-500: Microsoft Azure Security Technologies

Purpose of this document

This study guide should help you understand what to expect on the exam and includes a summary of the topics the exam might cover and links to additional resources. The information and materials in this document should help you focus your studies as you prepare for the exam.

Useful links	Description
How to earn the certification	Some certifications only require one exam, while others require more. On the details page, you'll find information about what skills are measured and links to registration. Each exam also has its own details page covering exam specifics.
Certification renewal	Once you earn your certification, don't let it expire. When you have an active certification that's expiring within six months, you should renew it—at no cost—by passing a renewal assessment on Microsoft Learn. Remember to renew your certification annually if you want to retain it.
Your Microsoft Learn profile	Connecting your certification profile to Learn brings all your learning activities together. You'll be able to schedule and renew exams, share and print certificates, badges and transcripts, and review your learning statistics inside your Learn profile.
Passing score	All technical exam scores are reported on a scale of 1 to 1,000. A passing score is 700 or greater. As this is a scaled score, it may not equal 70% of the points. A passing score is based on the knowledge and skills needed to demonstrate competence as well as the difficulty of the questions.
Exam sandbox	Are you new to Microsoft certification exams? You can explore the exam environment by visiting our exam sandbox. We created the sandbox as an opportunity for you to experience an exam before you take it. In the sandbox, you can interact with different question types, such as build list, case studies,

Useful links	Description
	<p>and others that you might encounter in the user interface when you take an exam. Additionally, it includes the introductory screens, instructions, and help topics related to the different types of questions that your exam might include. It also includes the non-disclosure agreement that you must accept before you can launch the exam.</p>
<p>Request accommodations</p>	<p>We're committed to ensuring all learners are set up for success. If you use assistive devices, require extra time, or need modification to any part of the exam experience, you can request an accommodation.</p>
<p>Take a practice test</p>	<p>Taking a practice test is a great way to know whether you're ready to take the exam or if you need to study a bit more. Subject-matter experts write the Microsoft Official Practice Tests, which are designed to assess all exam objectives.</p>

Objective domain: skills the exam measures

The English language version of this exam was updated on November 1, 2022.

Some exams are localized into other languages, and those are updated approximately eight weeks after the English version is updated. Other available languages are listed in the **Schedule Exam** section of the **Exam Details** webpage. If the exam isn't available in your preferred language, you can request an additional 30 minutes to complete the exam.

Note

The bullets that follow each of the skills measured are intended to illustrate how we are assessing that skill. Related topics may be covered in the exam.

Note

Most questions cover features that are general availability (GA). The exam may contain questions on Preview features if those features are commonly used.

Skills measured

- Manage identity and access (30–35%)
- Implement platform protection (15–20%)
- Manage security operations (20–25%)
- Secure data and applications (20–25%)

Functional groups

Manage identity and access (30–35%)

Manage identities in Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra

- Create and manage a managed identity for Azure resources
- Manage Azure AD groups
- Manage Azure AD users
- Manage external identities by using Azure AD
- Manage administrative units

Manage secure access by using Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra

- Configure Azure AD Privileged Identity Management (PIM)
- Implement Conditional Access policies, including multifactor authentication
- Implement Azure AD Identity Protection
- Implement passwordless authentication
- Configure access reviews

Manage application access

- Integrate single sign on (SSO) and identity providers for authentication
- Create an app registration
- Configure app registration permission scopes
- Manage app registration permission consent
- Manage API permissions to Azure subscriptions and resources
- Configure an authentication method for a service principal

Manage access control

- Configure Azure role permissions for management groups, subscriptions, resource groups, and resources
- Interpret role and resource permissions
- Assign built-in roles in Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra
- Create and assign custom roles, including Azure roles and Azure AD roles

Implement platform protection (15–20%)

Implement advanced network security

- Secure the connectivity of hybrid networks
- Secure the connectivity of virtual networks
- Create and configure Azure Firewall

- Create and configure Azure Firewall Manager
- Create and configure Azure Application Gateway
- Create and configure Azure Front Door
- Create and configure Web Application Firewall (WAF)
- Configure a resource firewall, including storage account, Azure SQL, Azure Key Vault, or Azure App Service
- Configure network isolation for Web Apps and Azure Functions
- Implement Azure Service Endpoints
- Implement Azure Private Endpoints, including integrating with other services
- Implement Azure Private Links
- Implement Azure DDoS Protection

Configure advanced security for compute

- Configure Endpoint Protection for virtual machines (VMs)
- Implement and manage security updates for VMs
- Configure security for container services
- Manage access to Azure Container Registry
- Configure security for serverless compute
- Configure security for an Azure App Service
- Configure encryption at rest
- Configure encryption in transit

Manage security operations (20–25%)

Configure centralized policy management

- Configure a custom security policy
- Create a policy initiative
- Configure security settings and auditing by using Azure Policy

Configure and manage threat protection

- Configure Microsoft Defender for Servers (not including Microsoft Defender for Endpoint)
- Evaluate vulnerability scans from Microsoft Defender for Cloud
- Configure Microsoft Defender for SQL
- Use the Microsoft Threat Modeling Tool

Configure and manage security monitoring solutions

- Create and customize alert rules by using Azure Monitor
- Configure diagnostic logging and log retention by using Azure Monitor
- Monitor security logs by using Azure Monitor
- Create and customize alert rules in Microsoft Sentinel
- Configure data connectors in Microsoft Sentinel

- Evaluate alerts and incidents in Microsoft Sentinel

Secure data and applications (20–25%)

Configure security for storage

- Configure access control for storage accounts
- Configure storage account access keys
- Configure Azure Files identity-based authentication for SMB access
- Configure delegated access

Configure security for data

- Enable database authentication by using Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra
- Enable database auditing
- Configure dynamic masking on SQL workloads
- Implement database encryption for Azure SQL Database
- Implement network isolation for data solutions, including Azure Synapse Analytics and Azure Cosmos DB

Configure and manage Azure Key Vault

- Create and configure Key Vault
- Configure access to Key Vault
- Manage certificates, secrets, and keys
- Configure key rotation
- Configure backup and recovery of certificates, secrets, and keys

Study Resources

We recommend that you train and get hands-on experience before you take the exam. We offer self-study options and classroom training as well as links to documentation, community sites, and videos.

Study resources	Links to learning and documentation
Get trained	Choose from self-paced learning paths and modules or take an instructor-led course
Find documentation	Azure documentation Azure Active Directory (AD) Azure Firewall documentation Azure Firewall Manager documentation

Study resources

Links to learning and documentation

- [Azure Application Gateway documentation](#)
- [Azure Front Door and CDN Documentation](#)
- [Web Application Firewall documentation](#)
- [Azure Key Vault documentation](#)
- [Azure virtual network service endpoint policies](#)
- [Manage Azure Private Endpoints - Azure Private Link](#)
- [Create a Private Link service by using the Azure portal](#)
- [Azure DDoS Protection Standard documentation](#)
- [Endpoint Protection on a Windows VM in Azure](#)
- [Secure and use policies - Azure Virtual Machines](#)
- [Security - Azure App Service](#)
- [Azure Policy documentation](#)
- [Overview of Microsoft Defender for Servers](#)
- [Microsoft Defender for Cloud documentation](#)
- [Microsoft Threat Modeling Tool overview](#)
- [Azure Monitor documentation](#)
- [Microsoft Sentinel documentation](#)
- [Azure Storage documentation](#)
- [Azure Files documentation](#)
- [Azure SQL documentation](#)

Ask a question

[Microsoft Q&A | Microsoft Docs](#)

Get community support

[Azure Community Support](#)

Follow Microsoft Learn

[Microsoft Learn - Microsoft Tech Community](#)

Find a video

[Exam Readiness Zone](#)

[Azure Fridays](#)

[Browse other Microsoft Learn shows](#)
