

training code: SC-300 / ENG DL 4d / EN

Microsoft Identity and Access Administrator

Authorized Microsoft Identity and Access Administrator **SC-300**
Distance Learning training.

Target audience:

- Administrator
- IT specialist
- Security specialist
- Security engineer



Purpose of the training

The training is intended for:

- Implementing solutions for identity management
- Implementing solutions for authentication and access management
- Implementing application access management
- Scheduling and implementing strategy of identity management

The course is intended for identity and access administrators, who plan to take related certification exam or who perform administration tasks related to identity and access in everyday work. The course would also be helpful for administrator or engineer who specialises in providing solutions for supporting identity and systems of Azure platform based solutions access management; fulfilling the integral role in protecting an organisation.



Benefits of completing the training

Benefits from the training completion:

- Implement solution for identity management

- Implement solutions for authentication and access management
- Implement application access management
- Plan and implement strategy of identity management

The course provides IT Identity and Access Professional, together with IT Security Professional, knowledge and skills necessary to implement solutions to manage identity based on Microsoft Azure AD and combined identity technologies. This course included the content of identity for Azure AD service, registering applications for companies, conditional access, supervision over identity and other tools for identity management.



Examination method

The exam is on-line. You can enroll at: <https://home.pearsonvue.com/Clients/Microsoft.aspx>



Exam description

After the **SC-300** course, you can take **Microsoft** certification **exams**: an Authorized Test Center, online being monitored by an offsite proctor. Details on the website:

<https://docs.microsoft.com/pl-pl/learn/certifications/exams/sc-300>



Expected Listener Preparation

- Basic knowledge of Microsoft 365 platform
- Basic knowledge about Microsoft products related to securities, compatibility and identity
- Intermediate knowledge of Windows 10 system
- Knowledge of Azure platform services
- Basic understanding of script concepts
- Certain experience with Windows and Linux operational systems
- An ability to use English language materials

To make work more convenient and training more effective we suggest using additional screen. Lack of extra screen does not make it impossible to participate in the training, but significantly influences the convenience of work during classes

Information and requirements concerning participation in distance learning trainings is available at: <https://www.altkomakademia.pl/distance-learning/#FAQ>



Training Language

- **Training:** English
- **Materials:** English

Training Includes

* electronic handbook available at:

<https://learn.microsoft.com/pl-pl/training/>

* access to Altkom Akademia student portal

Training method:

- theory
- demos
- individual laboratories
- 50% theory
- 50% practice

Duration

4 days / 28 hours

Training agenda

1: Implementing solution for identity management

- Implement initial configuration of Azure AD service
- Create, configure and manage identities
- Implement external identities and manage them
- Implement and manage hybrid identity

2: Implementing solution for authentication and access management

- Secure Azure AD user with the use of MFA service
- Manage user authentication
- Plan, implement and manage conditional access

- Manage identity security in Azure AD service

3: Implementing application access management

- Plan and design company integration in terms of single registration
- Implement and monitor corporate application integration for the needs of single sign-in
- Implementing application registration

4: Planning and implementing strategy of identity management

- Plan and implement authentication management
- Plan, implement and manage access reviews
- Plan and implement privileged access
- Monitor and maintain Azure AD service