
Manage Identities

Duration: 1 Day **Course Code: M-AZ-100T05**

Overview:

This course teaches IT Professional how to use Azure Active Directory (AD) to provide employees and customers with a multi-tenant cloud-based directory and identity management system. Students will learn the differences between Azure AD and Active Directory Domain Services (AD DS), as well the differences in functionality offered by the different editions of Azure AD. Students also learn how to configure self-service password reset, or to use the option of password writeback to reset user passwords regardless of their location. Students are then introduced to Azure AD Identity Protection and learn how they can use it to protect their organizations from compromised accounts, identity attacks, and configuration issues. Students also learn how to integrate Azure AD with the many Software as a Service (SaaS) applications that are used, in order to secure user access to those applications.

Next, the concepts of Azure domains and tenants, and users and groups are explained and students learn how to work with the various Azure AD objects. Students are introduced to Azure role-based access control to be able to provide a more granular access based on the principle of least privilege. An administrator, or user, can do exactly the task they need to accomplish; no more, no less. Students also learn how to work with Azure joined devices and Hybrid AD joined devices, enabling their users to be productive wherever and whenever – but ensuring that corporate assets are protected and that devices meet security and compliance standards.

Students learn how to use Azure AD Connect to integrate their on-premises directories with Azure AD, providing a common identity for their users of Office 365, Azure, and SaaS applications integrated with Azure AD. Lastly, students also learn how to use Azure AD Application Proxy to be able to provide their users with remote access to web application that are published on-premises, such as SharePoint sites, Outlook Web Access, or any other line of business (LOB) applications the organization has.

Target Audience:

This course is for Azure Administrators. Azure Administrators manage the cloud services that span storage, networking, and compute cloud capabilities, with a deep understanding of each service across the full IT lifecycle. They take end-user requests for new cloud applications and make recommendations on services to use for optimal performance and scale, as well as provision, size, monitor and adjust as appropriate. This role requires communicating and coordinating with vendors. Azure Administrators use the Azure Portal and as they become more proficient they use PowerShell and the Command Line Interface.

Objectives:

- After completing this course, students will be able to:
 - Implement Azure Active Directory, Self-Service Password Reset, Azure AD Identity Protection, and integrated SaaS applications.
 - Configure domains and tenants, users and groups, roles, and devices.
 - Implement and manage Azure Active Directory integration options and Azure AD Application Proxy.
-

Prerequisites:

■

Content:

Module 1: Managing Azure Active Directory

In this module, you'll be introduced to Azure Active Directory. What is Azure Active Directory and how is it different from Active Directory Domain Services? What is Self-Service Password Reset and how is it configured? How can Azure AD Identity protection improve your security posture. How do you integrate SaaS applications with Azure AD?

Lessons

- Azure Active Directory Overview
- Self-Service Password Reset
- Azure AD Identity Protection
- Integrating SaaS Applications with Azure AD
- Azure Domains and Tenants
- Azure Users and Groups
- Azure Roles
- Managing Devices
- Azure Active Directory Integration Options
- Azure AD Application Proxy

After completing this module, students will be able to:

- Configure domains and tenants, users and groups, roles, and devices.
- Implement and manage Azure Active Directory integration options and Azure AD Application Proxy.

Implement Azure Active Directory, Self-Service Password Reset, Azure AD Identity Protection, and integrated SaaS applications.

Module 2: Managing Azure Active Directory Objects

In this module, you will learn the basics of implementing Azure AD objects. These objects include domains and tenants, users and groups, roles, and devices. In each lesson you will practice how to configure these objects through the portal and with Azure PowerShell. The Azure roles lesson will be your introduction to role-based access control.

Lessons

- Azure Active Directory Overview
- Self-Service Password Reset
- Azure AD Identity Protection
- Integrating SaaS Applications with Azure AD
- Azure Domains and Tenants
- Azure Users and Groups
- Azure Roles
- Managing Devices
- Azure Active Directory Integration Options
- Azure AD Application Proxy

After completing this module, students will be able to:

- Configure domains and tenants, users and groups, roles, and devices.
- Implement and manage Azure Active Directory integration options and Azure AD Application Proxy.

Module 3: Implementing and Managing Hybrid Identities

In this module, you will learn how to integrate Active Directory with your existing infrastructure. You will learn about different authentication options like AD Connect, Single Sign On, and Pass-through authentication. You will also learn how to configure Azure AD Application Proxy and how it is used.

Lessons

- Azure Active Directory Overview
- Self-Service Password Reset
- Azure AD Identity Protection
- Integrating SaaS Applications with Azure AD
- Azure Domains and Tenants
- Azure Users and Groups
- Azure Roles
- Managing Devices
- Azure Active Directory Integration Options
- Azure AD Application Proxy

After completing this module, students will be able to:

- Configure domains and tenants, users and groups, roles, and devices.
- Implement and manage Azure Active Directory integration options and Azure AD Application Proxy.

Module 4: Lab - Implement and Manage Hybrid Identities

This module is provided to give you hands-on experience with the information provided in the course.

Lab : Implement and Manage Hybrid Identities

- Deploy a VM with an AD domain controller
- Create and configure an Azure AD tenant
- Synchronize an AD forest with an Azure AD tenant

After completing this module, you will be able to:

- Deploy an Azure VM hosting an Active Directory domain controller.
- Create and configure an Azure Active Directory tenant.
- Synchronize Active Directory forest with an Azure Active Directory tenant.

Further Information:

For More information, or to book your course, please call us on 353-1-814 8200

info@globalknowledge.ie

www.globalknowledge.com/en-ie/

Global Knowledge, 3rd Floor Jervis House, Millennium Walkway, Dublin 1