CANTON WEKE OTIENO

SECURITY ENGINEER TRACK

STUDENT TRACKING NUMBER; ADC-SE01-24010

CYBER SHUJAA

INSTRUCTOR: Dr. Paula

AZ-104: MANAGE IDENTITIES AND GOVERNANCE IN AZURE

Introduction

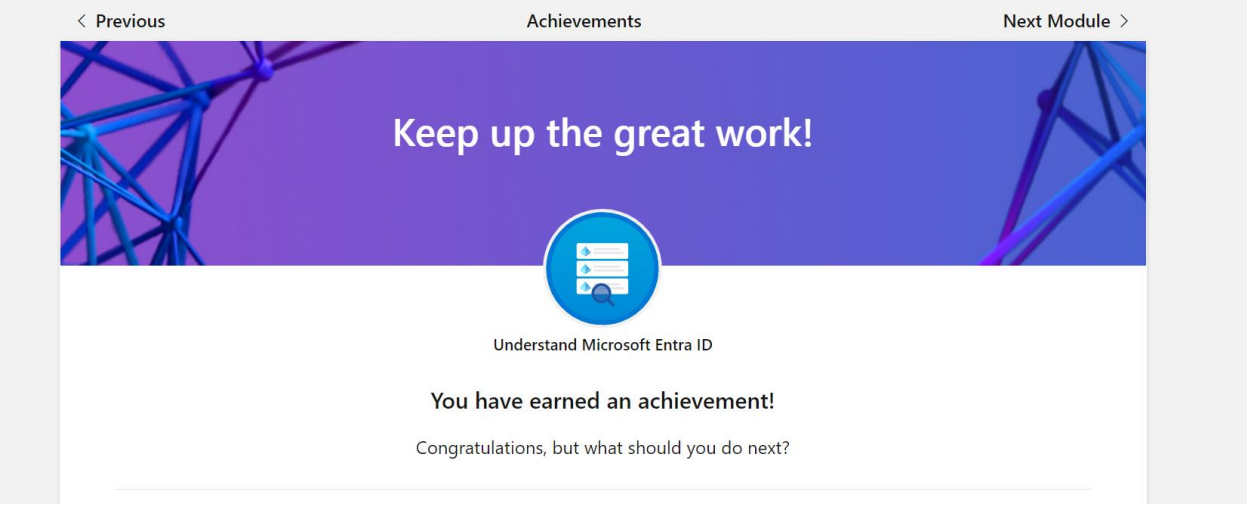
In the quickly changing digital world of today, controlling and safeguarding user access to vital resources is essential. My report delves into essential strategies and configurations within Microsoft's Azure ecosystem, focusing on empowering users and administrators with robust security and access management tools. Key topics discussed include enabling users to reset their passwords independently using Microsoft Entra's self-service password reset, and securing Azure resources with Azure Role-Based Access Control (RBAC). These tools not only strengthen security but also streamline user management, lowering the administrative strain and enhancing operational efficiency.

The creation and management of Azure users and groups under Microsoft Entra ID, as well as the configuration of role-based access control to guarantee proper permissions and access levels, are also covered in this module. It also covers the importance of Azure Policy in enforcing organizational compliance, the setup of subscriptions, and the comprehensive management of user and group accounts. An in-depth understanding of Microsoft Entra ID is also provided, highlighting its pivotal role in identity and access management within the Azure platform. By employing these principles, organizations can greatly strengthen their security posture while simplifying user and resource management.

Understand Microsoft Entra ID

Microsoft Entra ID is part of the platform as a service (PaaS) offering and operates as a Microsoft-managed directory service in the cloud. It’s not a part of the core infrastructure that customers own and manage, nor is it an Infrastructure as a service offering.

Microsoft Entra constitutes a separate Azure service. Its most elementary form, which any new Azure subscription includes automatically, doesn't incur any extra cost and is referred to as the Free tier. If one subscribe to any Microsoft Online business services (for example, Microsoft 365 or Microsoft Intune), automatically get Microsoft Entra ID with access to all the Free features.

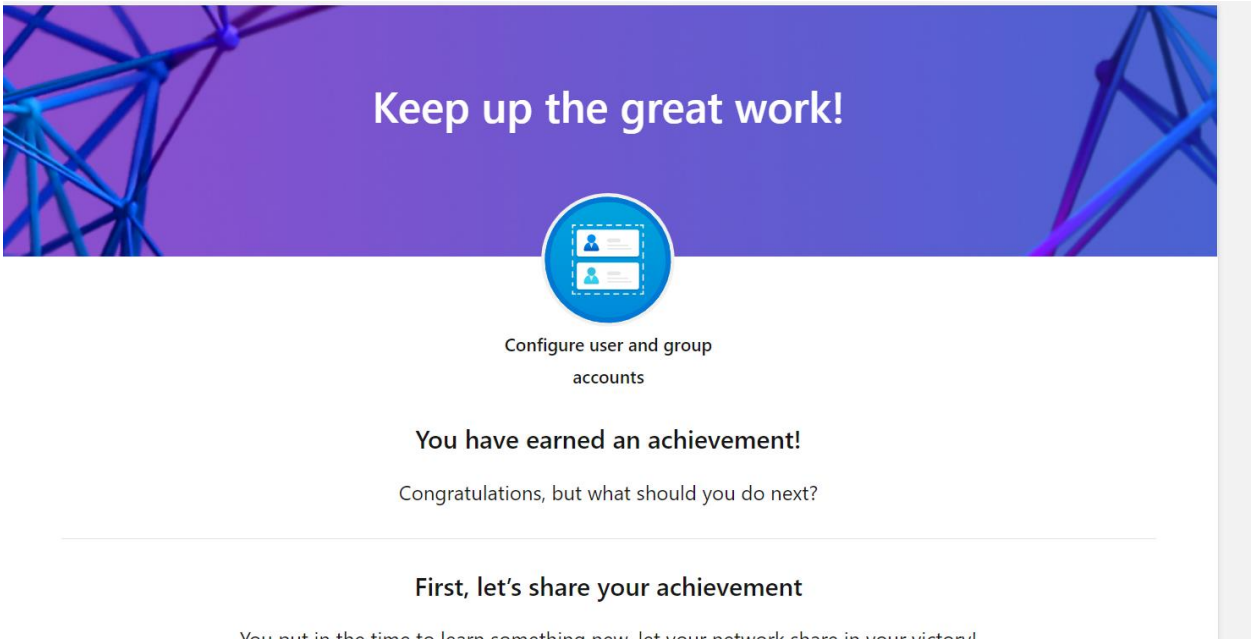


https://learn.microsoft.com/api/achievements/share/en-us/CantonOtieno-0232/8AGJZB2W?sharingId=17A12B375B49B311

Active Directory provides the core service of identity management. AD DS is the traditional on-premises solution, whereas Microsoft Entra ID is the cloud-based solution. Microsoft Entra ID is frequently adopted at first to facilitate authentication for cloud-based apps, but can provide authentication services for the entire infrastructure. While they provide similar solutions, each offer different capability and are often used together to provide a best-of-breed solution. Microsoft Entra ID is offered as a free service, with paid tiers for additional capabilities, depending on an organization's needs

Configure user and group accounts

Every user who wants access to azure resources need an Azure user account. A user account has all the information required to authenticate the user during the sign-in process. Microsoft Entra ID supports three types of user accounts. The types indicate where the user is defined (in the cloud or on-premises), and whether the user is internal or external to your Microsoft Entra organization.



https://learn.microsoft.com/api/achievements/share/en-us/CantonOtieno-0232/BGVRUPWD?sharingId=17A12B375B49B311

In this module, I have learnt that every user who wants access to azure resources need an Azure user account. Microsoft Entra ID supports access to organization's resources by assigning access rights to users and groups. This module made me discover how user and group accounts are created in Microsoft Entra ID. I explored how to configure and manage user and group accounts,

including bulk configuration. I managed to review how organization can support group account organization, and manage accounts across multiple directories.

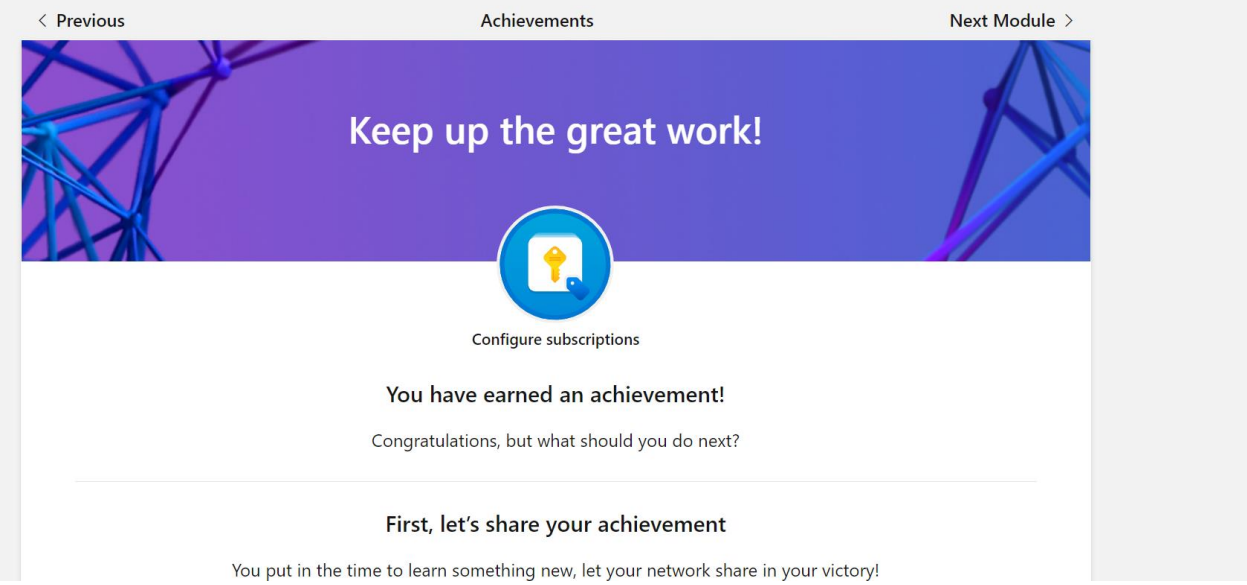
Configure subscriptions

In this module I have Learnt how to configure Azure subscriptions, including how to obtain a subscription, implement cost management, and apply Azure resource tags.

Azure Administrators commonly obtain and manages Azure subscriptions. Azure subscriptions help you effectively identify and manage costs for your organization, so you can provide services and resources for specific scenarios

The module contain the following; determining the correct region to locate Azure services. reviewing features and use cases for Azure subscriptions, obtaining an Azure subscription, understanding billing and features for different Azure subscriptions, using Microsoft Cost Management for cost analysis. Discovering when to use Azure resource tagging. Identifying ways to reduce costs.

.

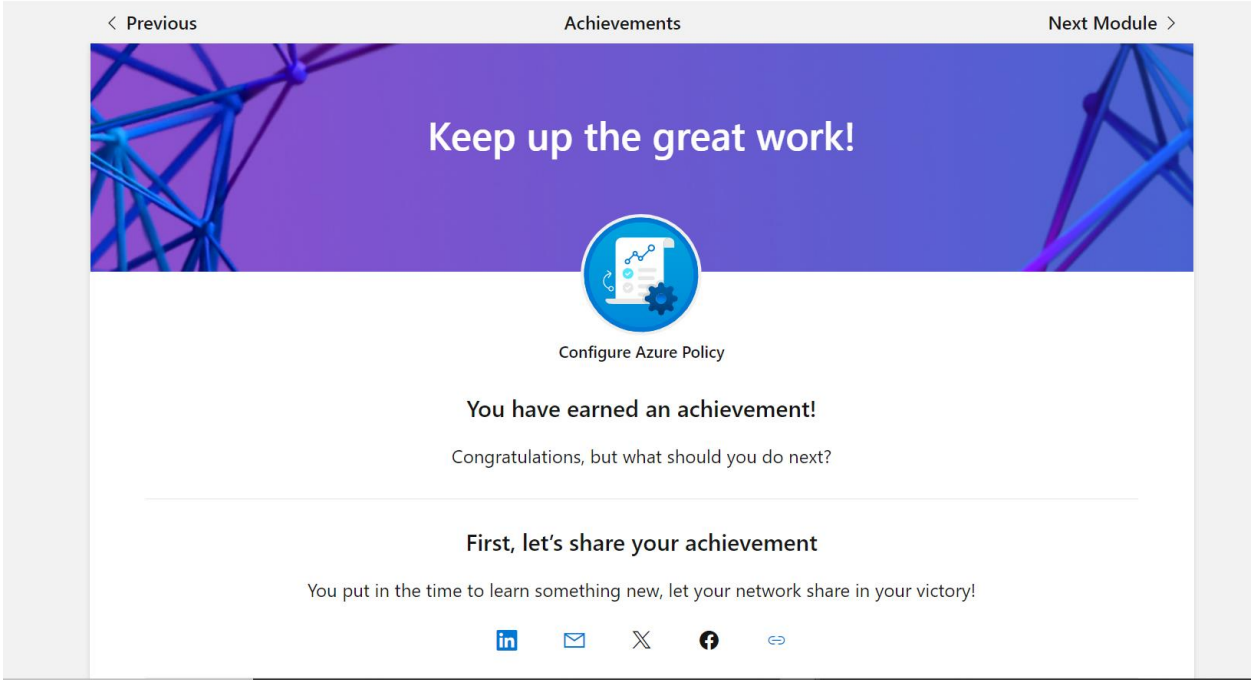


https://learn.microsoft.com/api/achievements/share/en-us/CantonOtieno-0232/W76TJ48N?sharingId=17A12B375B49B311

Configure Azure Policy

Azure Policy is a service in Azure that enables one to create, assign, and manage policies. Azure Policy helps you define and implement governance strategy by using policies to control and audit resources.

In this module, I have learnt about Azure Policy and how it allows one to control and audit your resources. It involves exploring how to implement Azure policy definitions and initiatives for corporate departments. I also learnt how to create management groups, scope policies, and manage spending budgets. Finally, I reviewed how Azure policies can be scoped to meet compliance regulations.



https://learn.microsoft.com/api/achievements/share/en-us/CantonOtieno-0232/3Y56UMYH?sharingId=17A12B375B49B311

Configure role-based access control

Azure RBAC is an authorization system built on Azure Resource Manager that provides fine-grained access management to Azure resources.

Azure role-based access control (Azure RBAC) helps one to manage who has access to Azure resources, what they can do with those resources, and what areas they have access to.

The goal of this module is to understand the features and use cases for Azure role-based access control (RBAC). learn how to create role definitions and role assignments, and find and use built-in Azure RBAC roles. Additionally, explore how to use RBAC to manage access to subscriptions. Review the differences between Azure RBAC and Entra ID roles**.**

Azure role-based access control (RBAC) is a system that enables granular access management of Azure resources. Azure Administrators use Azure RBAC to segregate duties within a team, and grant users the specific access they need to perform their jobs.

In this module, I learnt how to identify the features and use cases for RBAC. I also discovered how to create role definitions and role assignments, and find and use built-in Azure RBAC roles. I explored how to use RBAC to manage access to subscriptions with RBAC. And reviewed the differences between Azure RBAC and Microsoft Entra roles.

The main takeaways from this module are:

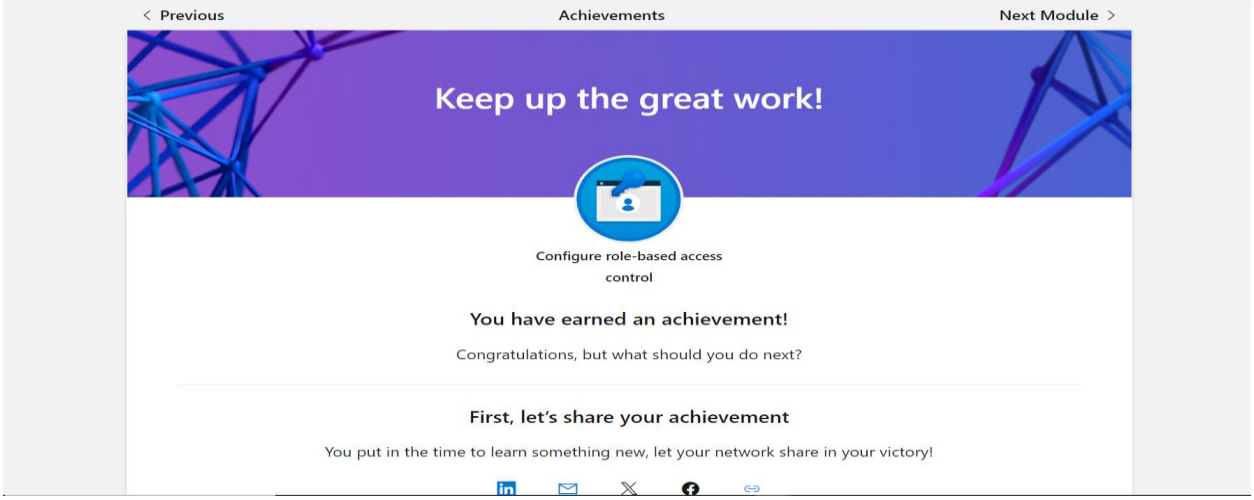
Azure RBAC is a system that enables granular access management of Azure resources. It allows one to segregate duties within a team and grant users specific access based on their job requirements.

Role definitions in Azure RBAC define sets of permissions that list the allowed operations. one can use built-in role definitions or create custom role definitions to meet the specific requirements of your organization.

Role assignments attach role definitions to security principals at a particular scope. This assignment determines the level of access granted to the requestor. Access can be revoked by removing a role assignment.

Azure RBAC roles can be assigned at different scopes, including management groups, subscriptions, resource groups, and resources. The scope limits the permissions available to the assigned requestor.

Azure RBAC roles and Entra ID administrator roles can be used together to manage access to both Azure resources and Entra ID resources.



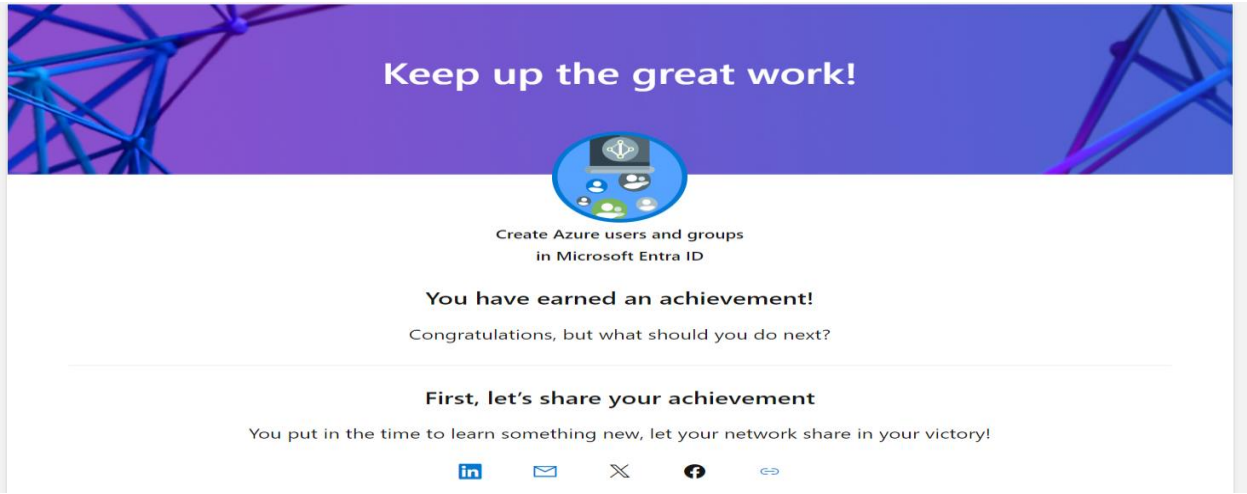
https://learn.microsoft.com/api/achievements/share/en-us/CantonOtieno-0232/W763M7ZN?sharingId=17A12B375B49B311

Create Azure users and groups in Microsoft Entra ID

In Microsoft Entra ID, all user accounts are granted a set of default permissions. A user's account access consists of the user type, their role assignments, and their ownership of individual objects**.**

In this module, learnt how to add a user and a group to a Microsoft Entra organization that I created. In I addition I also learnt how to invite guest user from an external development team to allow for collaboration with the other development team . Finally the modules cover how to add an enterprise application to Microsoft Entra organization and allow a guest user to access the application**.**

Below is my certificate and achievement



Link to verify my achievement

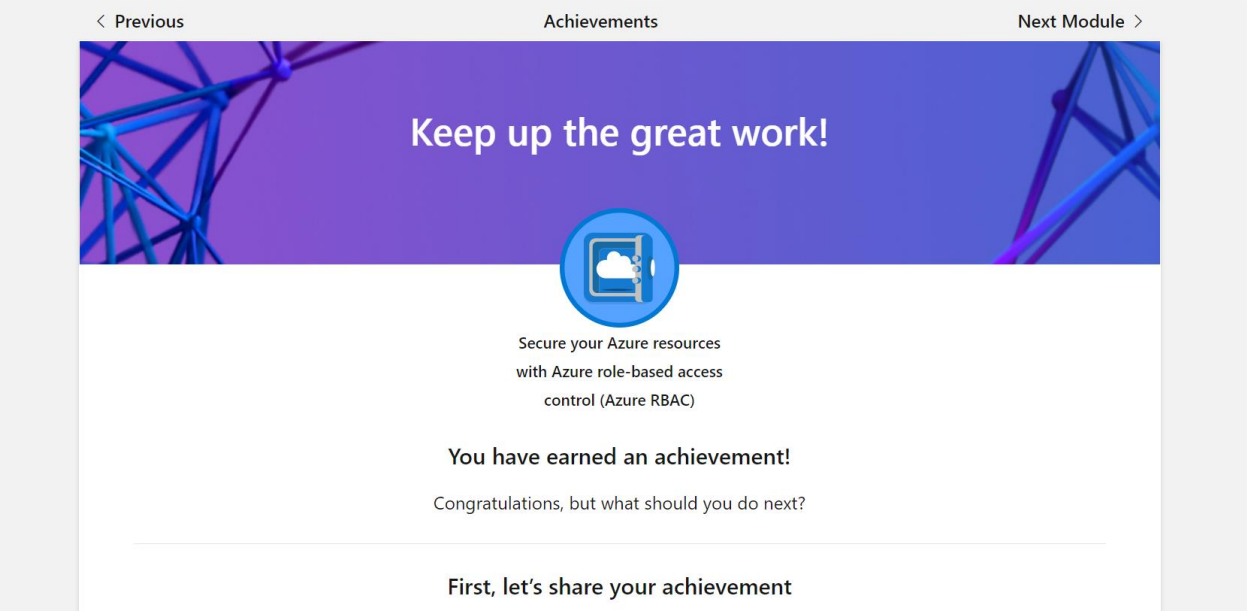
https://learn.microsoft.com/api/achievements/share/en-us/CantonOtieno-0232/8AGHCLFW?sharingId=17A12B375B49B311

Secure your Azure resources with Azure role-based access control (Azure RBAC)

Azure RBAC is an authorization system built on Azure Resource Manager that provides fine-grained access management to Azure resources. Securing your Azure resources such as virtual machines, websites, networks, and storage is a critical function for any organization using the cloud. With Azure RBAC, one can grant the exact access that users need to do their jobs.

In this module I have learnt the following about Azure role-based access control (Azure RBAC) and how you can use it to secure Azure resources. To grant access, one needs to assign users a role at a particular scope. Using Azure RBAC, one can grant only the amount of access to users that they need to perform their jobs. Azure RBAC has more than 200 built-in roles, but if an organization needs specific permissions, one needs to create own custom roles. And finally, I have learnt that Azure keeps track of Azure RBAC changes and you can track all the changes.

Below is my certificate



Link to verify my achievement

https://learn.microsoft.com/api/achievements/share/en-us/CantonOtieno-0232/PS7EQL64?sharingId=17A12B375B49B311

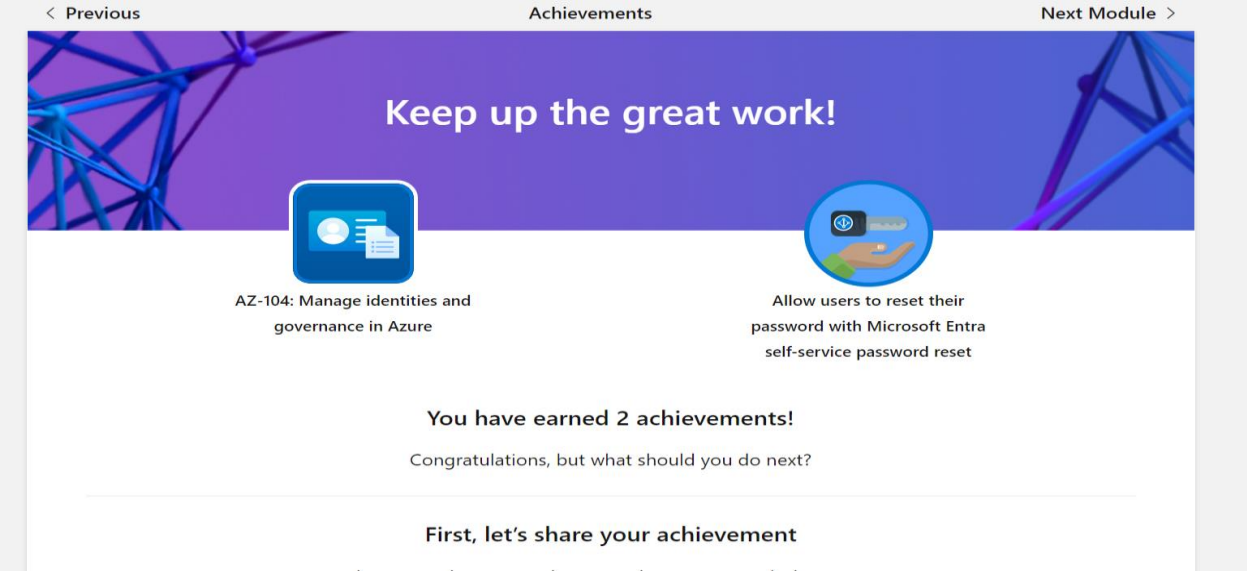
Allow Users To Reset Their Password With Microsoft Entra Self-Service Password Reset

Self-Service Password Reset (SSPR) is a Microsoft Entra feature that enables users to reset their passwords without contacting IT staff for help. SSPR helps reduce the amount of work required from administrators. It also minimizes the productivity impact for users when they forget their password.

In this module, I have learnt how to use self-service password reset (SSPR) in Microsoft Entra ID to allow users to reset their forgotten or expired passwords.

It improves service to end-users by streamlining their password reset request process. It improves enterprise security and reduces the risk of breaches by enforcing strong and secure end-user password controls.

Below is my certificate



Link to verify my achievement

https://learn.microsoft.com/api/achievements/share/en-us/CantonOtieno-0232/3Y5UUVEH?sharingId=17A12B375B49B311

https://learn.microsoft.com/api/achievements/share/en-us/CantonOtieno-0232/AE8RRJS7?sharingId=17A12B375B49B311

Concussion

Through the comprehensive modules on Microsoft Entra and Azure, I have gained valuable insights into various critical aspects of modern identity and access management. The ability to allow users to reset their passwords independently with Microsoft Entra's self-service password reset enhances user autonomy and reduces administrative workload. Securing Azure resources with Azure RBAC and understanding the creation and management of Azure users and groups in Microsoft Entra ID have equipped me with the skills to enforce stringent security measures and manage access effectively. Additionally, configuring Azure Policy and subscriptions, as well as user and group accounts, has provided me with the knowledge to ensure compliance and streamlined resource management. Overall, these modules have significantly deepened my understanding of Microsoft Entra ID's integral role in safeguarding and managing digital environments within the Azure ecosystem.