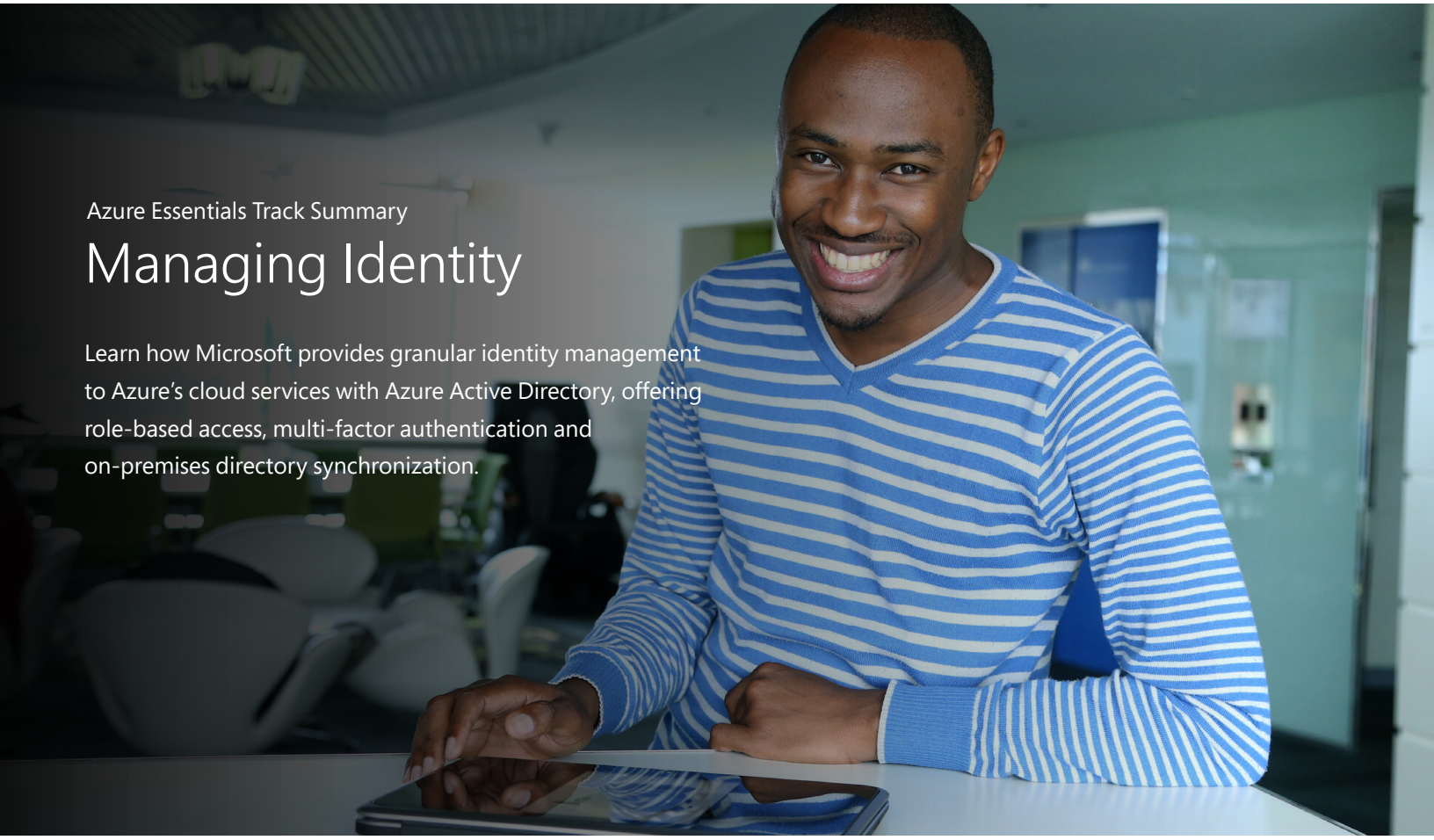
Microsoft Azure Essentials



Azure Essentials Track Summary

Managing Identity

Learn how Microsoft provides granular identity management to Azure's cloud services with Azure Active Directory, offering role-based access, multi-factor authentication and on-premises directory synchronization.

An important part of cloud security is configuring who can access and manage your cloud resources. Identity and Access for Microsoft Azure is one of the most pivotal things every Azure user needs to understand. This brief summary will walk you through the essential topics that you need to know in this area.

AZURE ACTIVE DIRECTORY

At the heart of Identity and Access management for Azure is Azure Active Directory (AD). It's the identity management system for Azure. Every Azure subscription trusts an Azure AD tenant for sign-in; and multiple subscriptions can trust a single Azure AD tenant.

An important tip here if you have an Azure AD work account that you use with Office 365 or other Microsoft services, you can transfer your subscription from your personal account to your work account, which will also move it to your work Azure AD tenant. You can find out more on how to do this, including how to create a subscription using your Azure AD work account at **this link**.

It's important to note that Azure AD is the identity system for all Microsoft business cloud services, such as Office 365, Dynamics 365, and Microsoft Intune. If your organization already has Azure Active Directory, you can use that to sign in to Azure. If you create an Azure subscription using your personal Microsoft account, then a new Azure AD tenant is created for you, and your subscription trusts that tenant.

You can view and manage the users and groups in the directory that can be granted access to Azure resources in the Azure Portal. There, you can also view sign-in activity and other audit logs. You can manage Azure AD from the portal, PowerShell, the Azure CLI and also programmatically using the Microsoft Graph API.

CONNECTING ACTIVE DIRECTORY TO AZURE ACTIVE DIRECTORY

If you have on-premises Active Directory, it's easy to connect it with Azure Active Directory to create a hybrid directory with a single point of management. Using the Azure AD Connect tool you can synchronize users between AD and Azure AD so that they can be managed in one place. You can choose from a variety of options for reduced sign on or single sign in, including hashed password sync, pass through authentication, and standards-based federation using a federation server such as Active Directory Federation Services.

Connecting your Active Directory to Azure AD can reduce management effort and make it easier to comply with policy.

AZURE ROLES BASED ACCESS CONTROL

You can control access to Azure resources by using Roles Based Access Control (RBAC). With Azure RBAC you can grant users the ability to take specific actions on specific sets of resources. Azure comes with three main built in roles, the Owner, Contributor, and Reader roles.

- **The Owner** can perform all actions on all resource types.
- **The Contributor** is similar to the owner role can except it doesn't allow for managing RBAC itself.
- **The Reader** can perform all read actions on all resource types.

Azure also provides a set of resource-specific built in roles for more granular control. For example, the VM Contributor role can perform all actions on VMs, but cannot perform actions on any other resource type. This distinction makes it possible to separate the people who can manage network resources, from the people who can manage VM resources. Using Azure RBAC you can also create custom roles that align exactly to your team's responsibilities. These custom roles can be created using the command line or Azure Resource Manager API.

You can grant access to resources by assigning a user, group, or service principal, such as a process or an application, to a specific role at a specific scope. The scope can be at the level of a subscription, a resource group, or an individual resource such as a VM. When a role assignment is made on a subscription or resource group, the assignment is inherited by the resources in that scope.

Example: if you have been assigned the owner role at the subscription scope, then you have full access to all the resource groups and resources in that subscription. If you have been assigned the owner role at the resource group scope, then you have full access to all resources in that resource group.

In addition to controlling access you can track actions happening in the system with the Activity Log that will show you subscription level events, including RBAC changes.

You can grant access to people from outside their organization with Azure Active Directory B2B. To do this, enter the person's email address when making a role assignment. Azure will then invite the user to become a Guest in your Azure AD. By default, all users can invite guests, but you can also control who can make guest invitations.

If your user account has been granted access to an Azure subscription from another organization, then you can manage that subscription by switching to the other organization's directory using the sign in control in the portal.

AZURE ACTIVE DIRECTORY MULTI-FACTOR AUTHENTICATION

To help you to protect your user accounts, Azure Active Directory supports a range of multi-factor authentication methods, including by phone call, SMS message, or using the Microsoft Authenticator mobile app. Additionally, using the Azure AD Premium conditional access feature, you can configure multi-factor authentication to be required only under certain conditions, such as when users are accessing Azure from home or while traveling, and are not on the work network.

Azure

Take some time to explore all the options for conditional access. For example, you can require multi-factor authentication based on the user's sign-in risk level, and you can limit access to only users on managed devices.

Managing Identity

Demo Topics

AZURE ACTIVE DIRECTORY AS AN IDENTITY PLATFORM FOR AZURE

As an Azure Administrator you want to guard and configure the right permissions on your subscription resources as you operate and consume services in the Cloud. Azure Active Directory is the foundation for all controls and permissions within the Microsoft cloud. When your organization subscribes to Microsoft Azure, you are assigned an Azure tenant. Each Azure tenant provisions a dedicated Azure Active Directory. This directory service is configured to authenticate and authorize you and your users to any subscribed services within your tenant. Using Azure Active Directory, you can manage users individually and create role-based access groups.

ROLE BASED ACCESS CONTROL (RBAC)

Once you've set up Active Directory for your Azure tenant and Integrated it with your on-premises Active Directory, users will be able to sign in with their on-premises identity and password. Now instead of giving everybody unrestricted permissions to your Azure subscription or resources, you can determine the level of access and the types of actions that they can take using RBAC.

MULTIFACTOR AUTHENTICATION (MFA)

The convenience of working from anywhere, anytime also increases the risk of user accounts getting compromised. One of the best ways to mitigate that risk is by enforcing Azure Multi-Factor Authentication (MFA), which is Microsoft's two-step verification solution. It delivers strong authentication via a range of verification methods, including phone call, text message, or mobile app verification. In addition to MFA, you can also utilize Conditional Access feature in Azure AD to apply what actions you want to take such as blocking or limiting access to your resources under specific location or device based circumstances.

PRIVILEGED IDENTITY MANAGEMENT

Azure AD Privileged Identity Management introduces the concept of an eligible admin. Eligible admins should be users that need privileged access now and then, but not every day. The role is inactive until the user needs access, then they complete an activation process and become an active admin for a predetermined amount of time.

Azure

CONTINUE LEARNING

Identity and Access Management is a critical area to understand as an Azure user. You can find out more with these useful resources.

AZURE LEARNING PATHS

Azure Administrator

HANDS-ON LABS

Self-paced Labs

MICROSOFT MECHANICS

Azure Active Directory: Your options from AD sync to the new Pass-through authentication and more

Azure Active Directory B2B Collaboration: simple, secure external sharing of your Apps and Services