**Microsoft Azure Fundamentals: Managing Azure Authentication**

**Azure Authentication Methods**

**Authentication and Authorization**

* Authentication refers to proof of identity
* Authorization refers to access to resources based on assigned permissions

**Authentication**

* Username/password
* Key fob
* Biometric
* Public key infrastructure (PKI) certificate

**Microsoft Entra ID Authentication**

* Users
* Device
* Service principals
* Managed identities

**Multi-factor Authentication (MFA)**

* Something you are
* Something you know
* Something you have
* Something you do

**Azure AD MFA User Settings**

**Ein Bild, das Text, Screenshot, Quittung enthält.

KI-generierte Inhalte können fehlerhaft sein.**

**Azure AD Authentication Methods**

Ein Bild, das Text, Software, Computersymbol, Webseite enthält.

KI-generierte Inhalte können fehlerhaft sein.

**Azure AD Authentication Methods - Microsoft Authenticator**

**Ein Bild, das Screenshot, Text, Software, Webseite enthält.

KI-generierte Inhalte können fehlerhaft sein.**

**Azure Passwordless Login**

**Microsoft Entra ID Passwordless Login**

* Password is not required for authentication
* Password is replaced with a different authentication category such as „something you have“
* This mitigates phising and password spray attacks

**Microsoft Entra ID Passwordless Login**

* Something you have:
  + Windows device
  + Security key fob
  + Smartphone with authenticator app
* Someting you know or are:
  + PIN
  + Fingerprint
  + Facial regocnition

**Windows Hello for Business**

* This is available users have a designated Windows 10/11 PC
* The user device must be registered with an identity provider such as Microsoft Entra ID (for cloud-only deployments)
* Successfull biometric authentication or PIN authentication on the PC unlocks the Windows Hello private key
* The Windows Hello private key is used with the related public key in the identity provider to secure communications

**Microsoft Authenticatior App**

* User possession of their smartphone is used as an additional authenticatin factor
* Support is provided for iOS and Android devices
* User device must be registered with Microsoft Entra ID

**Security Key**

Open authentication standard that supports passwordless login

Fast Identity Online (FIDO2) security key (USB, near-field communication [NFS], or Bluetooth device)

User device must run the latest version of Windows 10 or higher and be joined to Microsoft Entra ID

**FIDO2 Security Key Authentication Method**

**Ein Bild, das Text, Screenshot enthält.

KI-generierte Inhalte können fehlerhaft sein.**

**Web Browser Security Key Sign-In**

**Ein Bild, das Text, Screenshot, Software, Multimedia-Software enthält.

KI-generierte Inhalte können fehlerhaft sein.**

**Enabling Passwordless Login**

Create new user

Add member to group

Users 🡪 . . . 🡪 Per-user MFA 🡪 Enable

Security 🡪 Authentication methods 🡪 Policies 🡪 Add Group (Passwordless)

Devices 🡪 All devices

**Azure Single Sign-On (SSO)**

**Single Sign-on (SSO)**

* Is an Microsoft Entra ID authentication method
* Removes the need to sign in to each app after initial successful authentication

**SSO Methods**

1. Federation
2. Password
3. Linked

**Microsoft Entra ID Enterprise Applications**

**Ein Bild, das Text, Schrift, Screenshot, Visitenkarte enthält.

KI-generierte Inhalte können fehlerhaft sein.**

**Microsoft Entra ID Enterprise App SSO Configuration**

Ein Bild, das Text, Screenshot, Schrift, Design enthält.

KI-generierte Inhalte können fehlerhaft sein.

**Microsoft Entra ID Enterprise App Security Assertion Markup Language (SAML) Configuration**

Ein Bild, das Screenshot, Text, Software, Schrift enthält.

KI-generierte Inhalte können fehlerhaft sein.

**Microsoft Entra ID Enterprise App User Assignment**

**Ein Bild, das Text, Screenshot, Software, Webseite enthält.

KI-generierte Inhalte können fehlerhaft sein.**

**Indentity Federation**

* Identity federation is a centrelazied trusted authenticator
* Authentication capabilities are removed from apps
* Apps rely upon the trusted authenticator
* Trusted authenticator can span organizations

**Trusted Third Party (TTP) Authentication**

**Ein Bild, das Text, Screenshot, Schrift, Design enthält.

KI-generierte Inhalte können fehlerhaft sein.**

**Identity and Resource Providers**

* Identity provider (IdP)
* On-premise or cloud-based
* Resource provider (RP)
* Also called service provider (SP)
* App that trusts the IdP

**Identity Federation Claims**

* Claims are assertions about a user or device
* Claims are contained within a digitally signed security token and are then consumed by apps
* Claim: date of birth, subnet IP, security clearance level, email address

**Microsoft Entra ID App SAML-based Sign-on**

**Ein Bild, das Text, Screenshot, Schrift, Zahl enthält.

KI-generierte Inhalte können fehlerhaft sein.**

**Identity Federation**

Ein Bild, das Text, Schrift, Screenshot, Diagramm enthält.

KI-generierte Inhalte können fehlerhaft sein.

**Service Principals and Managed Identities**

Provide script/code permissions to access Azure resources (ne credentials in code)

**Service Principals**

* Are automatically created in Microsoft Entra ID when an app is registered
* Are used to grant script/code/app permissions to an Azure resource

**Service Principals Types**

Legacy

Application

Managed identity

**Managed Identities**

System-assigned

* Identity is tied tot he life cycle of the associated resource

User-assigned

* Identity is not tied to a specific resource and can be associated with multiple resources

**Virtual Machine Managed Identities**

**Ein Bild, das Screenshot, Text enthält.

KI-generierte Inhalte können fehlerhaft sein.**

**Assigning Permissions to a Managed Identity**

**Ein Bild, das Text, Screenshot, Zahl enthält.

KI-generierte Inhalte können fehlerhaft sein.**

**Managing Service Principals**

Choose Tenant before

Enterprise applications 🡪 All applications 🡪 „Cisco Webex“

App registrations 🡪 Register an application

Storage Account 🡪 „storeacc“ 🡪 Access Control (IAM) 🡪 Add role assignment

**Managing Managed Identities**

Storage accounts 🡪 „storeacc“

Virtual machines 🡪 „ubuntuserv“ 🡪 Identity

Storage accounts 🡪 „storeacc“ 🡪 Access Control (IAM) 🡪 Add role assignment (Managed identity)

Virtual machines 🡪 „ubuntuserv“ 🡪 Identity 🡪 Status On

Storage accounts 🡪 „storeacc“ 🡪 Access Control (IAM) 🡪 Add role assignment (Managed identity)

**Enabling Azure User Account Multi-factor Authentication (MFA)**

Choose Tenant

All users 🡪 . . . 🡪 Per-user MFA 🡪 Enable

**Configuring Azure Active Directory (AD) Conditional Access**

Choose Tenant

Security 🡪 Conditional Access

Licenses 🡪 Products 🡪 Assign license

Users 🡪 Properties 🡪 Location

Security 🡪 Conditional Access 🡪 Create new policy

Security 🡪 Conditional Access 🡪 Named locations 🡪 IP ranges location

Security 🡪 Conditional Access 🡪 Policies 🡪 Create new policy

**Enabling Self-service Password Reset (SSPR)**

Choose Tenant

Security 🡪 Authentication methods

Users 🡪 Password reset

Groups 🡪 „DevGroup“ 🡪 Members

Licenses 🡪 Products