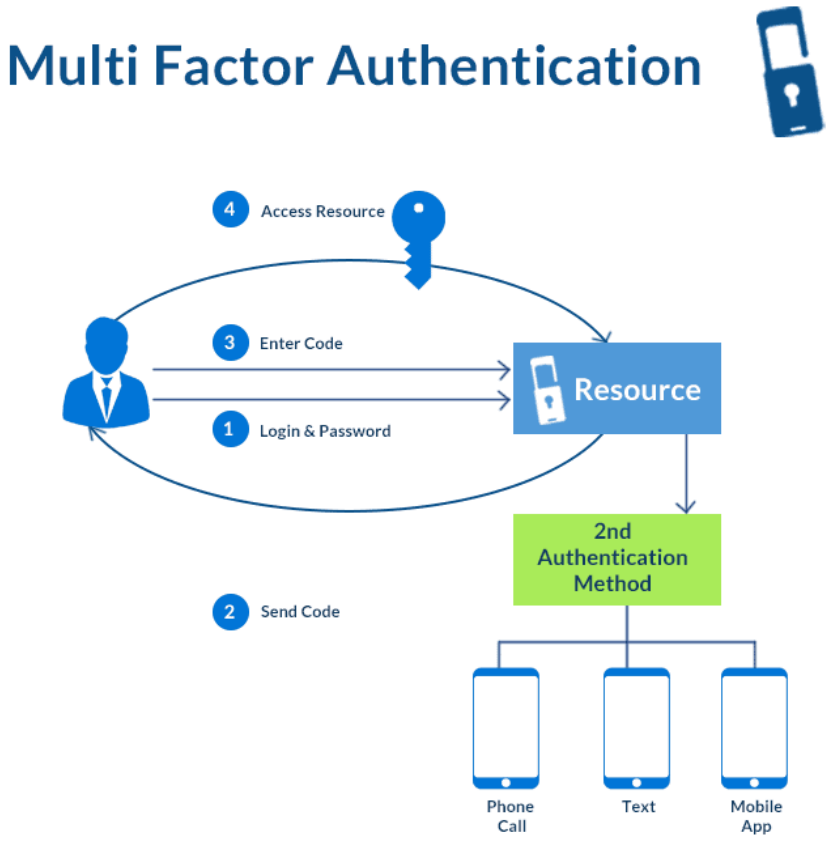
# Azure AD Multi-Factor Authentication

So the term **Authentication** means the process of identifying a user's identity to know whether the user is genuine or not.

## What is Azure Multi-Factor Authentication (MFA)?




Azure Multi-Factor Authentication is an **addition to a two-step verification process**. This becomes quite a challenge for attackers to hack into someone's ID. Even if the hacker or attacker knows the user ID and password, it is useless without an additional authentication method. This is a **trusted security feature** that can guarantee the **solid security** of your accounts. Various methods such as facial recognition, fingerprint access, registered mobile number, etc., are helpful in Multi-Factor Authentication.

## Relevant Authentication Factors

There are a couple of authentication factors available. Let's see them one by one.

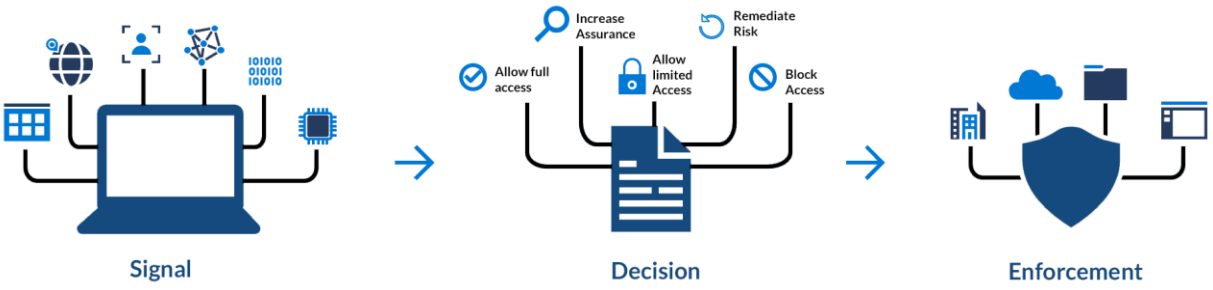
- **Single Factor OTP:** OTP stands for **One-time-Password.** It is a software or hardware token generator that generates one-time passcode to authenticate the user. There is not any need for a second channel to receive the passcode because the password is generated with the device clock and seed value. This passcode is valid for a limited time and gets changed when you request a new OTP. When you enter this OTP into the system, this OTP also gets verified at the server-side to confirm whether the genuine user is requesting to log in.
- **Memorized secret:** It is a **static pin code** assigned to the user for authentication when the users use the Azure MFA server on-premises.
- **Out of Band Device:** It is another method of authentication. Out of Band Device is a **physical device** that can communicate securely over a distinct communication channel. If we talk about Azure MFA, this device is your mobile phone, and the secondary network is your internet when you use Microsoft authenticator APP.

## How can Azure MFA verify a user's identity?

There are multiple ways Azure MFA can verify a user's identity.

- **Phone call:**
  - The user responds to the call by pressing #
  - Azure MFA can choose caller ID
  - Optional Pin code
- **Text Message**
  - there can be a one-way message
  - There can also be a two-way message
  - Optional Pin Code via Azure MFA Server
- **Microsoft Azure Authenticator App**
  - It authenticates through Push Verification
  - Optional Pin Code

## What is Conditional Access?




Conditional access is a great feature available for administrators to **track users** and **protect an organization's data**. Admins can **block or grant access to users** using conditional access. Conditional access can be implemented with IP locations, types of devices, certain users or groups, etc. There are various Azure Active Directory plans available. Plan 1 is relied on the group, location, device status, etc., whereas plan 2 has risk-based access policies. The basic conditional access helps to reduce MFA prompts and uses a second factor such as connection in an organizations' office or a domain-joined PC.