

Multifactor Authentication with Azure Conditional Access

Authentication in Azure

Icon

Description automatically generated with medium confidence

BY

Timothy Fabelurin

## Multifactor Authentication

This is a process where user is required to provide an additional form of identification when signing in. Security is increased when this second form of identity is not easy for an attacker to obtain. For example, fingerprint scan, mobile phone code.

With MFA enabled and enforced using conditional access policies, cloud-based applications access was restricted, and all affected users need to authenticate with either SMS, Phone call or Microsoft Authentication App in conjunction with their passwords. Conditional access policy can be applied to only provide access at a particular location or range of IP address or operating system (windows, ios, android, macOS etc). With this measure in place, security is enhanced on the platform.

1. Below indicates different available policy templates that can be implemented. Care must be taken however, in ensuring that there is an account that can be used to salvage a scenario of total lockout of the platform due to configuration error.

Graphical user interface, text, application

Description automatically generated

1. Across the whole tenant (Cloud environment), It is possible to individually or collectively either disable, enable, or enforce MFA on users by the admin. General settings was also set up. For instance, “Trusted IP ranges” and verification methods can be configured.

Graphical user interface

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

1. MFA is often used in conjuction with Conditional access. The conditional access policy provide different security settings options by which if any of the conditions are met, there system triggers one or couple of actions before authentication is passed.

Graphical user interface, text, application, email

Description automatically generated

Conditional access policy page on Azure Portal

1. There are diffent levels of decisions that need to be made and this has a lot to do with the organisational policies. Few of those include,
2. Types of users – Guest users, all users or specific users
3. Applications to effect this policy on – Office 365, Azure, Power analytics etc
4. Conditions – Places consider as “High-risk” locations, IP address out the Trusted range, types of devices (ios, windows, mac etc), State of device (Domain joined, hybrid joined etc)
5. Access Control – This is the point decision to either Grant or Block is decided and what more measure are needed for authentication to be passed.

Below images shows few steps taken when configuring the test scenario.

Graphical user interface, application, Teams

Description automatically generated

Graphical user interface, application

Description automatically generated Background pattern

Description automatically generated with medium confidence

1. Using a user ([tim@fabbietygmail.onmicrosoft.com](mailto:tim@fabbietygmail.onmicrosoft.com)) in the tenant as a use case, additional verification information was required at the instance of login into azure application, being the first time after the settings were effected.

Graphical user interface, text, application, email

Description automatically generated

1. Text message for verification code from microsoft as that was te choice of verification method selected. This is required for a successful authentication even after the user has provided correct password.

Graphical user interface, text, application, chat or text message

Description automatically generated

Graphical user interface, application

Description automatically generated