MULTI-FACTOR AUTHENTICATION

Companion Guide for **AZ-104 Exam Prep: Microsoft Azure Administrator**

Contents

Introduction

This companion guide for the "Multi-Factor Authentication" section of AZ-104 Exam Prep: Microsoft Azure Administrator is intended to provide some background context and use cases for topics covered in this section. Combining this information with the demos and hands-on labs should ensure you have a full grasp of the topics in this section of the course.

Fraud Alerts

Fraud alerts allow users to report fraudulent attempts to access their resources. When a suspicious MFA prompt is received by the user, the affected user can report the fraud attempt through the Microsoft Authenticator app or via their phone.

There are two fraud alert options available:

- **Automatically block users who report fraud:** When fraud is reported by a user, the Azure AD MFA authentication attempts for the affected account are blocked for 90 days - or until an admin unblocks the account.
- **Code to report fraud during initial greeting:** When a user receives a phone call as part of an MFA verification, they normally press # to confirm their sign-in. However, to report fraud, the user, instead, enters a code before pressing #. This code is 0 by default, but you can customize it.

Trusted IPs

Trusted IPs is a feature of Azure AD Multi-Factor Authentication that allows a user to bypass multi-factor authentication prompts when signing in from a defined IP address range. Organizations will usually set trusted IP ranges that reflect their on-prem environments, so when users login from their on-prem networks, there's no Azure AD Multi-Factor Authentication prompt.

It's important to note, however, that trusted IPs can include private IP ranges only when you use MFA Server. When using cloud-based Azure AD Multi-Factor Authentication, you can only use public IP address ranges.

Verification Methods

There are several verification methods to choose from, when configuring MFA. When users enroll their accounts for MFA in Azure AD, they are prompted to choose their preferred verification method. The choices they are presented are controlled by the admin, meaning the options enabled by the admin are those that the user gets to choose from.

The following verification methods are available:

- **Call to phone:** Places an automated voice call. The user answers the call and presses # in the phone keypad to authenticate. The phone number is not synchronized to on-premises Active Directory.
- **Text message to phone:** Sends a text message that contains a verification code. The user is prompted to enter the verification code into the sign-in interface. This process is called one-way SMS. Two-way SMS means that the user must text back a particular code. Two-way SMS is

deprecated and not supported after November 14, 2018. Administrators should enable another method for users who previously used two-way SMS.

- **Notification through mobile app:** Sends a push notification to your phone or registered device. The user views the notification and selects Verify to complete verification. The Microsoft Authenticator app is available for Windows Phone, Android, and iOS.
- **Verification code from mobile app or hardware token:** The Microsoft Authenticator app generates a new OATH verification code every 30 seconds. The user enters the verification code into the sign-in interface. The Microsoft Authenticator app is available for Windows Phone, Android, and iOS.