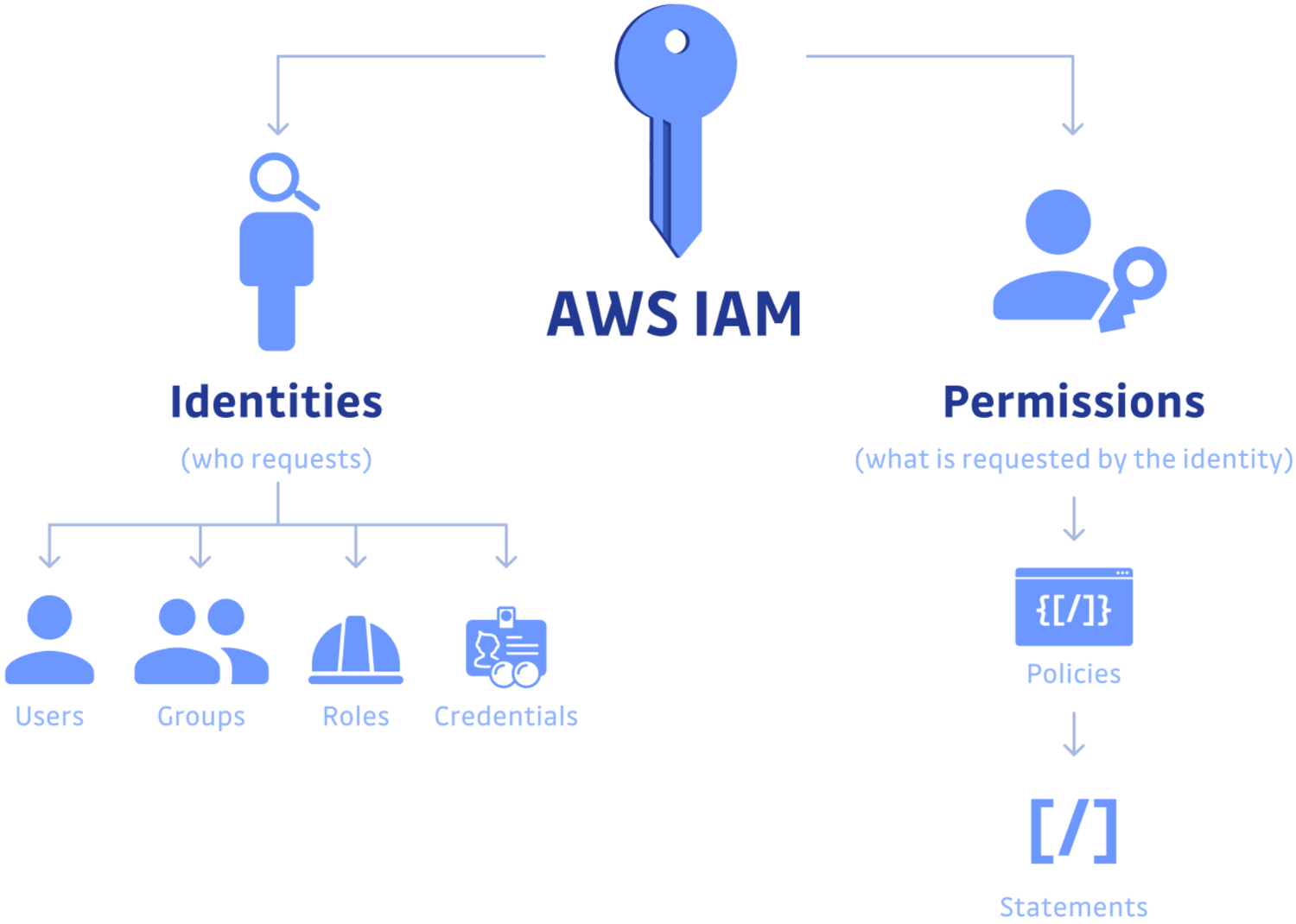
iamneo

# IAM and MFA

# Agenda

- IAM Overview
- Roles of IAM in AWS Security
- Simple and Secure
- Control Access
- Centralize Management

# Users, Groups, Roles, and Policies in IAM



# IAM Best Practices

- Use temporary credentials
- Use IAM Access Analyzer
- Require multi-factor authentication (MFA)
- Set permissions guardrails across multiple accounts
- Rotate access keys regularly for use cases that require long-term credentials
- Safeguard your root user credentials and don't use them for everyday tasks
- Use permissions boundaries to delegate permissions management within an account.
- Use strong and unique passwords for IAM users and root accounts, and avoid sharing or reusing passwords.

# Multi-Factor Authentication (MFA)

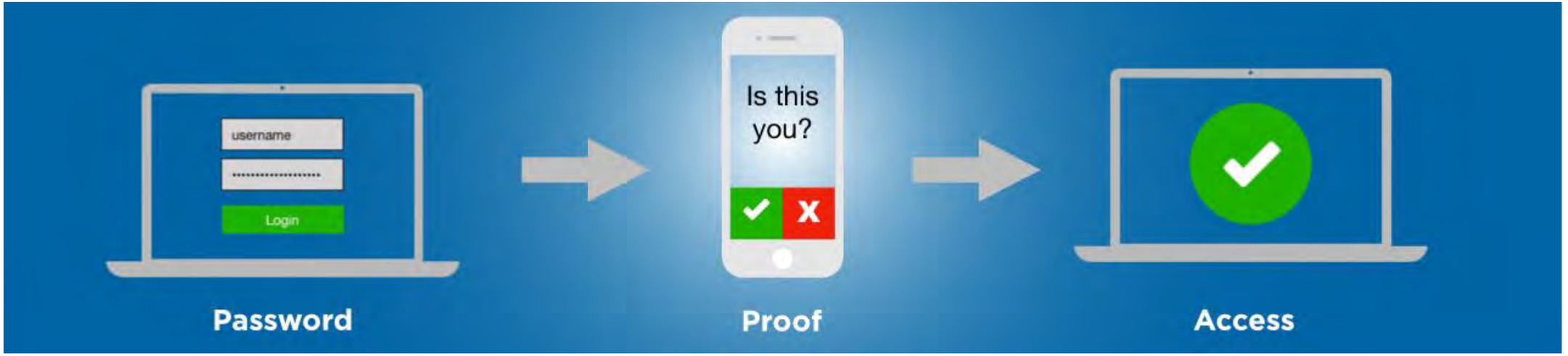
MFA is to enhance account security for IAM users and root accounts. MFA adds an extra layer of security to protect user accounts from unauthorized access and data breaches, which can lead to financial losses and reputation damage. Implementation of MFA has become increasingly important in today's digital age.

# The Importance of MFA

**Phishing attacks:** MFA helps to prevent unauthorized access to user accounts, even if the user's password has been compromised in a phishing attack.

**Stolen credentials:** Even if a hacker manages to steal a user's credentials through malware or other means, MFA can help to prevent access to user accounts.

**Ransomware:** Even if a hacker manages to steal a user's credentials through malware or other means, MFA can help to prevent access to user accounts.



# Types of MFA in AWS IAM

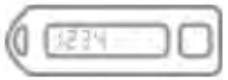
Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.

**Authenticator app**

Authenticate using a code generated by an app installed on your mobile device or computer.

**Security Key**

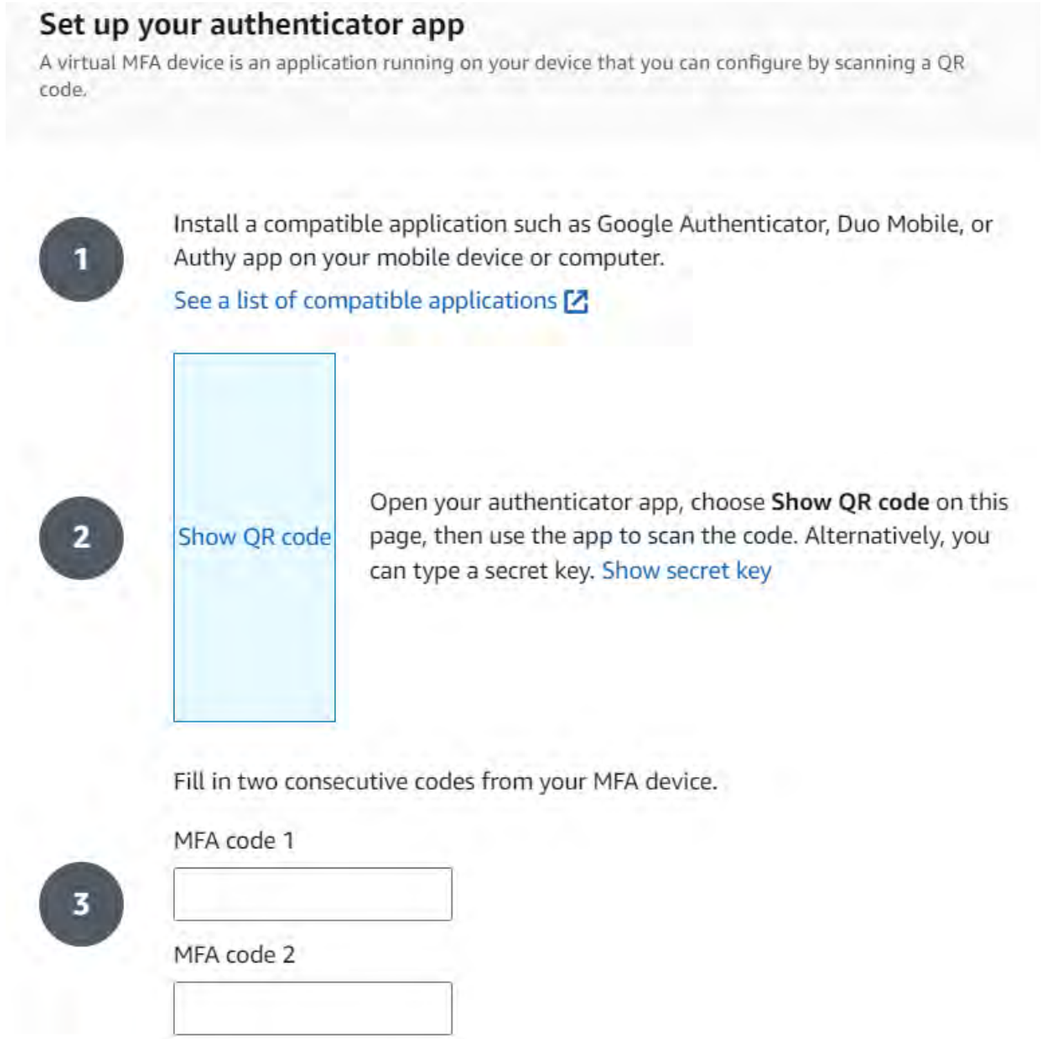
Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.



**Hardware TOTP token**

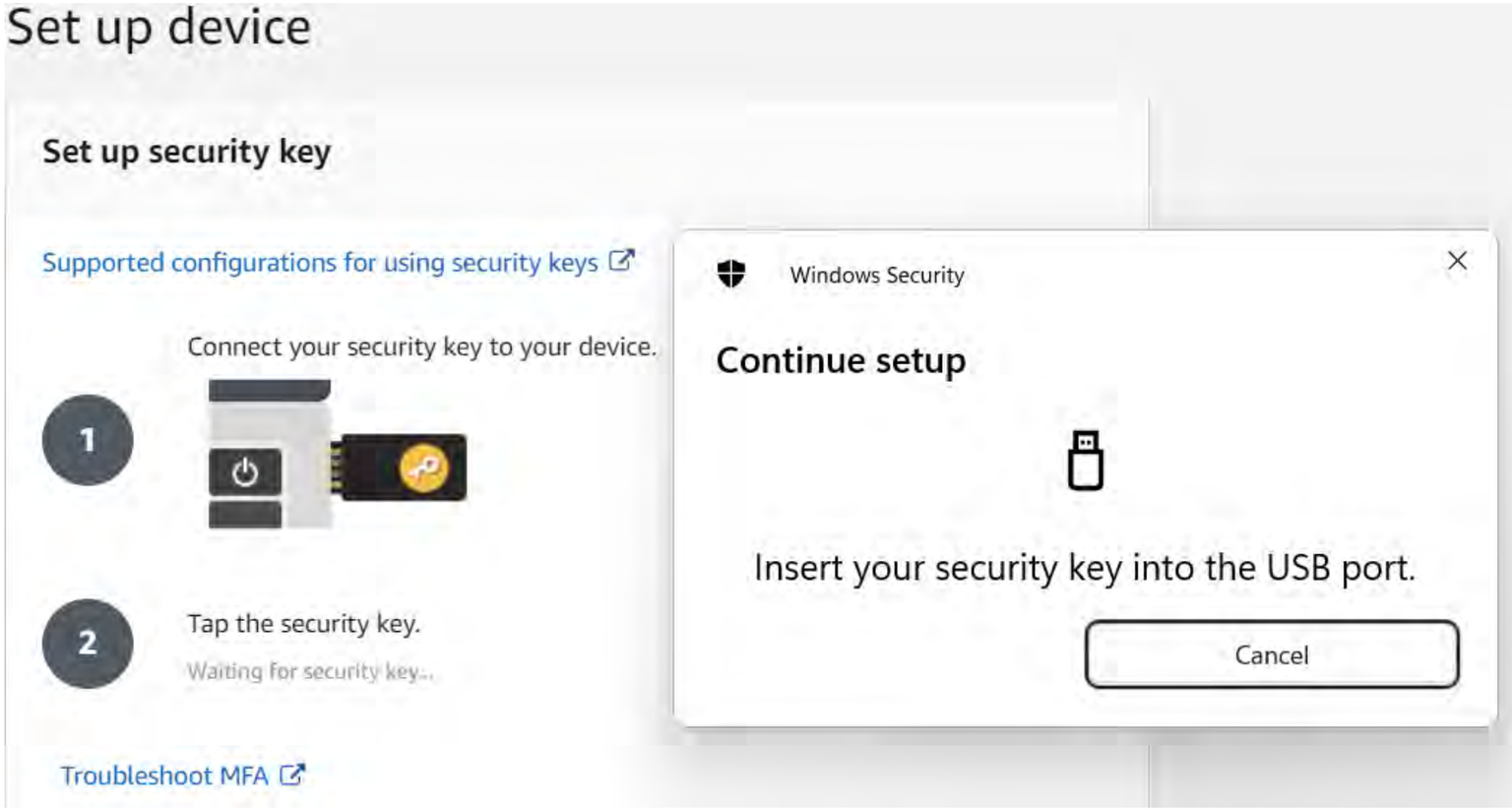
Authenticate using a code displayed on a hardware Time-based one-time password (TOTP) token.

# MFA Authenticator app



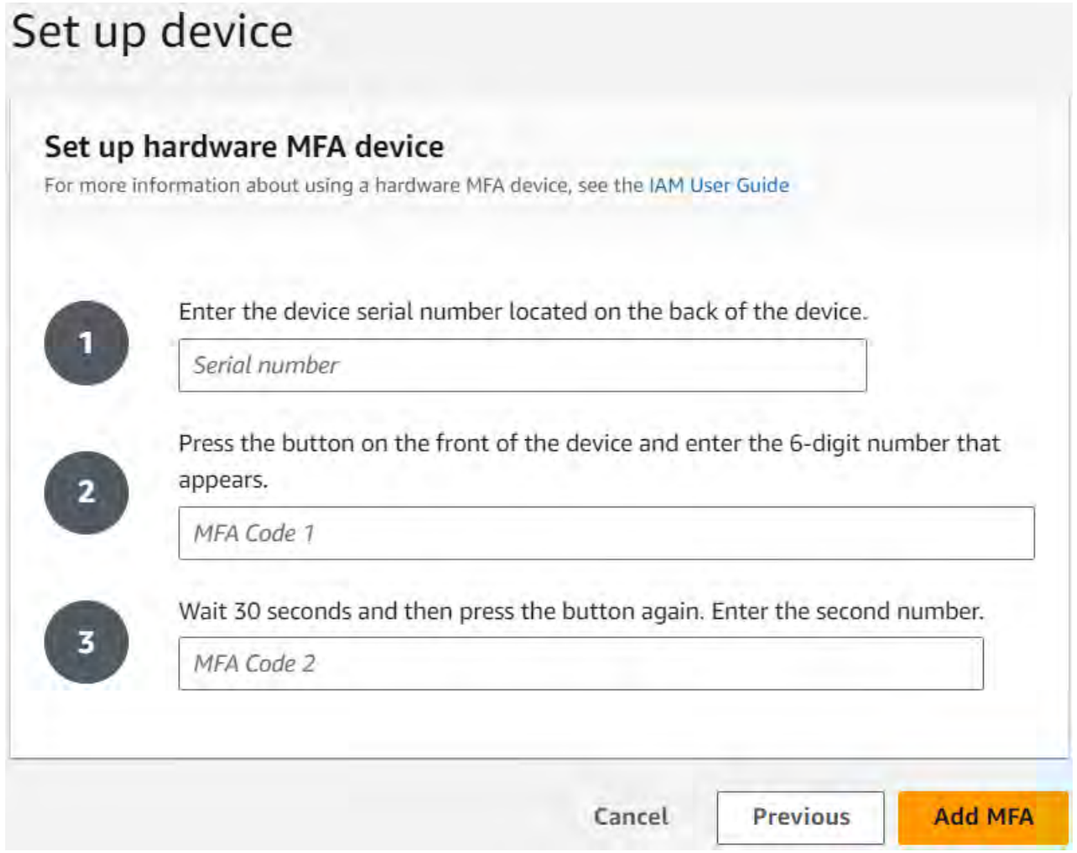
# Security Keys

Security keys are USB devices that provide an extra layer of security by requiring physical access to a device to log in.



# Hardware MFA Devices

A hardware key fob token is a small, physical device that generates Time-based one-time password (TOTP) token that is required for login.



# Configuring MFA for IAM Users

Implementing MFA for IAM users can provide an additional layer of security for their AWS account access.

| Step | Description |
| --- | --- |
| 1 | Login to AWS Console |
| 2 | Select IAM from the list of services |
| 3 | Click on "Users" from the left navigation menu |
| 4 | Select the user to whom MFA has to be added |
| 5 | Click on the "Security Credentials" tab |
| 6 | Click "Activate MFA" and follow the prompts to configure and set up MFA |

# Configuring MFA for Root Accounts

MFA for the AWS root account provides an additional level of security and helps to prevent unauthorized access to the account.

1

## Steps to Configure MFA for Root Account:

Login to the AWS Management Console, go to the Account Settings page, click on "Security Credentials", select "Activate MFA", and follow the prompts to set up MFA.

2

## Additional Security Benefits

MFA for the AWS root account can help to prevent accidental or deliberate changes to critical account settings, which could result in detrimental business impact.

3

## Importance of protecting root account

Root account access should be limited to only a few trusted individuals to reduce the risk of a security breach.

iamneo

# Thankyou