Authentication vs. authorization

Sachin Raaghav
Apr 20 · 10 min read

The terms authentication and authorization may sound similar, but they are distinct when it comes to their core functions. Authentication and authorization are security processes that are executed when users try to access their resources. Authentication and authorization play vital roles in preventing cybersecurity breaches and bolstering the security system of an organization.

- **Authentication:** Verifying the identity of a user—who is the user?
- **Authorization:** Checking if the user has permission to access resources—what resources can the user access?

What is authentication?

Authentication is the process of verifying a user's identity who requires access to resources such as applications, systems, and networks. Access to these resources is only permitted if the user is successfully authenticated after entering the credentials or other modes of authentications such as biometrics.

What is authorization?

Authorization is the process of validating the user to check if the user has the privileges to access a specific system, application, or network. Authorization is associated with control of access and user privileges. Factors such as the user's age, role, and other metadata play an important role in the authorization process.
To access a resource, the user is authenticated first and then authorized.

Different methods of authentication

Using passwords

This is an authentication process in which a password is a combination of letters, numbers, and special characters. Simple passwords are created by users so that they can easily remember them, but this makes their accounts vulnerable to hackers. Hackers gain access to the user's account by continuously trying out different combinations of letters, numbers, and special characters. A long (more than 10 characters) combination of different characters, letters, and numbers is recommended for passwords.

Using biometrics

This is an authentication process that involves utilizing the user's biological information for identity verification. Biometrics are convenient to use and are faster when compared to passwords. Some biometrics used frequently are as follows:

Biometric	Authentication factor
Fingerprint recognition	Authentication is based on the unique fingerprint pattern of the user.
Facial recognition	Authentication is based on the unique facial characteristics of the user.
Retina/iris scanners	Authentication is based on the unique pattern of a person's iris.

Token-based authentication

Authentication is based on a unique, encrypted string of characters. A token-based authentication application sends an encrypted text to the user's smartphone or email; the user has to enter this encrypted text to gain access to their resources.

Multi-factor authentication (MFA)

Multi-factor authentication involves two or more authentication methods. For example, a user's fingerprint and one-time password (OTP) sent to the user's smartphone are required to log in.

Here's a tip: Using AD360, you can seamlessly manage passwords and prevent security threats such as malicious logins and password attacks. AD360 provides a wide range of authentication factors, including fingerprint and Face ID authentication, YubiKey, Google Authenticator, push notification, and SMS verification. With its user-friendly interface and threat intelligence mechanism you can bolster your organization's security in just a few clicks.

Different types of authorization

ABAC authorization

Attribute-based access control (ABAC) authorization is related to a specific user attribute. Information such as age, demographics, and relationships are some attributes of a user. ABAC authorization is executed when the user is trying to access the resources; it requires a specific attribute for granting permissions to the user.
For example, a voting system will only authorize the permission to vote if the user's age is 18 or greater.

RBAC authorization

Role-based access control (RBAC) authorization is related to the role of the user, not the user directly. In an organization, different users have different roles. In this authorization method, permission to use a resource is only granted if the role of the user has the privilege

to access the resource.

For example, the ability to onboard or offboard an employee is only possible if the user account has an HR role.

Comparison of authentication and authorization

Authentication	Authorization
Authentication verifies the user's identity	Authorization checks if the user has the privilege to access the resources
Authentication is processed before authorization	Authorization is processed after authentication
Visible to the user	Not visible to the user
Data for authentication moves as an ID token	Data for authorization moves as an access token
The authentication process is managed by user credentials, biometrics, OTPs, or other applications	The authorization process is managed by IT administrators or IT security
Authentication processes like login credentials are partially changeable by the user	Authorization settings cannot be changed by the user; they can only be changed by the IT administrators or IT security teams

Strengthening security via authentication and authorization

Technology advances every day, and many organizations are also adapting quickly. IT administrators need to ensure that their organization's security system is updated. The authentication and authorization procedure is a critical component of any security system. When dealing with an organization's sensitive data assets, both authentication and authorization are essential; neglecting either of these processes would leave the organization vulnerable to data breaches and illegal access.

Organizations are gradually moving away from passwords and toward authentication apps and biometrics, which provide a better user experience and better security. There are various types of authentication and authorization methods that can be implemented accordingly to fortify an organization's security system.

Actionable IAM insights straight to your inbox

One email. Every month.

Email ID KR Subscribe now

By clicking **Subscribe now**, you agree to processing of personal data according to the Privacy Policy.

Join 40,000+ Readers 

ManageEngine
AD360

AD360 is an integrated identity and access management (IAM) solution for managing user identities, governing access to resources, enforcing security, and ensuring compliance.

INDUSTRY SOLUTIONS

Healthcare

Finance and banking

Education

Government

RESOURCES

E-Books

Blogs

Case Studies

Webinars

FAQs

NAVIGATION

Home

Awards

Demo

Pricing

Download

© 2023 Zoho Corporation Pvt. Ltd. All rights reserved.