Authentication vs. Authorization

Authentication and authorization might sound similar, but they are distinct security processes in the world of identity and access management (IAM).

Authentication confirms that users are who they say they are. **Authorization** gives those users permission to access a resource.

What Is Authentication?

Authentication is the act of validating that users are whom they claim to be. This is the first step in

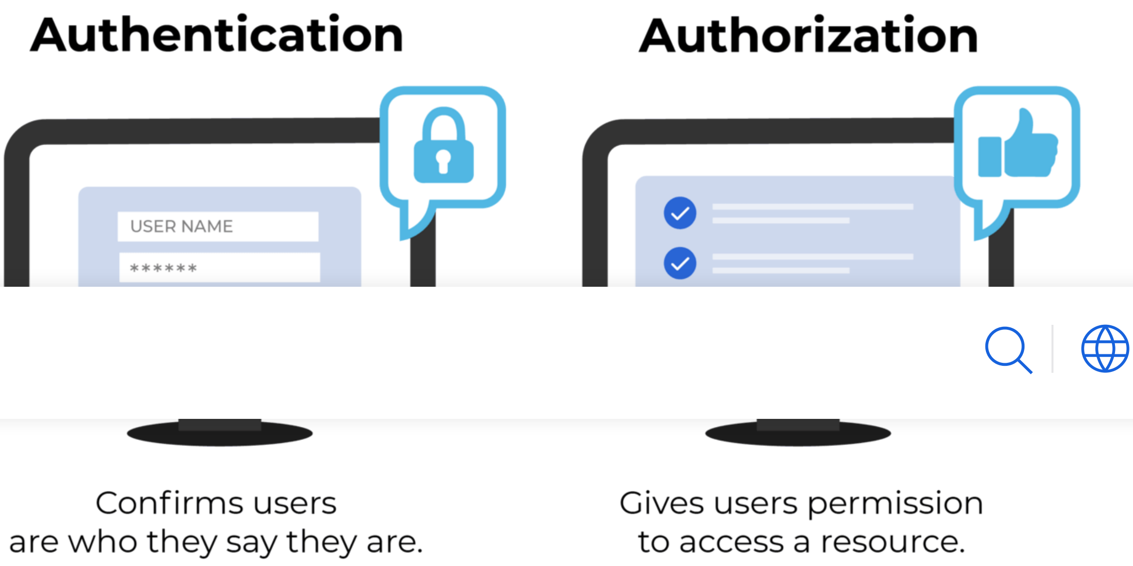
- **Passwords.** Usernames and passwords are the most common authentication factors. If a user enters the correct data, the system assumes the identity is valid and grants access.
- **One-time pins.** Grant access for only one session or transaction.
- **Authentication apps.** Generate security codes via an outside party that grants access.
- **Biometrics.** A user presents a fingerprint or eye s

What Is Authorization?

Authorization in a system security is the process of giving the user permission to access a specific resource or function. This term is often used interchangeably with access control or client privilege.

Giving someone permission to download a particular file on a server or providing individual users with administrative access to an application are good examples of authentication.

In secure environments, authorization must always follow authentication. Users should first prove that their identities are genuine before an organization's administrators grant them access to the requested resources.


Authentication
Authorization
USER NAME
******
Confirms users are who they say they are.
Gives users permission to access a resource.

Authentication vs. Authorization

Let's use an analogy to outline the differences.

Consider a person walking up to a locked door to provide care to a pet while the family is away on vacation. That person needs:

- **Authentication**, in the form of a key. The lock on the door only grants access to someone with the correct key in much the same way that a system only grants access to users who have the correct credentials.
- **Authorization,** in the form of permissions. Once inside, the person has the authorization to access the kitchen and open the cupboard that holds the pet food. The person may not have permission to go into the bedroom for a quick nap.

Authentication and authorization work together in this example. A pet sitter has the right to enter the house (authentication), and once there, they have access to certain areas (authorization).

	Authentication	**Authorization**
What does it do?	Verifies credentials	Grants or denies permissions
How does it work?	Through passwords, biometrics, one-time pins, or apps	Through settings maintained by security teams
Is it visible to the user?	Yes	No
How does data move?	Through ID tokens	Through access tokens

Systems implement these concepts in the same way, so it’s crucial that IAM administrators understand how to utilize both:

- **Authentication.** Let every staff member access y le nt credentials in response to your chosen authentication requirements.

Understand the difference between authentication and authorization, and implement IAM solutions that have strong support for both. You will protect your organization against data breaches and enable your workforce to be more productive.

Granting Permissions with Okta

Okta Lifecycle Management gives you an at-a-glance view of user permissions, meaning you can easily grant and revoke access to your systems and tools as needed. Meanwhile, Okta Adaptive MFA lets you safeguard your infrastructure behind your choice of authentication factors.

For example, make production orders accessible only to certain users who may then have to authenticate using both their company credentials and voice recognition.

The opportunities to streamline IAM in your organization are endless. Find out how Okta can keep you, your employees, and your enterprise safe.

Learn more

Want to know how else Okta can help with authentication and authorization? Check out our page on Privileged Access Management.

Quick Links

Pricing

Careers

Support

Press Room

It’s time to move on from Active Directory.

Identity 101

Contact Us

Customer Experience Center

Solutions

Move to the Cloud

Adopt a Zero Trust Security Model

Improve M&A Agility

Reduce IT Friction

Collaborate with Partners

Securely Enable Remote Work

Cultivate User Trust

Enhance Customer Engagement

Modernize Infrastructure

Transform Into a Digital Platform

View All ›

Products

- Single Sign-On
- Multi-factor Authentication
- Lifecycle Management
- Universal Directory
- API Access Management
- Advanced Server Access

Customer Identity

Hey there! Back again to check us out? Things must be getting serious!

1

- B2B Integration
- Lifecycle Management
- User Management

Okta Integration Network

Platform Services

Privacy Policy Security FAQ Sitemap Visit our Developer Site

United Kingdom

France

Germany

Japan