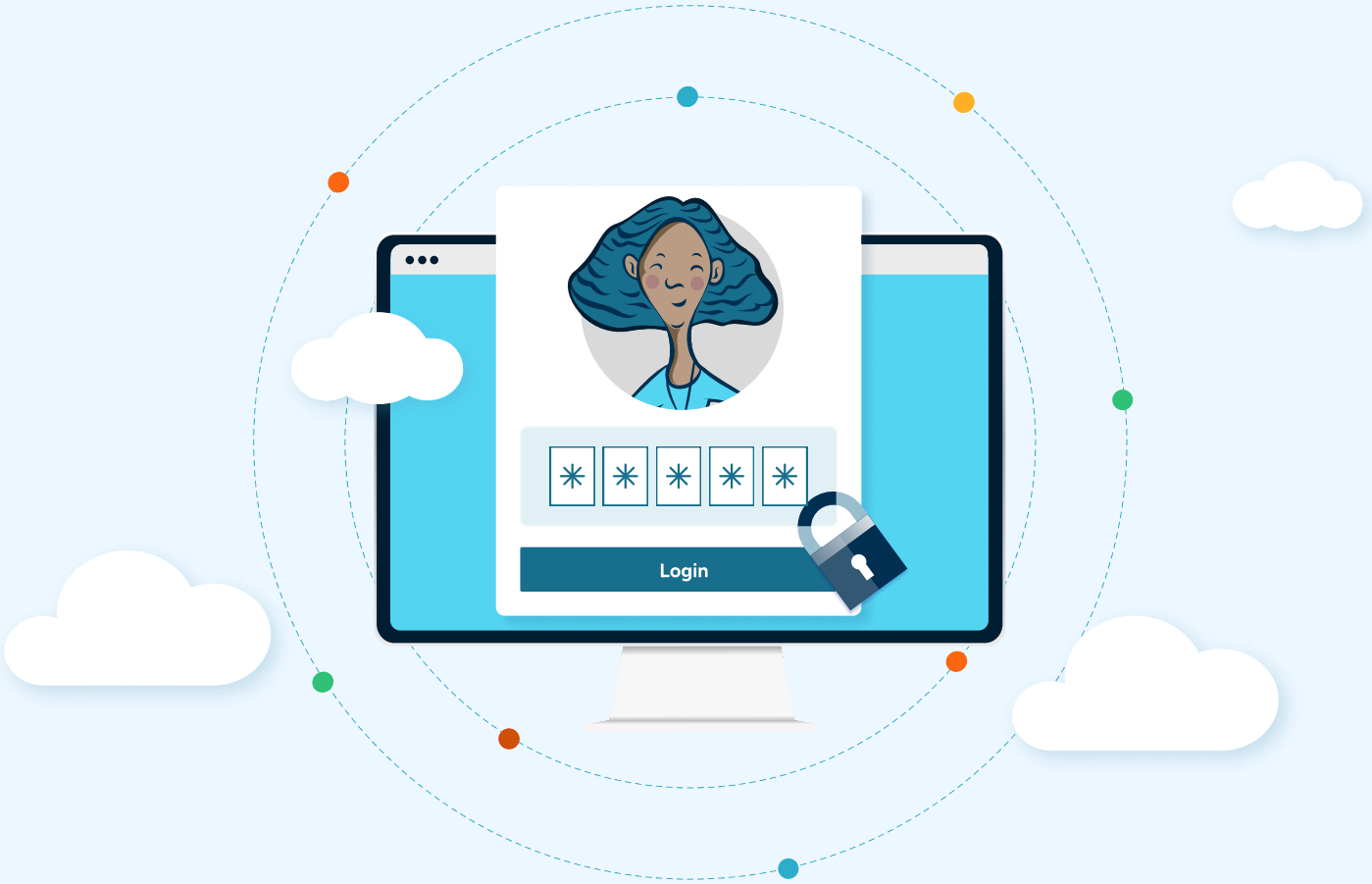
The Definitive Guide to Authentication

strongdm

Table of Contents



Good cybersecurity relies on granting the right people access to the right information at the right time. But how do you ensure the users trying to access your systems are who they say they are? Authentication. In this ebook, we'll take a comprehensive look at authentication, including what it is, how it works, and what the future of authentication looks like. By the end of this piece, you'll understand the different types of authentication, the three main authentication factors, and how authentication is used to secure data and systems from threats.

01

What is Authentication?

Authentication is the process of verifying a user or device before allowing access to a system or resource.

In other words, authentication means confirming that a user is who they say they are. This ensures only those with authorized credentials gain access to secure systems. When a user attempts to access information on a network, they must provide secret credentials to prove their identity. Authentication allows you to grant access to the right user at the right time with confidence. But this doesn't occur in isolation.

Authentication is part of a three-step process for gaining access to digital resources:

1. **Identification—Who are you?**
2. **Authentication—Prove it.**
3. **Authorization—Do you have permission?**

Identification requires a user ID like a username. But without identity authentication, there's no way to know if that username actually belongs to them. That's where authentication comes in—pairing the username with a password or other verifying credentials.

The most common method of authentication is a unique login and password, but as cybersecurity threats have increased in recent years, most organizations use and recommend additional authentication factors for layered security.

02

History of Authentication

Digital authentication goes back to the 1960s when modern computers became available at large research institutes and universities. Back then, computers were massive—often taking up entire rooms—and a scarce resource. Most universities that had a computer only had one. That meant students and researchers had to share it. But this also meant that users could access other users' files without limitation.

When Fernando Corbato, a student at MIT, noticed this weakness, he created a basic password program that prompted the user to enter their password and saved it within a plaintext file in the file system. From there, digital authentication was born.

A Timeline of Digital Authentication

1960S: PASSWORDS AND ENCRYPTION

In 1961, Corbato created a password program to use on the MIT computer system. By the late 1960s, programmers worked to develop a stronger password solution—one that wasn't stored in plaintext files. Robert Morris, a cryptographer at Bell Labs, developed a password encryption scheme while working on Unix. It used a key derivation function that calculates a secret value and makes it easy to compute in one direction, but not in the opposite.

1970S: ASYMMETRIC CRYPTOGRAPHY

Asymmetric cryptography, also known as public-key cryptography, uses a mathematically related pair of keys—one public and one private—to encrypt and decrypt information. Asymmetric cryptography was developed in the 1970s by UK government employees, James Ellis, Clifford Cocks, and Malcolm J. Williamson. However, this knowledge was not made public until 1997.

1980S: DYNAMIC PASSWORDS

Traditional passwords quickly became insufficient as technology advanced. Passwords were easily guessable, and many people reused their passwords, making them vulnerable. So computer scientists developed dynamic passwords. Dynamic passwords change based on variables like location, time, or a physical password update. Eventually, two dynamic password protocols were introduced:

TOTP—Time-based One-Time Password (OTP), where the password is generated based on the time requested.

HOTP—HMAC (Hash-based Message Authentication Code) OTP is an event-based OTP, where the password is generated by a hash code that uses an incremental counter.

Dynamic passwords are often used in combination with regular passwords as one form of two-factor authentication.

1990S: PUBLIC KEY INFRASTRUCTURE

Once asymmetric cryptography was made public, computer scientists built on that work and standardized it through the development of public key infrastructure (PKI). PKI defined how to create, store, and send digital certificates—adding more robust protection for online users and communication.

2000S: MULTI-FACTOR AUTHENTICATION AND SINGLE SIGN-ON

By the early 2000s, programmers built stronger authentication technologies with layered protections.

Multi-factor authentication required users to provide two forms of verification before gaining access. And single sign-on (SSO) streamlined the verification process so that users only have to provide credentials at one access point—verified by a trusted third party.

2010S: BIOMETRICS

Before the 2010s, biometric authentication was reserved for high-security government access and spy movies. But with the advancement of recent technology, biometrics is now a common form of authentication—including fingerprint TouchID and FaceID on smart devices.

03

Importance of Authentication

Cyberattacks are a critical threat to organizations today. As more people work remotely and cloud computing becomes the norm across industries, the threat landscape has expanded exponentially in recent years. As a result, **94% of enterprise organizations have experienced a data breach—and 79% were breached in the last two years**, according to a **recent study** by the Identity Defined Security Alliance (IDSA).

Additionally, research by Cybersecurity Insiders found that **90% of survey respondents experienced phishing attacks** in 2020, and another 29% experienced credential stuffing and brute force attacks—resulting in significant helpdesk costs from password resets.

With global **cybercrime costs expected to grow by 15%** per year over the next five years, reaching $10.5 trillion USD annually by 2025, it's more important than ever for organizations to protect themselves.

As a result, authentication has become an increasingly important mitigation strategy to reduce risk and protect sensitive data. Authentication helps organizations and users protect their data and systems from bad actors seeking to gain access and steal (or exploit) private information. These systems can include computer systems, networks, devices, websites, databases, and other applications and services.

Organizations that invest in authentication as part of an identity and access management (IAM) infrastructure strategy enjoy multiple benefits, including:

- Limiting data breaches
- Reducing and managing organizational costs
- Achieving regulatory compliance

The Rise of Multi-Factor Authentication

One of the most **important ways to protect data** is through multi-factor authentication (MFA). The **2021 DBIR report** found that credentials are the most frequently compromised data in a breach—especially in a phishing attack, which typically goes after the victim's credentials to gain further access to the target organization.

But multi-factor authentication adds another layer of verification that can help thwart these kinds of attacks. In other words, even if hackers steal your credentials, that won't be enough to get into the system.

Microsoft and Google have both recently touted the **benefits of including multi-factor authentication** in their own security hygiene best practices:

"Our research shows that simply adding a **recovery phone number to your Google Account can block up to 100% of automated bots, 99% of bulk phishing attacks, and 66% of targeted attacks** that occurred during our investigation," Google shared.

Microsoft found that **enabling MFA blocks 99.9% of unauthorized login attempts—even if hackers have a copy of a user's current password.** This is especially important as passwords alone are no longer enough to protect accounts, explains **Alex Weinert**, Group Program Manager for Identity Security and Protection at Microsoft.

Advances like multi-factor authentication are essential to a layered mitigation strategy that reduces the risk of unauthorized access and brute force attacks so organizations and users can confidently secure their accounts and other important data.

04

Authentication Use Cases

Today, authentication is common practice not only among IT professionals and scientists, but for non-technical users as well. Whether they're logging in to Facebook with a username and password or opening a phone with TouchID or a unique PIN, most people have used authentication to access their private information and devices at home and at work.

Of course, as technology has advanced and hackers have become more adept and widespread, new methods of authentication are gaining traction to better secure personal, business, and government resources from unauthorized access. We'll talk more about these methods below.

05

How Does Authentication Work?

Basic authentication involves proving a user is who they say they are through authentication methods such as a username and password, biometric information such as facial recognition or fingerprint scans, and phone or text confirmations (which are most often used as part of two-factor authentication methods).

But how does authentication work on the backend?

For identity authentication with a login and password (the most common form of authentication), the process is fairly straightforward:

1. **The user creates a username and password to log in to the account they want to access. Those logins are then saved on the server.**
2. **When that user goes to log in, they enter their unique username and password and the server checks those credentials against the ones saved in its database. If they match, the user is granted access.**

Keep in mind that many applications use cookies to authenticate users after the initial login, so they don't have to keep signing in to their account every time. Each period during which a user can log in without having to re-authenticate is called a session. In order to keep a session open, an app will do two things when the user logs in the first time:

1. **Create a token (a string of unique characters) that is tied to the account.**
2. **Assign a cookie to the browser with the token attached.**

When the user goes to load a secure page, the app will check the token in the browser cookie and compare it to the one in its database. If they match, the user maintains access without having to re-enter their credentials.

Eventually, the app destroys the token on the server, causing the user's session to timeout. The advantage of this type of authentication is that it creates a streamlined user experience and saves time for the user. However, it also means that the device or browser the user is logged in on is vulnerable if it falls into the wrong hands.

06

Authentication Factors

An authentication factor is a category of credentials used to authenticate or verify a user's identity. Authentication factors can include passwords, security tokens (like keys or smart cards), and biometric verification such as fingerprint scans.

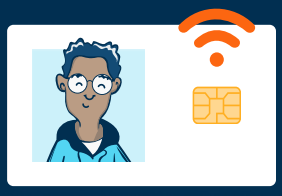
In the IT context, there are three types of telemetry:

SOMETHING YOU KNOW // aka knowledge factors

This is the most common authentication factor. It verifies identity by confirming users through confidential information they have, such as a login and password.

SOMETHING YOU ARE // aka inherence factors

An inherence factor verifies identity through inherent biometric characteristics of the user—like a fingerprint, voice, or iris pattern. The advantage of biometric authentication is that they're harder to lose or replicate. But they can be expensive and less accurate than traditional authentication factors.



SOMETHING YOU HAVE // aka possession factors

Users verify their identity with a unique object such as an access card or key fob. This authentication removes the risk of forgetting passwords; however, it means the user must have the object with them whenever they need to access a system, and they run the risk of losing it by accident or theft.

Are There More Authentication Factors?

Some point to measures like location (somewhere you are) and time (what time is it) as additional authentication factors. But, these are better categorized as security controls or supplemental authentication.

As the **National Institute of Standards and Technology** (NIST), a federal agency that publishes official cybersecurity guidelines explains:

"Other types of information, such as location data or device identity, may be used by a relying party (RP) or verifier to evaluate the risk in a claimed identity, but **they are not considered authentication factors**."

This is because you can't verify someone's identity based solely on where they are or when they are accessing a system. For example, two people can be in the same place, but they are clearly not the same person. Their location alone cannot be an identifying factor. Similarly, time alone cannot be used to identify someone.

But these can be applied as additional layers of secure access control to supplement the primary authentication factors. For instance, you can schedule access during set hours of the day or week. Users who try to access the system outside those time windows will be denied. Additionally, you can use location, such as a GPS location or an IP address, to help spot anomalous activities.

07

Types of Authentication

Single-Factor Authentication

Single-factor authentication (SFA) or one-factor authentication involves matching one credential to gain access to a system (i.e., a username and a password). Although this is the most common and well-known form of authentication, it is considered low-security and the Cybersecurity and Infrastructure Security Agency (CISA) recently added it to its list of **Bad Practices**.

The main weakness is that single-factor authentication provides just one barrier. Hackers only need to steal the credentials to gain access to the system. And practices such as password reuse, admin password sharing, and relying on default or otherwise weak passwords make it that much easier for hackers to guess or obtain them.

Two-Factor Authentication

Two-factor authentication (2FA) adds a second layer of protection to your access points. Instead of just one authentication factor, 2FA requires two factors of authentication out of the three categories:

1. **Something you know (i.e., username and password)**
2. **Something you have (e.g., a security token or smart card)**
3. **Something you are (e.g., TouchID or other biometric credentials)**

Keep in mind that although a username and password are two pieces of information, they are both knowledge factors, so they are considered one factor. In order to qualify as two-factor authentication, the other authentication method must come from one of the other two categories.

2FA is more secure because even if a user's password is stolen, the hacker will have to provide a second form of authentication to gain access—which is much less likely to happen.

Three-Factor Authentication

Three-factor authentication (3FA) requires identity-confirming credentials from three separate authentication factors (i.e., one from something you know, one from something you have, and one from something you are). Like 2FA, three-factor authentication is a more secure authentication process and adds a third layer of access protection to your accounts.

Multi-Factor Authentication

Multi-factor authentication (MFA) refers to any process that requires two or more factors of authentication. Two-factor and three-factor authentication are both considered multi-factor authentication.

Single Sign-On Authentication

Single sign-on (SSO) authentication allows users to log in and access multiple accounts and applications using just one set of credentials. We see this most commonly in practice with companies like Facebook or Google, which allow users to create and sign in to other applications using their Google or Facebook credentials. Basically, applications outsource the authentication process to a trusted third party (such as Google), which has already confirmed the user's identity.

SSO can improve security by simplifying username and password management for users, and it makes logging in faster and easier. It can also reduce help desk time focused on resetting forgotten passwords. Plus, administrators can still centrally control requirements like MFA and password complexity, and it can be easier to retire credentials after a user leaves the organization.

Biometrics

Biometric authentication relies on biometrics like fingerprints, retinal scans, and facial scans to confirm a user's identity. To do this, the system must first capture and store the biometric data. And then when the user goes to log in, they present their biometric credentials and the system compares them to the biometric data in their database. If they match, they're in.

One-Time Password

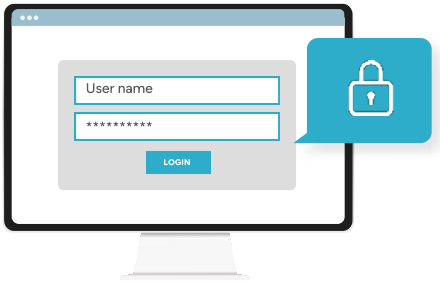
A one-time password (OTP) or one-time PIN (sometimes called a dynamic password) is an auto-generated password that is valid for one login session or transaction. OTP is often used for MFA. For instance, a user will start to log in with their username and password, which then triggers the application to send an OTP to their registered phone or email. The user can then input that code to complete the authentication and sign in to their account.

Passwordless Authentication

Passwordless authentication, as the name suggests, doesn't require a password or other knowledge-based authentication factor. Typically, the user will enter their ID and will then be prompted to authenticate through a registered device or token. Passwordless authentication is often used in conjunction with SSO and MFA to improve the user experience, reduce IT administration and complexity, and strengthen security.

Certificate-Based Authentication

Certificate-based authentication (CBA) uses a digital certificate to identify and authenticate a user, device, or machine. A digital certificate, also known as a public-key certificate, is an electronic document that stores the public key data, including information about the key, its owner, and the digital signature verifying the identity. CBA is often used as part of a two-factor or multi-factor authentication process.



AUTHENTICATION

08

Authentication vs. Authorization

So what's the difference between authentication and authorization?

Put simply, authentication is the process of verifying a user's identity, and authorization is the process of verifying what files, data, and applications that user is allowed to access. Once a user is authenticated, authorization grants them access to different levels of information and to perform specific functions based on pre-determined rules established for specific types of users.

AUTHORIZATION

For example, sales employees may have access to certain applications and databases that enable them to do their jobs and collaborate effectively. But they won't have access to the backend servers and software that IT uses to manage the company's information infrastructure. This security strategy is called least-privilege access (or formally, **principle of least privilege [POLP]**), and it ensures users are granted access only to the information and systems they need to do their jobs—nothing more, nothing less. This protects the organization's data by limiting the number of users who can access confidential information, reducing the surface area for threats.

Organizations can use authentication and authorization as part of a strategic framework for intelligently controlling access across their systems.

09

Emerging Authentication Trends

Authentication methods are continually evolving. As security threats become increasingly complex, we'll see more and more advanced authentication protocols to ensure secure access across industries. One of the biggest trends will be improving and expanding biometric authentication capabilities.

Statista reports that the global biometric system market is forecast to reach nearly $43 billion in 2022. And the market is expected to explode in the coming years, reaching a size of $83 billion by 2027.

Another key area of growth will be in adaptive authentication. This next generation of MFA relies on artificial intelligence and machine learning to identify additional user information such as location, time, and device to contextualize the login attempt and flag suspicious access behavior.

As security threats grow more complex, adaptive MFA measures will be essential for locking out bad actors.

10

Securing a Brighter Future

Strong authentication methods are critical to securing your organization and reducing risks that threaten your future viability. Yet, weak authentication remains a **common vulnerability** for information systems.

As the **CISA Capacity Enhancement Guide** illustrates: "An asset with the weakest method of authentication becomes a potential path to bypass stronger authentication for a system that it is connected to. A concrete and steel building with reinforced doors and sophisticated locks can still easily be entered by intruders if there are large, open windows."

11

Authentication at StrongDM

StrongDM's infrastructure access platform provides comprehensive access management solutions for your entire organization. Manage and audit access to your databases, servers, clusters, and web apps—all from one simple solution.

StrongDM secures access at every step from authentication to authorization, delivering full-stack observability so you know you're covered at every access point.

Protect your infrastructure, including all your sensitive data, with StrongDM.

Book a free no-BS demo today.

12

More Authentication Resources

- What is a Brute Force Attack? Types, Examples & Prevention
- 11 Authentication-Based Vulnerabilities You Need to Know
- How to Avert Authentication Bypass Vulnerabilities
- What is WebAuthn? Web Authentication Explained
- The Definitive Guide to FIDO2 Web Authentication
- Passwordless Authentication: Everything You Need to Know
- How to Set Up SSH Passwordless Login (Step-by-Step Tutorial)
- StrongDM Works with your Secrets Manager
- Kubernetes Role-Based Access Control (RBAC)
- SSH Key Management

StrongDM is a Dynamic Access Management platform that puts people first by giving technical staff a direct route to the critical infrastructure they need to be their most productive. End users enjoy fast, intuitive, and auditable access to the resources they need. Administrators gain precise controls, eliminating unauthorized and excessive access permissions. IT, Security, DevOps, and Compliance teams can easily answer who did what, where, and when with comprehensive audit logs. It seamlessly and securely integrates with every environment and protocol your team needs, with responsive 24/7 support.