CISCO DUO

5-Step Path to Passwordless

The Future of Authentication

5-Step Path to Passwordless

The Future of Authentication

Table of Contents

Foreword

It goes without saying in the IAM space that security exists on a spectrum. On one side is the utmost protection of secrets at all costs. On the other side is ultimate usability. How can we build something that leverages strong multi-factor authentication while remaining something customers of all skill levels are comfortable using? We continue to find success in investing in building a user-centric solution that handles best-in-class multi-factor security across a wide range of customer use cases.

Historically, many companies including Duo have focused on finding solutions to the question of, "how can we make password-based auth more secure?" Second-factor authentication methods like SMS one-time passcodes, time-based one-time passcodes, and Duo Push have incrementally improved our customers' security posture by adding a "something you have" factor to a password's "something you know." But despite our best efforts, some of these second-factor technologies retain a fundamental weakness: they can be vulnerable to phishing, just like the passwords they are intended to protect. This isn't just a problem for Duo, but for any company that has sensitive data that they want to control access to.

I don't think it's fully appreciated, then, that we are in an unprecedented time in multi-factor authentication. With the introduction and widespread adoption of passkeys, we can finally offer customers a way to protect access to sensitive systems that increases security and usability and eliminates password use. The pendulum head has impossibly widened to cover more of the spectrum than ever before in a way that is almost too difficult to believe.

As Duo continues to evolve its support for passkey-backed authentication, we have also increased the security of our beloved Duo Push to help keep customers secure across a wider range of use cases than with passkeys alone. Together, Passwordless offers customers a path to benefiting from all these recent innovations in a streamlined way that offers users security without them really having to think about it. Because at the end of the day, you and your users have more important things to spend your time on.

Matthew Miller

Duo Technical Lead & WebAuthn SME, FIDO Alliance Board Member for Cisco, W3C Web Authentication Working Group Editor

1.0 The Problem with Passwords

Passwords are plagued with problems. Combined with user friction and frustration, passwords alone are an increasingly insecure factor for identity verification.

Passwords are costly and burdensome to manage.

Passwords take up a lot of IT and help desk support time each year – so much so, that many large U.S.-based organizations have allocated over $1 million annually for password-related support costs, according to Forrester.

Expired or reused passwords can cost organizations of all sizes. With 10 billion passwords leaked and the uptick in password-spraying attacks, frequent password resets can be a time-consuming and expensive process. It also increases reliance on the individual user to choose strong and secure passwords that can't be easily "popped."

"Passwords remain a significant source of risk for organizations – even when incorporated with another method for MFA – and of friction, frustration and fatigue for users and administrators," notes the Gartner Group in their Market Guide for User Authentication

Passwords rely on user vigilance.

A survey of 2,000 end-users conducted by 1Password revealed that seven out of 10 respondents found having to remember or reset passwords a regular annoyance. This isn't a surprise – lockouts pause productivity and contribute to poor user login experiences.

In addition to password lockouts, the sheer number of cloud services and passwords that a user needs to log into to do their job has increased over the years. Now, the average enterprise uses over 1,000 different applications, while the average business user must juggle an average of 168 passwords. In the same survey by 1Password, nearly a third of respondents said they're open to using any new technology that makes life simpler.

Passwords are easily compromised.

Passwords don't last as long as they used to. Adversaries now have access to simple and effective password-related attack vectors. A few examples include credential stuffing (large-scale, automated login attempts using stolen credentials); phishing (an attempt to deceive users and illegally acquire sensitive information, like passwords); brute-force attacks (password guessing); and push-bombing attacks.

> **"Passwords have multiple weaknesses that attackers can exploit. Even the best password policy cannot mitigate spyware or phishing attacks."**
>
> – Gartner IAM Leaders' Guide to User Authentication

Passwords are inherently easy for adversaries to subvert. Due to password fatigue, users often choose weak passwords. They also often reuse or only slightly modify old passwords for different accounts. This often leads to disastrous consequences: Over the past 10 years, stolen credentials have appeared in almost one-third (31%) of breaches, according to the 2024 Verizon Data Breach Investigations Report.

Given this alarming (and evolving) trend, organizations are being forced to re-evaluate their security posture. While simple two-factor authentication (2FA) like SMS codes, physical tokens, or app-based push notifications was once enough of a safeguard against most attacks, that's no longer the case. MFA should now be considered the first line of defense and should offer both security for the organization and a frictionless login experience for the user.

This is where passwordless authentication comes in.

What is Passwordless Authentication?

Passwordless authentication establishes a strong assurance of a user's identity without relying on passwords, allowing users to authenticate using biometrics, security keys or a mobile device. Traditional MFA relies on something you have, like a mobile device, and something you know, like a password. Passwordless may seem like it counter-intuitively removes a knowledge factor (the account's password--something you know), but the password is replaced it with something you have (a possession factor, for example, a locked device with Touch ID) with something you are (an inherent factor, your biometric). This balances usability with stronger MFA authentication. Passwordless gives users a frictionless login experience, while reducing administrative burden and overall security risks for the enterprise.

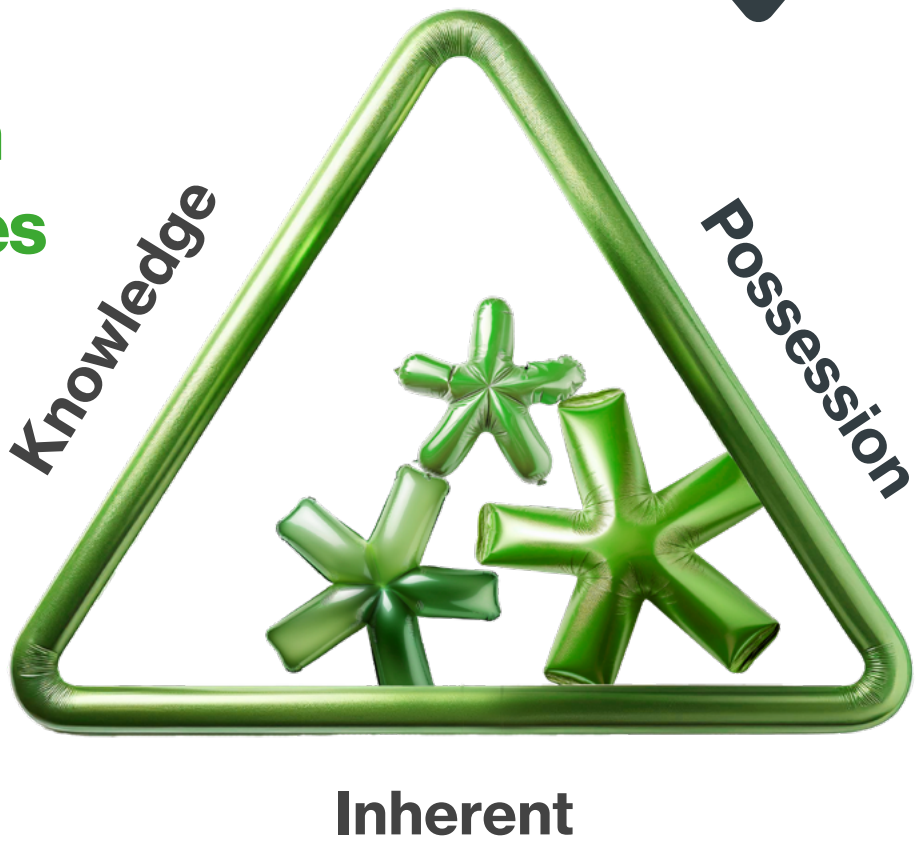
Business Benefits of Passwordless

Passwordless authentication provides a single, strong assurance of users' identities to achieve user trust. As a result, enterprises can realize the following benefits:

- Better User Experience: By eliminating reliance on passwords, users benefit from a reduction in login fatigue and frustration, as well as an increase in user productivity.
- Reduced IT Time and Costs: Similarly, administrators and enterprises can benefit from reduced burden due to password-related help desk tickets and password resets.
- Stronger Security Posture: Eliminating system reliance on passwords can result in the elimination of related threats and vulnerabilities, including phishing, stolen or weak passwords, password reuse, brute-force attacks, etc.

3 Authentication Factor Categories

MFA checks for at least two of the 3 authentication categories, colloquially: "something you know," "something you have," and "something you are."



2.0 The 5-Step Path to Passwordless

The Challenge:

Adopting a New Technology

Today, many authentication solutions only solve for one use case or enable a password-lite experience for users through single sign-on (SSO), changing the order of factors and session management. However, these piecemeal approaches can leave security gaps while not fully solving the weakness of passwords. For example, will the passwordless solution cover every authentication flow, and even if it does, will it assess the posture of devices accessing without a password?

Modern enterprises cannot cover all of their access use cases today with a single passwordless solution.

There are additional business challenges to consider:

Complex and Hybrid IT Environments

Finding a solution that supports both legacy and cloud applications and provides a consistent, simplified user experience is a challenge. Cloud federation provides passwordless only for cloud applications – users can log in and verify their identity using biometrics or a security key. But in reality, modern enterprises need to protect access to a hybrid mix of both cloud and on-premises applications.

Administrative and Management Costs

Supporting passwordless technology may involve cost-prohibitive security hardware and device management. The cost of security keys and biometric-based authentication can be a barrier to entry to supporting different types of users across an enterprise.

Compliance Regulations

Many companies or supply chain partner companies that need to meet compliance standards for data regulation have tied their policies to passwords, making it difficult to shift to stronger authentication methods. Cyber insurance providers and federal standards like NIST 800-63 outline more guidelines for passwords, MFA, and phishing-resistant authentication methods, with more recent guidance on dropping password end and complexity requirements.

An industry-wide shift

Problem Statement

Passwordless point solutions today do not solve every common use case across modern enterprises, causing critical gaps in access security.

Passwordless Challenge

Establish a basis for user identity trust that doesn't rely on passwords – no matter where the user goes or what they attempt to access.

Passwordless can't be achieved by one solution alone. It requires a compatible IT and application ecosystem that puts security at the forefront. Platforms like Windows Hello, Touch ID, Face ID and fingerprint APIs must work in tandem with hardware-based biometric authenticators, supporting open standards like WebAuthn, SAML, and CTAP. Providers must upgrade to set the technical groundwork for seamless, secure passwordless experiences.

The Solution:

5-Step Path to Passwordless

We recommend taking a phased approach to providing secure access for the workforce, with each step taking you closer to a fully passwordless future:

1. Identify passwordless use cases and enable strong authentication.

The first step is identifying and selecting specific enterprise use cases and evaluating the “starting point” for modernizing infrastructure in support of stronger authentication. Rank the use cases by user experience, IT time and costs, and security and compliance risks. Group the use cases by applicable passwordless solutions, so as not to end up with a series of point solutions. Create implementation plans for areas that have the biggest impact with the shortest time to value.

Reduce your reliance on passwords as the only form of user authentication and plan additional factors to later provide primary authentication. Protect cloud and on-premises applications with strong MFA. This enables you to lower the risk of credential theft by requiring a second method of identity verification that cannot be easily stolen remotely by an attacker.

2. Streamline and consolidate authentication workflows.

Rationalize authentication for a set of use cases as part of the implementation plan. For cloud apps, reduce reliance on passwords by using SSO for SAML-based applications. For on-premises services, integrate the workflows using access proxies and authentication proxies.

With MFA in place and a consolidated login experience, you can change password policies that require stringent and complex password characters, as well as policies around password reset frequency. You can also minimize the number of times users need to authenticate (or perform MFA) by implementing solutions where a single strong authentication persists across different applications and the users are prompted only when there is a change in context or risk. This lowers the user frustration related to password security and reduces your reliance on password complexity as your primary authentication.

3. Increase trust in authentication.

Increase Trust with Adaptive Policies and Device Trust

An often-raised concern about passwordless is the potential for increasing security risk when reducing the steps people take to authenticate. Address that head-on by increasing control based on the context of the user's authentication.

Is the authentication coming from a trusted device? Does the access device's security posture meet the organization's security hygiene standards? Finally, check for suspicious behavior like unusual authentication factors, unusual locations, strange times of day, or access attempts by high-risk users or against high-risk applications. Apply adaptive access policies based on the context of the user, device, location, behavior, and more, to ensure the authentication is trusted.

4. Provide a passwordless experience.

If MFA is a password with one or more authentication factors, passwordless is best described as two or more authentication factors without passwords. People can log in using a biometric authenticator and the possession of a trusted device to access applications. **This would be something they have and something they are, instead of relying on something they know (a password).**

In this step of the journey, implement standard technology to remove passwords as the primary authentication factor for the use cases and areas with the biggest impact on user experience, cost, and security.

For example, consider using passwordless authentication to securely log on to your SSO solution. In this way, all of the applications federated behind the solution receive the benefit of passwordless. Choosing the right passwordless authenticator will depend on your environment – leveraging hardware with built-in biometrics is one option and investing in security keys that support FIDO2 is another. There are also phone-as-a-token providers that can enable passwordless via a mobile application. Many of these methods will leverage WebAuthn in the background. WebAuthn is an open standard that enables strong public key cryptography to ensure user presence at the point of authentication. It requires a supported web browser, operating system, and built-in authenticator such as Touch ID, or USB-based security keys.

5. Optimize the passwordless toolset.

Achieve passwordless authentication for all use cases, including passwordless for legacy tools using older protocols along with cloud-based applications. The path to passwordless is an iterative approach to selecting, streamlining, and securing authentication. The final step in the journey is integrating the technology and moving towards continuous improvement. Passwordless will eventually end your need to rely on passwords for any login workflow, either behind the scenes or throughout your users' experiences.

This is the challenge in the market today that passwordless-pioneering technology platform providers need to solve. Duo is working on support for a comprehensive ecosystem that enables passwordless across every enterprise use case.

3.0 Cisco's 130,000-user Passwordless Deployment

Cisco fully rolled out Duo Passwordless across over 130,000 users in August 2023, but planning and small pilot groups began two years prior. As a modern enterprise, the Cisco IT security team faces a complex and hybrid IT environment, regulation and compliance requirements, and a general need to keep administrative and management costs to a minimum.

Password resets and account lockouts result in lost time and resources, and standard form-based login with MFA increases security but at the expense of repeated user friction. Streamlining and consolidating authentication workflows became a priority for the Cisco IT team. With Duo Passwordless, Cisco was able to implement a FIDO2-based login flow that utilized Duo SSO and built-in hardware biometric platforms like Touch ID and Windows Hello to improve the overall login experience without compromising security.

Cisco's Zero Trust Security

Responsive and adaptive access policies also contribute to a smoother end-user login experience and stronger zero trust security practices. Cisco deployed Risk-Based Authentication (RBA) alongside passwordless. RBA steps up authentication to a more secure method when risk factors or novel attack patterns are detected such as impossible travel, push harassment, and push spray. Risk is assessed at each authentication request, even if the end user doesn't interact with Duo directly.

Another component of Cisco's Zero Trust strategy is to define device trust standards, especially with a hybrid BYOD-accessing workforce. Duo enabled Cisco to limit sensitive application access to only trusted endpoints like corporate-managed devices. This added another layer of defense if credentials are compromised.

With thorough planning, alignment with leadership, and active communication and feedback practices, Cisco's rollouts saw high levels of adoption with minimal related helpdesk tickets — a resounding success in enterprise security.

"We rolled out Duo Passwordless globally to 130,000+ users. It almost was a non-event at some point. We have just a few open cases and maybe 90 after 3 weeks, which is nothing. Adoption level shave been fantastic. A global rollout, with no problems whatsoever. That's phenomenal. That never happens when we roll things out at this scale."

– Sarabjeet Rana,
Principal Architect, *Cisco IT Security Team*

Rolling out stronger security

Passwordless journey at Cisco.

October 2021

Pilot starts within Enterprise Security
(160 users)

August 2022

Pilot expands to Infra and Infosec teams
(3,000 users)

November 2022

Duo Passwordless is Generally Available

December 2022

Pilot expands to Security Business and Sales, and Cisco ONEx
(30,000 users)

February 2023

Duo provides capability for mobile users to access zero trust-enabled apps.
Pilot expands to Supply Chain and CX
(60,000 users)

July 2023

Optimization of SSO, Form Auth, and Passwordless algorithms

August 2023

Duo Passwordless is rolled out to all of Cisco
(130,000 users)

KPIs:

- Passwordless adoption end-user sentiment
- # of device biometric enrollments
- % of passwordless authentications
- # of step-down and step-up authentications
- # of apps protected by Duo
- # of authentication-related help desk tickets

Best Practices:

- **Take time to identify your organization's application landscape.** What percentage of applications are WebAuthn and CTAP-compatible today? What are key applications that need to be protected?
- **Define pre-requisites and establish your definition of "done."** Passwordless is just one component of a zero trust strategy. What are specific metrics your organization or leadership focus on?
- **Start small to go faster at scale.** Pilot programs with limited users can result in valuable feedback and important monitoring.
- **Get executive buy-in/sponsorship.** Sharing benefits with leadership and employees can help win "air cover" to make decisions and move quickly. Weekly newsletters and fireside chats to stakeholders can create momentum and a sense of urgency.

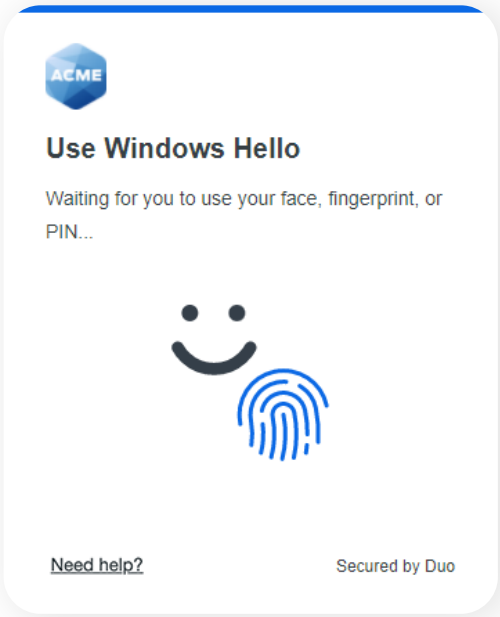
[Read the full Cisco & Duo case study]

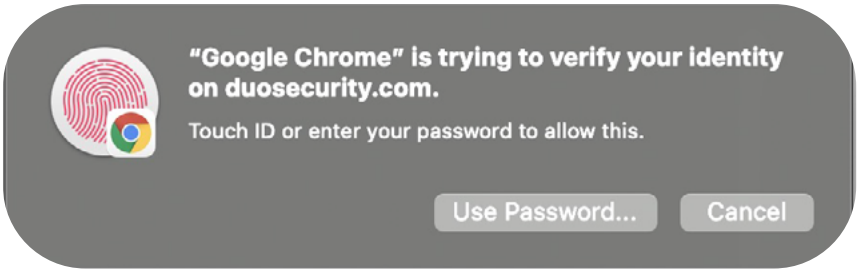
4.0 Building Your Organization Towards a Passwordless Future

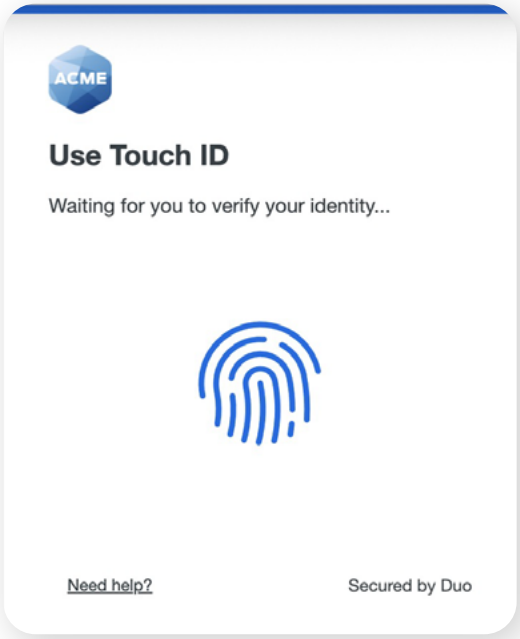
Passwordless is a building block for organizations working towards a zero trust security strategy, from small businesses to major enterprises like Cisco. It provides a key aspect of establishing a single, strong user identity and trust, and enables the shift to a mobile and cloud-first enterprise — allowing users to work remotely, increasing productivity and driving business agility.

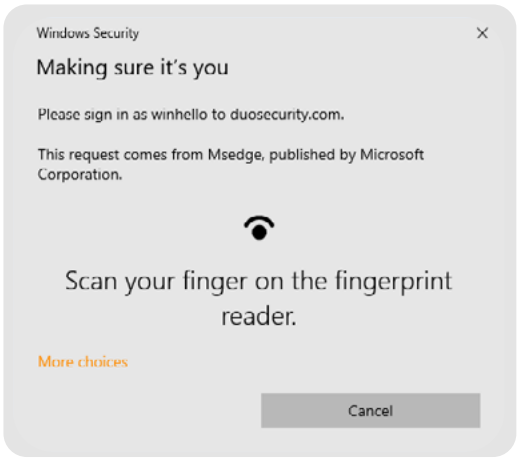
Duo offers a flexible implementation of passwordless authentication to meet the needs of businesses and their use cases. This includes:

- Wide support for phishing-resistant roaming and platform authenticators: WebAuthn FIDO2 passkeys and security keys with biometric or PIN verification, and authenticators or biometric sensors built into the device like Touch ID, Android Biometrics, or Windows Hello
- OS-level passwordless authentication for Windows Logon, compatible with Duo Passport to deliver a true and secure single sign-on experience across protected platforms and applications
- Strong authentication using passwordless with Duo Mobile application
- Full compatibility with Microsoft Entra ID MFA requirements through external authentication methods integration (replacing Custom Controls)
- Risk-based authentication with Duo Passwordless for automatic authentication step-ups, and native integration of passwordless with Trusted Endpoints to define access for managed and unmanaged devices
- Out-of-box analytics and detailed logging to track and report on passwordless adoption









[WebAuthn and Agnostic Integrations] **are available in all Duo editions.**

"It was exactly what I was looking for, which was a simple and elegant way to use YubiKeys or Windows Hello or Touch ID to replace the password. It simultaneously simplifies a user's life and takes the risky password off the table."

– **Jason Watts**
CISO [Inductive Automation]

Passwordless Enables Zero Trust.

A combination of user and device trust, driven by adaptive policies ensures access to applications and data is secured. Duo's Passwordless authentication improves the working experience while strengthening our trust in authentication for all Duo customers. Establish a passwordless login workflow for cloud apps without ripping and replacing existing infrastructures.

Additional Resources

Don't let passwords burst your balloon. Learn more about what Duo is doing to enable the passwordless future by working to make passwordless technology and standards open, accessible and easy for the broader community:

- What is WebAuthn?
- WebAuthn.io
- Web Authentication: What It Is and What It Means for Passwords

Blog:
What are passkeys?

Webinar:
The State of Passkeys

Mini-Docu Series:
The Life and Death of Passwords

Duo Passwordless Documentation:
https://duo.com/docs/passwordless

Cisco Duo protects against breaches with a leading access management suite that provides strong multi-layered defenses and innovative capabilities that allow legitimate users in and keep bad actors out. As a trusted partner, Duo quickly enables strong security while also improving user productivity.

Try it for free at duo.com.