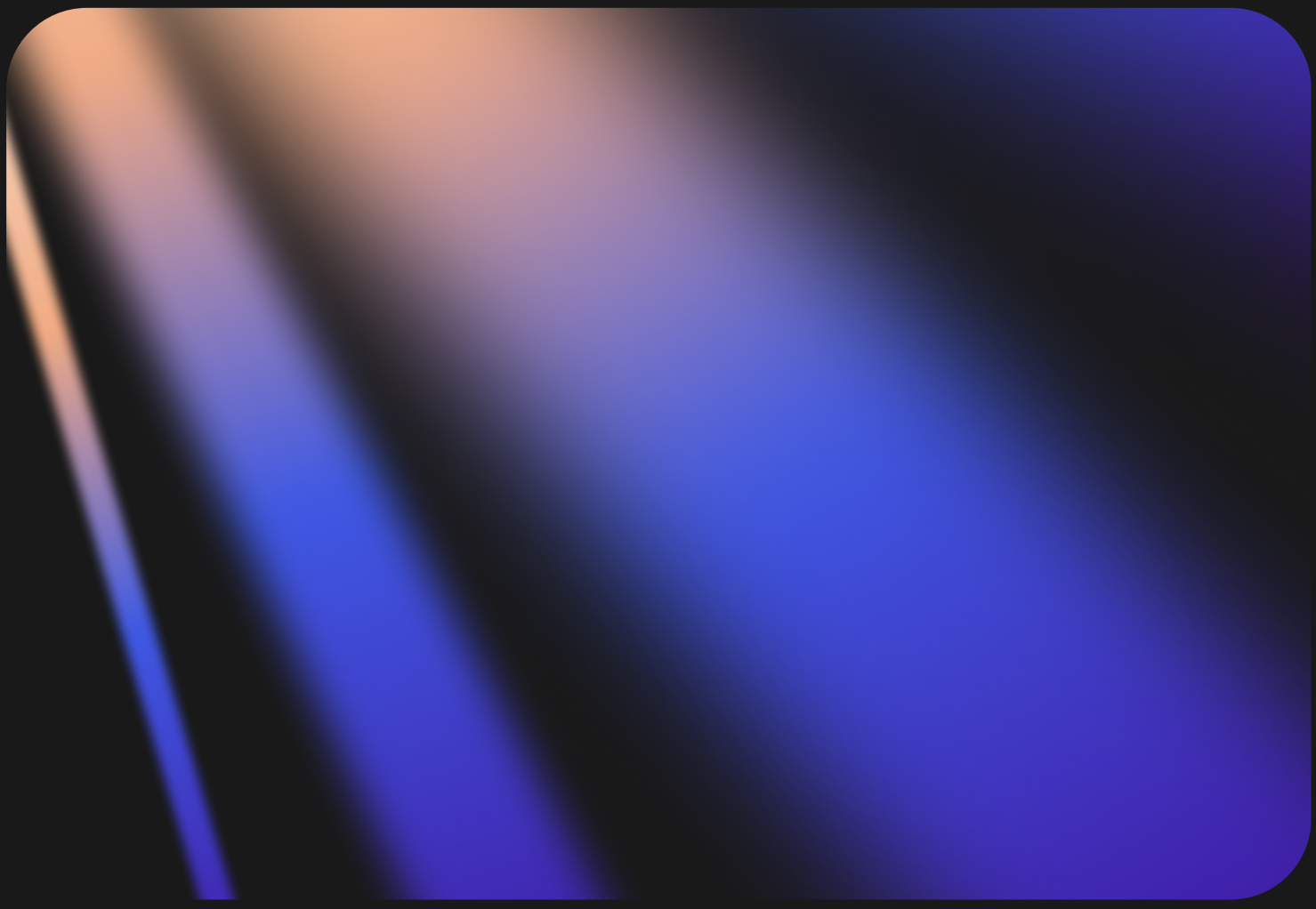
auth0

Whitepaper

Customer Identity Buyer's Guide

Essential features and capabilities for delivering convenient and secure customer experiences



okta

The World's Identity Company™

Contents

2 Introduction: The Customer Identity maturation journey

5 **Stage 1 |** Fundamental: Meet immediate needs while creating a strong foundation for the future

11 **Stage 2 |** Scaling: Introduce automation while further streamlining and securing authentication

22 **Stage 3 |** Advanced: Extend automation and integration, and refine the authentication experience

30 **Stage 4 |** Strategic: Optimize and extend Identity

35 Summary

Introduction: The Customer Identity maturation journey

Today's organizations require a holistic approach to Customer Identity and Access Management (CIAM), but the journey from satisfying basic needs to mature Identity infrastructure that not only meets customer expectations — but also enables organizational efficiency and growth is a significant undertaking.

To help organizations consciously plan and progress along an Identity roadmap, Auth0 distilled the most successful practices from thousands of our customers into the Customer Identity Maturity Model.

Explained in detail in the whitepaper A Comprehensive Guide for Your Customer Identity Maturity Journey, the model empowers organizations to:

- Assess the relative state of their Customer Identity posture
- Identify and implement new capabilities that will aid in the organization's maturation
- Measure the impact and outcomes of Identity initiatives as the organization progresses along the maturation journey

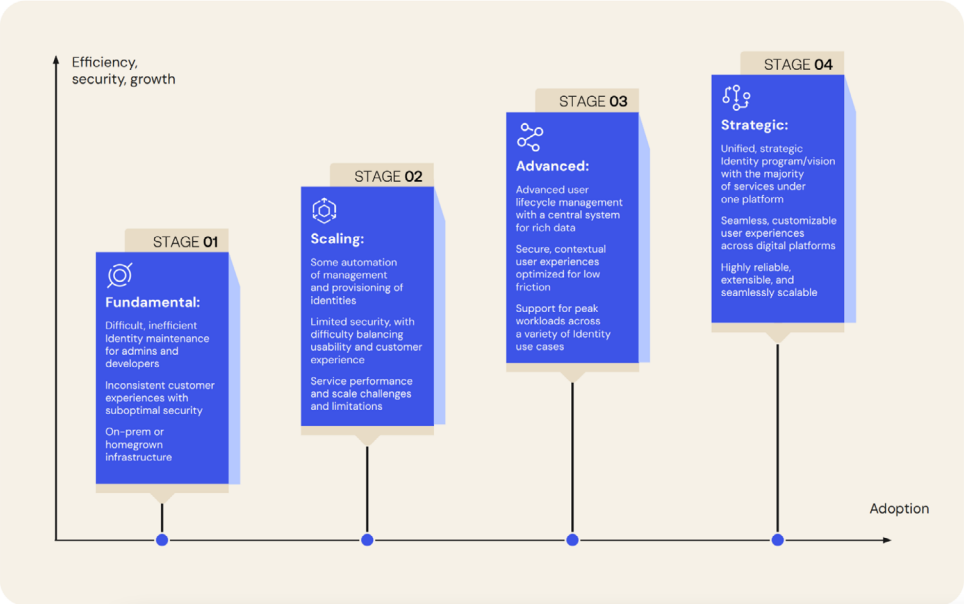
Auth0's Customer Identity Maturity Model is a comprehensive framework for assessing the current state of your Identity capabilities and effectiveness, creating a plan to improve them, and measuring ongoing success and value.

By understanding where you are today and where you could be in the future, you'll position your business to more accommodate new Identity and security requirements, and to meet ever-growing end-user demands.

This document is a companion piece to the whitepaper, and complements that extensive high-level roadmap by examining the many different elements that contribute to Customer Identity maturation.

For each stage — Fundamental, Scaling, Advanced, and Strategic — we review the main goals and outcomes of that part of the journey, before diving more deeply into the actual solutions that need to be introduced and implemented. For each component, we:

- Provide wider context that explains its importance
- Examine considerations that will help buyers to navigate a crowded market
- Suggest, where applicable, a "rollout roadmap" to provide additional context about incremental feature introduction and related capabilitie



Beyond the basics: the importance of extensibility

A modern CIAM solution can tackle the Identity basics (e.g., signups, logins, account updates, password resets, etc.), but satisfying advanced use cases often requires transacting with other business systems and third parties to execute complex conditional flows.

Building such advanced logic from scratch is a major undertaking requiring specific skill sets, tools, and knowledge; worse still, it's inefficient because each use case is a custom coding exercise with little that can be reused.

Alternatively, having a simple but effective (read: powerful, flexible, efficient, etc.) way to make Identity work with your other business systems allows developers to quickly implement customized Identity solutions without the time, expense, and headaches associated with custom coding projects.

In a computing context, "extensible" means "designed to allow the addition of new capabilities and functionality." An extensible CIAM solution increases your adaptability, allowing you to implement specialized and even unforeseen use cases — ideally with a range of implementation approaches (e.g., pro code, no/low-code, plug-and-play) to suit your needs and resourcing.

For example, an online retailer could integrate their CIAM solution with a Customer Data Platform (CDP), Identity-proofing utility, consent management solution, and fraud detection platform to:

- Gather zero- and first-party customer data in a compliant manner
- Prevent fraudulent registrations
- Protect and enrich existing user accounts
- Stop fraudulent checkouts
- Reward loyal customers

Learn how Auth0 empowers you to customize Identity



Stage 1

Fundamental: Meet immediate needs while creating a strong foundation for the future

This is the starting point, where an organization is typically just beginning the process of extending digital services, online portals, or software to its customers.

At this stage, most companies are primarily concerned with onboarding customers to the system and digitally managing their identities.

The bare essential capabilities and architecture for authentication (user sign-in), authorization (access rules, policies), and user management (user sign-up) may be in place, but building and maintaining these capabilities consumes limited resources, and a lack of experience around the larger role of Identity can lead to costly missteps.

Major benefits:

- Increased conversions due to lower-friction signups
- Consolidated user stores simplify administration and lay a foundation for future scale
- Stronger password hygiene limits appeal to attackers and can reduce impact of data breaches

In practice, this basic Identity stack is good enough … until it suddenly isn't — which is why the Fundamental stage focuses on meeting immediate needs while establishing a strong foundation for maturation.

Category	Feature / Element / Capability	B2C	B2B
Authentication	Social logins	✓	✓
	Consent management	✓	✓
Authorization	Consolidate and connect to existing user stores	✓	✓
Security	Password hashing	✓	✓



Authentication

Authentication is intended to establish that the customers signing up for accounts, and subsequently logging into them, are who they say they are. However, the effort required for customers to authenticate shouldn't be so burdensome that it has an unacceptably negative impact on the user experience (UX) — especially in B2C contexts.

Consequently, organizations should aim to simultaneously achieve — or, in the worst case, to balance — security (i.e., strength of authentication) and UX.

Note that some organizations may need to introduce stronger authentication security (e.g., using MFA) at the Fundamental stage. For example, under the EU's Revised Directive on Payment Services (PSD2), payment service providers are required to implement strong customer authentication (SCA).

Social login

Social login is a form of single sign-on (SSO) for your customers, as it allows them to log in to a single service and access a multitude of accounts. Importantly, social login simplifies the registration process, reducing friction by providing one-click sign up and allowing your customers to use their preferred/trusted Identity provider (e.g., "Sign in with Google") or one appropriate to the activity (e.g., "Sign in with GitHub").

Plus, many Identity providers — like Facebook or Google — permit websites and services to automatically obtain valuable biographical details users have consented to share, like their name, email address, location, interests, birthday, and more. Data obtained in this way is more likely to be accurate, and — better still — doesn't require the user to type it out, saving them effort and further reducing friction.

However, note that the security protecting accounts will vary from provider to provider. While Facebook, Google, and other large organizations have the resources and incentives to protect accounts, the same cannot be said for all social Identity providers — so organizations should carefully consider which Identity providers they want to offer to users as social login options.

Likewise, while social login is a compelling option for many organizations, it is unsuitable for those operating in highly regulated industries (e.g., finance, healthcare, etc.).

Considerations: When exploring third-party social login capabilities, pay particular attention to:

- ☐ Number and breadth of social Identity providers supported
- ☐ Ability to consolidate/link duplicate accounts across various providers

Rollout roadmap: Many organizations choose to introduce social login by supporting a small number of the most globally popular services, such as Google, Facebook, and Apple. Later, they subsequently roll out integrations with regional, and industry, or demographic-specific Identity providers (e.g., Weibo, LinkedIn, GitHub, etc.).

Making social login simple

Delivering a best-in-class authentication experience is crucial to standing out in never-ending competition for consumers.

Learn how Auth0 makes social login simple

Consent management

Through a combination of out-of-the-box functionality and the ability to integrate with third-party consent management platforms, a modern CIAM platform enables organizations to log and track consent from customers to collect and use their data.

Consent management is essential for complying with privacy regulations like the GDPR and CCPA and, as third-party cookies disappear, is an increasingly important foundation of customer insights and personalization.

Authorization

Effective authorization helps application providers to empower each user with the appropriate level of access to resources and capabilities. In this earliest stage of Customer Identity maturity, the emphasis should be on simplifying and centralizing user stores, creating a strong foundation for robust, efficient, and effective authorization.

Consolidate and connect to existing user stores

In the Fundamental stage, organizations often grapple with:

- Multiple user stores, including external Identity providers (e.g., via social login), databases, or passwordless authentication methods (typically later in the maturation journey)
- Migrations from one user store to another

By consolidating users stores and connecting to existing user stores, organizations can reduce the complexities of user management and can benefit from the efficiency gains associated with a centralized source of truth.

Considerations: When searching for an Identity solution, look for one that:

- ☐ Includes its own Identity provider service, to help you migrate away from legacy databases or to enable you to get up and running quickly if you're starting from scratch
- ☐ Can automatically sync user profile data with each user login, ensuring that changes made in the connection source are automatically captured
- ☐ Allows you to use an existing user store, or to store user credentials on your own server
- ☐ Supports trickle/lazy migration, rather than requiring all users to migrate at once

Enabling a "one identity" strategy

It's common for a single customer to have multiple identities on multiple platforms and brands all owned by one organization. For example, they may have a separate account for the website and another for the loyalty program or completely different accounts across multiple brands that combined via mergers and acquisitions.

Intelligent customer engagement requires a consolidated omnichannel view of customer Identity, preferences, and history across all interactions and transactions. However, data has historically been collected across siloed customer facing channels, and activated across siloed business systems — resulting in manual, error prone processes and data quality issues.

By helping to turn anonymous users into known customers, and by enabling business systems — including Customer Data Platforms (CDPs) — to consolidate data silos based upon customer Identity, CIAM enables the "one identity" strategy so critical for effective customer engagement and marketing initiatives.

Security

Legitimate customers aren't the only ones interested in what's behind the login gateway, and an entire ecosystem of technologies, services, and other resources exists to enable malicious actors to attack Identity systems.

As cybercriminals direct more effort and expertise into getting past the login box protecting it requires ever-more layers of ever-more sophisticated defenses. In the Fundamental stage, every organization should ensure basic password hygiene is in place to limit appeal to attackers and to reduce the impact of data breaches.

- Password hashing
- The portability of passwords and their continued use as knowledge factors for authentication make them prime targets for threat actors. For example, Verizon's Data Breach Investigation Report (DBIR) 2023 revealed that:
- The vast majority (86%) of web application breaches involve the use of stolen credentials
- Credentials are among the most common data exfiltrated during breaches
- To help preserve user privacy and to mitigate the risks associated with password theft, organizations should make sure never to store or log passwords in plain text — if your password database is truly illegible, then it has no value to hackers.

Considerations: Whether you choose a third-party CIAM solution or elect to built one in house:

- ☐ Make sure passwords are hashed with a modern password-hashing function

Secure password hygiene

The database hosted within the Customer Identity Cloud never stores or logs passwords in plain text; instead, all passwords are hashed with the bcrypt password-hashing function.

Learn more in Hashing in Action: Understanding bcrypt



Stage 2

Scaling: Introduce automation while further streamlining and securing authentication

Once companies gain experience launching more than one application or portal, they begin to appreciate the importance of being able to build and deliver great digital products and services repeatedly, at scale.

Doing so requires a focus on internal operational efficiencies to support business growth. For example, an organization might be looking to increase automation as a means of boosting productivity for admins and developers alike — and such efforts can stand to benefit from Identity features such as intuitive admin portals and centralized, low-touch user lifecycle management (LCM).

Major benefits:

- Increased appeal to business customers
- Reduced registration and login friction due to passwordless flows
- Reduced costs and freed-up resources from more efficient administration
- Dramatically stronger security posture reduces risk of fraudulent registrations and account takeovers

At the same time, security becomes a higher priority both as a means to reduce costs and to increase the application's appeal to potential customers.

Category	Feature / Element / Capability	B2C	B2B
Authentication	Enterprise federation	✗	✓
	Consistent login experiences	✓	✓
Authorization	Organization-based management & administration	✗	✓

Category	Feature / Element / Capability	B2C	B2B
Security	Multi-factor authentication	✓	✓
	Brute force attack detection for individual accounts	✓	✓
	Suspicious IP rate-limiting	✓	✓
	Breached password detection	✓	✓



Authentication

The Scaling stage is where B2B organizations tend to introduce the ability to work with a business customer's existing Identity systems.

Delivering consistent and convenient experiences — for business customers and for consumers — also becomes more important as an organization matures.

(B2B) Enterprise federation

With federation, your product outsources authentication to each business customer's owned-and-operated Identity provider, which is responsible for authenticating the user, applying access policies and, upon successful authentication, sending the user into your product.

Leveraging federation to enable single sign-on allows multiple applications to use the same authentication session, thereby avoiding repetitive credential entry and the fatigue that it causes. This is particularly important to enterprises because they typically will have many different services and a large number of end users. Additionally, SSO is usually a component of an enterprise's security strategy — with fewer credentials to remember, fewer credentials can be forgotten or stolen by enterprise users.

But the benefits go beyond security: SSO also improves the experience for the enterprise's users and can help to reduce IT administration and support costs. Administrators can easily manage user provisioning and deprovisioning via their own Identity provider, and users are less likely to need to contact support because of forgotten credentials.

Considerations: Look for an enterprise federation solution that:

- ☐ Supports configuration of any enterprise connection — including Active Directory, Lightweight Directory Access Protocol (LDAP), Security Assertion Markup Language (SAML), and more — with just a few lines of code
- ☐ Includes self-service configuration capabilities, which will empower your customers while also reducing the time and effort your own organization needs to apply to customer-facing operations, sales, and support teams
- ☐ Provides detailed logs, to simplify auditing and debugging

Rollout roadmap: For one reason or another, some organizations intend to hold off on introducing support for enterprise federation until forced to do so to win a large client. However, this approach overlooks the benefits outlined above, and also presumes that sourcing (or building) and introducing such functionality can be done quickly. The reality is that federation is just one of a long list of enterprise requirements, and the organization will be in a much stronger position to accommodate those requirements if federation is already checked off.

Consistent login experiences

Familiarity reduces friction and makes it easier for customers to do what they want to do within your application, making consistency an important part of the user experience for business customers and consumers.

An important contributor to consistency is branding. It can be quite jarring — and even confusing or alarming — for customers to bounce between brands (e.g., your brand and your login provider's brand) or to see different versions of your brand at different times.

To deliver consistent and correctly branded customer experiences, organizations need to move away from treating different login channels as separate entities, and instead manage them — from the login flows themselves to the branding — holistically.

Considerations: To enable consistent and positive user experiences, your Customer Identity solution should offer:

- ☐ Rich branding options (e.g., color palettes, fonts, logos, etc.), to create consistent user experiences across all login flows and authentication channels
- ☐ No-code and low-code customization options that allow you to deliver great experiences without drawing heavily upon developer resources
- ☐ Centralized configuration, so you can implement your login page just once for all your apps
- ☐ Accessible experiences (i.e., to WCAG AA standards), guaranteeing your organization's compliance requirements

Rollout roadmap: There are many reasons for a user to be a member of multiple organizations. Home realm discovery (HRD) — the process of identifying to which Identity provider the user belongs before authenticating them — can be a natural follow on to elevate the functionality of a universal login experience.

Flexible, frictionless authentication for every step of the way

With or without code, you can secure a seamless journey of digital access for customers.

Learn how Universal Login helps you efficiently deliver consistent — and great — user experiences



Authorization

As organizations attract more customers, a lack of efficiency can become a significant bottleneck to continued scale. As part of the maturity process, specific issues should be systematically addressed.

(B2B) Organization-based authorization management and administration

It's common for B2B organizations to expend considerable time and effort performing very granular Identity management and administration activities on behalf of their customers.

To lessen the pressure on internal resources, it's important to be able to manage each business customer at an organization level.

Considerations: Any potential CIAM platform should allow you to:

- ☐ Manage the login experience, connection model, and user roles (see this resource page for more details)
- ☐ Simplify onboarding of business customers
- ☐ Customize authorization workflows for your customers, at scale
- ☐ Build administrative capabilities into your products to allow your business customers to manage their own authorization at the organization level

Rollout roadmap: Most application providers focus on organization-based authorization in the Scaling stage, and address more granular controls and organization-based authentication in the Advanced stage.

Security

A strong security posture is a necessary condition for achieving scale — otherwise, enormous time and resources will be expended addressing symptoms and responding to attacks. The Scaling stage is typically when organizations move beyond the basics of password hygiene and shift attention to building layered defenses against today's Identity threats.

Multi-factor Authentication (MFA)

Multi-factor authentication (MFA) is a user verification method that requires more than one type of user validation (e.g., biometric, one-time passcode, or authenticator application).

Protecting accounts through the use of MFA drastically increases the time, effort, and — ultimately — cost of pursuing account takeovers (in which a threat actor gains access to and control over an existing account belonging to a legitimate user).

In a B2C context, attackers may gain access to resources (e.g., loyalty points), privileges (e.g., ability to make purchases, especially of products in limited supply), and valuable demographic and personally identifiable information (PII).

In a B2B context, an attacker who successfully compromises a user account may use it to access highly sensitive data, resulting in a breach with severe regulatory and contractual penalties for the targeted organization.

In practice, MFA's effectiveness as a countermeasure to ATOs is dependent upon the use of strong secondary factors that cannot be easily bypassed by threat actors (e.g., by guessing or researching knowledge-based factors, by brute-forcing OTPs, etc.).

Additionally, organizations implementing MFA need to be mindful that threat actors have begun to abuse SMS and call-based validation methods via SMS pumping and toll fraud, and that SIM swapping is becoming a go-to technique for bypassing SMS-based MFA.

Considerations: When evaluating potential MFA solutions, make sure you understand the costs associated with SMS or email-based MFA; additionally, look for solutions that:

- ☐ Support strong, modern secondary factors based on possession or biometric factors

- ☐ Allow you to white-label a device push into your own brand's app
- ☐ (B2B) Provide a set of configurable MFA policies to meet unique business needs
- ☐ Offer self-service configuration and reset capabilities
- ☐ Include measures to prevent and minimize SMS pumping and toll fraud

Rollout roadmap: To maximize convenience for their customers, organizations often roll out a handful of secondary factors, before consolidating over time on the most secure ones. Moreover, both B2B and B2C organizations have an evolutionary path for MFA — and for passwordless authentication.

Initially, organizations may introduce MFA security that requires third-party authenticator apps like (e.g., Google Authenticator), but as organizations mature, they integrate these MFA prompts into their own mobile applications to create a consistent and seamless user experience — one in which the user does not have to navigate to a third-party app.

In stage three, both B2C and B2B organizations may introduce Adaptive MFA, so that MFA challenges are only issued when a risk score threshold has been met.

Consider passwordless authentication to improve UX and security

Passwordless authentication (often just shortened to "passwordless") refers to any mechanism that authenticates a user without requiring them to enter their password. As it happens, such authentication is already common at the device level: think Apple Touch ID and Face ID, and Windows Hello, all of which allow users to access their devices in a passwordless manner.

Passwordless login flows for apps and web services improve the user experience by reducing friction while providing stronger authentication than passwords — but for many organizations the subject is novel and potentially confusing.

Learn more about passwordless, including different passwordless options and many common misconceptions, in Authentication After Passwords

Brute force attack detection for individual accounts

Threat actors may try to discover or validate credentials, and/or compromise an account by engaging in brute-force tactics — essentially, trying a large volume of passwords against a single username (or other identifier).

Detecting such attacks is an important element of a layered approach to securing customer Identity, as failing to detect and block such attempts:

- Can result in account takeovers
- May impair application performance — particularly if a threat actor is attacking multiple accounts — by slowing authentication for legitimate users or even rendering the authentication service completely unavailable

Considerations: To ensure appropriate levels of defense and flexibility, look for a solution that:

- ☐ Allows administrators to configure the threshold above which activity is considered to be an attack
- ☐ Automatically block offenders (typically on an IP-address level)
- ☐ Includes a rolling window (e.g., 30 days) to enable automatic removal of blocks (i.e., 30 days after the last observed abuse)
- ☐ Allows administrators to manually remove a block
- ☐ Automatically notifies each targeted user and allows them to unblock (i.e., in the case of the threshold being triggered by a user's own failed login attempts)

Rollout roadmap: At this stage in the maturation journey, brute force protection is typically focused on stopping targeted attacks against individual users/accounts. Other security features will be introduced, both within this stage and subsequently, to address other brute force attacks.

Implementing brute-force protection

Learn how to implement and configure Brute-Force Protection in Auth0.

Suspicious IP rate-limiting

Rate limiting (throttling) is a useful tool for countering high-volume, brute-force attacks by restricting (including outright blocking) suspicious or confirmed-malicious IP addresses.

For example, an IP that exceeds a threshold for login or signup attempts — across any number of accounts — within a given period is engaging in malicious behavior that strongly deviates from normal customer usage. Rate-limiting or blocking such abusive actors complements the individual account protections outlined above.

Additionally, blocking or rate-limiting IPs included within third-party Cybersecurity Threat Intelligence (CTI) feeds can proactively lessen the burden imposed by abusive actors.

In addition to helping to defend against account takeovers, rate-limiting is also effective at mitigating the impact of DDoS attacks that target the Identity service. For sites and services whose functionality is gated behind a login, overwhelming the authentication service has the same outcome as any other type of DoS attack: denying the ability for legitimate customers to use the service.

Considerations: Any suspicious IP rate-limiting capability should allow administrators to:

- ☐ Configure the thresholds above which observed activity is considered malicious
- ☐ Define the enforcement action (e.g., rate-limit or block) and specifics (i.e., the enforced rate)
- ☐ Require the offending IP address to complete a challenge (e.g., a CAPTCHA) before the rate limit is lifted
- ☐ Incorporate CTI feeds into the protective measures

Rollout roadmap: Most organizations begin by rate-limiting IP addresses that are directly observed exceeding the default thresholds used to determine abuse. In time, they may tighten the restrictions and increase the consequences by lowering the abuse thresholds and introducing blocking. In parallel, organizations may also incorporate CTI into their defensive policies — whether by integrating with feeds to which the organization already subscribes or by sourcing trustworthy feeds for the first time.

Implementing suspicious IP throttling

Learn how to implement and configure Suspicious IP Throttling in Auth0.

Breached password detection

It's now all too common for huge credential repositories (password dumps), containing credentials harvested from data breaches, to be published or leaked online. Because many people reuse passwords across multiple accounts, these repositories enable threat actors to engage in anything from targeted account takeover attempts to large-scale credential stuffing attacks.

Consequently, being able to detect when your customers are using breached credentials is an important element of a strong Identity security posture.

Note that breached password detection works by comparing hashes of passwords, rather than the actual passwords themselves — so privacy is preserved.

Considerations: Some CIAM solutions will include breached password detection functionality (along with the ability to integrate third-party tools), while others will require a third-party utility to provide this capability. In either case, only put your trust in a breached password detection solution that:

- ☐ Automatically updates its database of breached passwords as new repositories are published/leaked
- ☐ Blocks new users from signing up with breached credentials, both to prevent legitimate users from inadvertently using compromised credentials and to prevent malicious users from creating accounts in legitimate users' names
- ☐ Prevents returning users from logging in with breached credentials, and instead requires them to complete a configurable password reset process
- ☐ Contacts a user (e.g., via email) if a login attempt occurs, to inform them about the risk and instruct them to change their password immediately

Rollout roadmap: Many organizations begin their breached password detection journey by making API calls to third-party databases (e.g., Have I Been Pwned). However, such external API calls can impede scalability efforts by introducing latency into the authentication flow, so the next step of maturity is to leverage capabilities within the CIAM platform and/or incorporate a subscription feed of breached credentials.

As average customer lifetime value increases, customer trust becomes even more important, leading the most mature organizations to subscribe to more advanced breached password detection services that actively seek out credential dumps on the dark web, rather than waiting for such databases to appear publicly.

Detect breached passwords sooner with Credential Guard

Typical breached password detection services rely on breach data released to the public. While useful, the dependency on publicly accessible breach data can create long windows of time (e.g., many months) between a credential repository being published in cybercrime marketplaces and those same passwords being incorporated into breached password detection services.

Credential Guard is an Auth0 service that dramatically shortens this window of opportunity. A dedicated security team infiltrates criminal communities and gains access to breach data that isn't otherwise available — typically discovering and incorporating breached passwords within 12-36 hours of them appearing.

Learn more about Auth0's Breached Password Detection capabilities



Stage 3

Advanced: Extend automation and integration, and refine the authentication experience

An organization at this stage is typically fully focused on optimizing and scaling digital offerings, while safeguarding the security and privacy of end users and their data. Customer expectations are high, with a growing base of users demanding frictionless and personalized experiences.

Meeting these needs requires solutions that streamline the customer experience — like adaptive MFA and step-up MFA — so that users enjoy convenient, yet secure, access throughout the digital journey.

Also paramount is the ability to integrate Identity within the organization's broader technology stack (e.g., marketing engine, content management system, data management platform, etc.), allowing consolidation of data silos and providing the organization with a single view into its customer base.

Major benefits:

- Lower-friction customer experiences and increased resistance to password-based Identity attacks due to passwordless authentication
- Reduced costs and freed-up resources from more efficient administration
- Stronger appeal to enterprise customers (B2B) and richer control over consumer access (B2C)
- Lessened risk and lower costs due to significant reduction in scripted (bot-based) attacks

At this point, organizations also explore enhancements to their backend Identity systems and infrastructure by introducing more advanced automation and process efficiencies. This will minimize any intervention required from IT and developers, freeing up these teams for more important priorities that can help move the business forward.

Category	Feature / Element / Capability	B2C	B2B
Authentication	WebAuthn-enabled authentication	✓	✓
	Organization-based authentication management & administration	✗	✓

Category	Feature / Element / Capability	B2C	B2B
Authorization	Granular access controls	✓	✓
Security	MFA via authenticator app	✓	✓
	MFA integrated into organization's app	✓	✓
	Adaptive MFA	✓	✓
	Bot Detection	✓	✓



Authentication

With a strong authentication foundation in place, organizations are now ready to introduce advanced capabilities that increase user and administrator convenience while strengthening security.

WebAuthn-enabled authentication

The Web Authentication JavaScript API standard — typically shortened to WebAuthn — is part of the FIDO2 set of specifications. FIDO2 enables customers to use supported devices to easily authenticate to online services in both mobile and desktop environments; WebAuthn allows websites to update their login pages to add FIDO-based authentication on supported browsers and platforms.

Importantly, authentication using WebAuthn-enabled device biometrics (e.g., Apple Face ID, Apple Touch ID, Windows Hello) or WebAuthn-enabled security keys (e.g., YubiKey, Feitian, Titan) simultaneously deliver high security (threat actors hate WebAuthn) and high usability.

Passkeys — FIDO credentials that are discoverable by browsers, or housed within native applications or security keys for passwordless authentication — have the potential to dramatically strengthen customer authentication compared to password-based logins. Passwords are at the root of many Identity threats, and passkeys represent a major step in relegating passwords to a much smaller role:

- Synced passkeys in particular deliver strong authentication in a familiar and convenient manner — making them beautifully suited for B2C, which is especially sensitive to friction (in fact, as of October 10, 2023, Google offers passkeys as the default option across personal Google Accounts)
- Device-bound passkeys are a great option for B2B markets and other customer applications (even within B2C) that require the even stronger authentication that comes from FIDO Certified authenticators and security keys

Considerations: Any modern CIAM solution should support WebAuthn-enabled authentication, so the main considerations are ease of configuration and a strong track record of keeping pace with evolving standards and specifications.

(B2B) Organization-based authentication management and administration

Building upon the enterprise federation and organization-based authorization introduced in the Scaling stage, organization-based authentication management and administration allows for customization at scale (branding, logos, fonts, etc.), to increase brand trust, customer adoption, and customer utilization.

Considerations: Ensure your CIAM solution enables you to:

- ☐ Configure customer-branded, federated login flows
- ☐ Simplify onboarding of business customers
- ☐ Customize authorization workflows for your customers at scale
- ☐ Build administrative capabilities into your products to allow your business customers to manage their own authentication at the organization level



Authorization

An organization's maturation often coincides with securing larger customers (B2B) or achieving a large user base (B2C). In both cases, the ability to more precisely control and more efficiently manage access privileges takes on greater importance.

Granular access controls

Granular access controls — e.g., Attribute-based Access Control (ABAC), Role-based Access Control (RBAC), Policy-based Access Control (PBAC) — allows administrators to grant and manage access permissions (e.g., what data can be seen, what actions can be performed) with more precision than coarse approaches (e.g., by organization) permit.

In B2C contexts, granular access controls can accommodate different tiers of service, add-ons, etc.

In B2B contexts, granular access controls enable application administrators to manage the permissions of users within different teams, departments, and other groupings. Many regulations, certifications, and standards require RBAC as the minimum granularity of access control making it table stakes for selling into enterprises and mature organizations.

Considerations: Solving authorization in an application is not trivial, and you should only consider solutions that enable granular access controls that are:

- ☐ Reviewable, making it easy to determine what users can access what resources and perform what actions
- ☐ Easy to manage/change, with explicit and traceable change management
- ☐ Auditable, with detailed logs that reveal what users tried to access what resources (or perform what actions), and when
- ☐ Fast, because authorization decisions are made as part of most flows/requests, making delays visible to customers
- ☐ Reliable, as authorization is a key element of maintaining security and compliance

Rollout roadmap: For some organizations, RBAC may be sufficient; for others, these granular controls represent an intermediate step on the path to Fine-Grained Authorization (FGA), which is typically implemented in the Strategic stage. Moreover, progression to FGA can itself be achieved in multiple steps: starting with adoption of an Open FGA solution, before advancing to a more fully featured and supported commercial implementation.



Security

In addition to adding bot detection (explained below), and strengthening authentication security, Stage 3 is where many organizations make meaningful progress in operationalizing security.

In particular, IT and security teams will work to consolidate siloed signals and alerts into dashboards that provide real-time monitoring. By presenting a more holistic and timely view of the organization's security status, these dashboards contribute to reducing mean time to detect (MTTD) and mean time to respond (MTTR).

Similarly, leveraging extensibility — for instance, by linking Identity flows with specialized security tooling — can strengthen an organization's Identity security posture by increasing visibility and enabling additional response actions.

Adaptive MFA

Adaptive multi-factor authentication (Adaptive MFA) introduces additional intelligence into Identity flows by taking into account the ever-changing context in which an authentication request is made. By dynamically adapting security and authentication policies, adaptive MFA can simultaneously improve both security and the user experience.

For example, an adaptive MFA policy can reduce friction for users by prompting for MFA less frequently when customers sign in through SSO or through a managed or known device. However, the same adaptive MFA solution can prompt for an additional or more secure authentication factor when the risk associated with a request is assessed to be higher — for instance, if a login attempt is made at an unusual time of day or from a new device, or if a logged-in user is attempting to access particularly sensitive resources or information.

Considerations: To find an Adaptive MFA solution that fits your organization's specific needs, look for products that:

- ☐ Offer a high degree of flexibility and control — both of which are largely dependent upon the MFA factors available and the richness of the contextual intelligence incorporated into the risk assessment
- ☐ Incorporate a range of risk signals, including device, network, location, travel, IP — and even external risk signals from third parties — at each step of the authentication process
- ☐ Support step-up authentication, reserving additional MFA challenges for specific situations (e.g., when a user is attempting to access sensitive data or change account details)

Fine-tune your authentication process with Adaptive MFA

Auth0 Adaptive MFA provides intelligent access that fits your business needs while adapting to customers' login behaviors.

Learn more about how Adaptive MFA works

Bot detection

Bot traffic plagues Identity flows at all points of the customer journey, as malicious actors aim to fraudulently register fake users, validate credentials, and take over existing accounts. Plus, due to its sheer volume, bot traffic burdens application providers with extra compute costs.

By analyzing a variety of data sources and observations, it's possible to determine with high confidence when a connection attempt is coming from a bot — and trigger a policy (e.g., present a CAPTCHA) in response.

The goal of such a solution is to eliminate as much bot traffic as possible, while minimizing friction for legitimate customers. For instance, it's technically trivial to present a CAPTCHA to every user, but doing so would create a frustrating user experience, which itself would lead to lost business. An effective bot detection solution identifies the large majority of bot traffic while only very occasionally imposing a CAPTCHA (or some other policy) upon a legitimate human customer.

Considerations: To address today's bot-driven Identity threats, a bot detection feature needs to include:

- ☐ An abundance of data sources, to permit the depth of analysis required to detect modern bots
- ☐ AI-based detections, because threat actors are adept at learning how rules-based systems operate
- ☐ A range of response options (e.g., block, ignore, present a CAPTCHA)

Using machines to fight machines

As a vital part of the Attack Protection add-on in the Customer Identity Cloud, the Bot Detection feature mitigates scripted attacks (e.g., credential stuffing, password guessing, password spraying) against native applications, passwordless flows, and custom login pages.

By using machine learning (ML) to analyze more than 60 data sources — like past events associated with an IP address, recent login history, IP reputation data, and an assortment of other factors — Bot Detection can predict when an Identity request is likely to be coming from a bot. Above a certain prediction/confidence threshold, the authentication flow presents a countermeasure, such as a CAPTCHA.

Importantly, these improved defensive capabilities were achieved without introducing unnecessary user friction — by carefully training and continually tuning the AI at the heart of the Bot Detection feature, we can ensure that human users are rarely presented with a CAPTCHA.

Plus, a detailed internal study examining the before-and-after effects of Bot Detection has revealed a strong deterrent effect:

- On average, customers in the study who enabled Bot Detection saw a reduction in malicious traffic of more than 40%
- Some larger customers in the study saw bot traffic drop by nearly 90%!

These findings suggest that threat actors prefer to avoid targeting organizations with state-of-the-art defenses in place.



Stage 4

Strategic: Optimize and extend Identity

Organizations that reach stage 4 have mature digital and omnichannel initiatives that optimize for both user experience and security, and they view Identity as strategic to success.

Such companies typically have a robust and growing customer base that is diverse and often global. These customers interact with your business via multiple channels, while demanding more advanced features, integrations, and Identity capabilities for delightful yet trusted experiences. Different teams across the company work together to devise, develop, sell, and scale these digital offerings, but each has its own set of distinct requirements and priorities.

Major benefits:

- Stronger security posture reduces risk and increases appeal to customers
- More granular access control unlocks additional application capabilities

Addressing the varied and ever-evolving demands of both internal and external stakeholders at this stage is a balancing act like no other. As companies scale and evolve, so do customer expectations — against the ever-present backdrop of a dynamic threat landscape, changing regulatory requirements, and evolving Identity industry.

Category	Feature / Element / Capability	B2C	B2B
Authentication	Continuous Authentication	✓	✓
Authorization	Fine-grained Access Control / Authentication	✓	✓
Security	Step-Up Authentication	✓	✓



Authentication

In the traditional authentication model, a user is challenged to produce one or more factors — e.g., knowledge, possession, inherence — that sufficiently prove their ownership of a digital Identity associated with an account (and the privileges associated with it). Outside the use of step-up authentication, this challenge occurs only once — thereafter, for the duration of the session, the user's Identity is trusted.

However, as threat actors adopt session hijacking and other sophisticated Identity threats, new security measures are needed.

Continuous authentication

Continuous authentication is based on the idea that systems should still be managing Identity risk even after the initial authentication is granted.

For example, rather than assuming that the conditions that were true when initial authentication was granted are unchanging, they are instead retested at fixed or random intervals, and/or in response to some observation or trigger. If a condition is found to have changed, the system can enforce an action like terminating the session and requiring the user to re-authenticate, or challenging the user with step-up authentication.

Conversely, because continuous authentication can validate that context is still secure, it can be used to prolong sessions — improving the user experience by reducing or eliminating the need to re-authenticate unless the user has explicitly logged out.

Rollout roadmap: Continuous authentication can start with relatively simple context, like device posture and geolocation, before evolving to include additional risk signals (e.g., from a threat intelligence feed or through tight integration with fine-grained authorization).



Authorization

In keeping with the theme of this stage, optimizing authorization focuses on enabling developers to design authorization models — from coarse-grained to fine-grained — in a way that's centralized, flexible, fast, scalable, and easy to use.

Fine-grained authorization

As privacy and security awareness increases, and new use cases emerge, the need to apply the principle of least privilege across organizations is becoming more of a product requirement than a 'nice-to-have' feature. One result of this shift is that enterprises are recognizing the benefits of fine-grained authorization (FGA), which goes beyond traditional granular access controls to enable greater flexibility for enterprises with complex permission models.

FGA allows organizations to centralize access control across every application they build or acquire, and makes it easy for application developers to implement advanced permissions and sharing strategies. This is 'fine grained' because there is no limit to the granularity at which builders of the system can make authorization decisions — application builders have the freedom to determine precisely how granular they want authorization to be, and users are granted control to determine who has specific permissions on objects they manage.

For example, collaboration and social features (e.g., the "Share" button) are things modern software users expect, even in enterprise contexts, when collaborating on documents, spreadsheets, design mockups, project boards, etc., and FGA allows the easy sharing of these objects between users in a scalable manner.

Considerations: As with other authentication and authorization functions, it's important that your FGA solution provides:

- ☐ Low latency: every millisecond can impact your application's overall latency
- ☐ Availability and reliability: authorization is mission-critical, and any downtime can disrupt user access

- ☐ Scalability: the solution should be capable of supporting your business' growth, including accommodating unplanned needs (such as those relating to sudden increases in customer adoption or from merger and acquisition activity)
- ☐ Policy flexibility: support for different kinds of policies like RBAC or ABAC give you the ability to choose the best policy for your app, and to update policies as your needs evolve.

Rollout roadmap: As noted earlier, organizations may elect to start with an Open FGA solution before progressing to a commercial option.

Authorization built to scale

While Open FGA is a great option, the customer is responsible for administration, support, and other operational aspects. In contrast, Auth0 Fine Grained Authorization provides a wide range of benefits, including:

- High availability, database migrations, backups, and disaster recovery
- Caching, for reduced latency when calling the FGA API
- Cloud security and infrastructure provisioning, plus security patching
- Monitoring and support
- Status and management dashboard
- Supporting SOC 2 and HIPAA compliance



Security

These final refinements to securing Identity focus on maintaining a strong security posture while minimizing friction for users.

Step-up authentication

Step-up authentication is a way to strike a balance between security and friction, by adapting Identity requests to the importance of the resource and the risk level if it were to be exposed. This approach ensures users can access some resources with one set of credentials but will prompt them for an additional authentication factor when they request access to sensitive resources.

For example, an organization that wants to deploy a membership model could use step-up authentication to limit complete access to the associated site or service to paying users.

Similarly, step up authentication is applicable when users want seamless access to certain resources, but organizations want to verify their identities before users can access anything more sensitive.

Summary

Customer Identity is so broad and complex that it can easily seem like an overwhelming topic — but breaking down its implementation into distinct stages and components shows that a mature Customer Identity infrastructure is achievable.

Stage	Category	Feature / Element / Capability	B2C	B2B
Fundamental	**Authentication**	Social logins	✓	✓
		Consent management	✓	✓
	Authorization	Consolidate and connect to existing user stores	✓	✓
	Security	Password hashing	✓	✓
Scaling	**Authentication**	Enterprise federation	✗	✓
		Consistent login experiences	✓	✓
	Authorization	Organization-based management & administration	✗	✓
	Security	Multi-factor authentication	✓	✓
		Brute force attack detection for individual accounts	✓	✓
		Suspicious IP rate-limiting	✓	✓
		Breached password detection	✓	✓
Advanced	**Authentication**	WebAuthn-enabled authentication	✓	✓
		Organization-based authentication management & administration	✗	✓
	Authorization	Granular access controls	✓	✓
	Security	MFA via authenticator app	✓	✓
		MFA integrated into organization's app	✓	✓
		Adaptive MFA	✓	✓
		Bot Detection	✓	✓

Stage	Category	Feature / Element / Capability	B2C	B2B
Strategic	**Authentication**	Continuous authentication	✓	✓
	Authorization	Fine-grained authorization	✓	✓
	Security	Step-up authentication	✓	✓

Auth0 can help

With an extensive collection of products and features, Auth0 empowers your app developers, digital leaders, and security teams to accelerate time to market and grow your business.

Please reach out to discuss where you are on your Identity maturation journey and how we can help.

Stage	Product/Feature	Summary
Fundamental	Social Login / Single Sign-On	Give your customers the freedom of Single Sign-On through their preferred Identity provider — while keeping the control and enhanced security you need
	Consent Management	Seamlessly integrate with third-party consent management platforms to acquire, log, and track user consent
	Database Connections	Authenticate users, with credentials securely stored in the Auth0 user store or in your own database
Scaling	Universal Login	Secure a seamless journey of digital access for users — with or without code — with powerful flows, extensive branding customization, varied login methods and more
	Enterprise Connections	Authenticate users in an external, federated identity provider (IdP) such as Azure AD, Google Workspace, PingFederate, and more
	Organizations	Manage your business customers and partners as organizations, and easily configure and customize how their end users access your applications
	Multi-Factor Authentication	Add a layer of security during login that requires users to provide more than one credential to prove their digital identity
	Brute-Force Protection	Add a layer of security during login that requires users to provide more than one credential to prove their digital identity

Stage	Product/Feature	Summary
Scaling	Suspicious IP Throttling	Block traffic from any IP address that rapidly attempts too many logins or signups
	Breached Password Detection	Protect your applications from bad actors signing up or logging in with stolen credentials
Advanced	FIDO Authentication with WebAuthn	Protect your users and data with one of the most secure and usable authentication method on the web
	Role-based Access Control	Assign permissions to users based on their role within an organization
	Auth0 Guardian	A mobile application that can deliver push notifications to a user's pre-registered device, from which the user can immediately allow or deny account access via the press of a button
	Bot Detection	Mitigates scripted attacks by detecting when a request is likely coming from a bot
	Security Center	Provides observability tools that allow you to see potential attack trends and quickly respond to them in real-time
	Continuous Authentication	Helps to manage post-authentication Identity risks and can increase user convenience
Strategic	Credential Guard	Screens for breaches to allow faster notification of compromised credentials
	Step-Up Authentication	Applications that allow access to different types of resources can require users to authenticate with a stronger authentication mechanism to access sensitive resources

For documents with privacy/legal concepts or privacy/security advice:

These materials and any recommendations within are not legal, privacy, security, compliance, or business advice. These materials are intended for general informational purposes only and may not reflect the most current security, privacy, and legal developments nor all relevant issues. You are responsible for obtaining legal, security, privacy, compliance, or business advice from your own lawyer or other professional advisor and should not rely on the recommendations herein. Okta is not liable to you for any loss or damages that may result from your implementation of any recommendations in these materials. Okta makes no representations, warranties, or other assurances regarding the content of these materials. Information regarding Okta's contractual assurances to its customers can be found at okta.com/agreements.

About Okta

Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology—anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at okta.com.