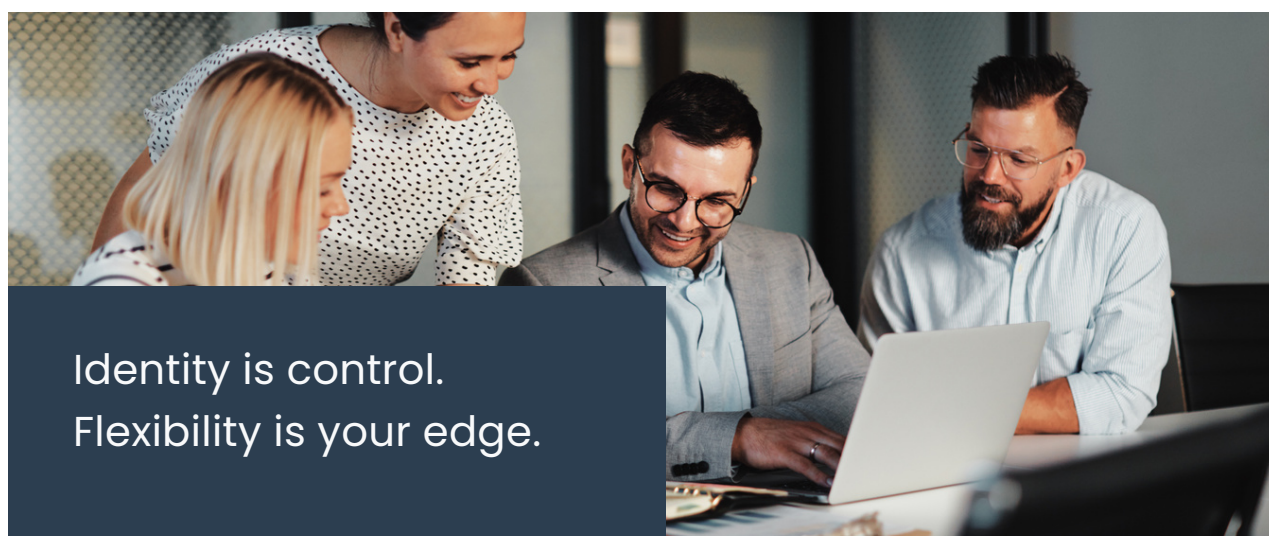


Commercial Platforms vs Managed Keycloak



Choosing the right IAM for Your organisation



Identity is control.
Flexibility is your edge.

Your users expect speed and your business needs security.
The right IAM platform delivers both.

Keycloak is a powerful open-source IAM offering SSO, MFA, federation, and user self-service with no license fees. But on its own, it requires time, expertise, and effort to manage.

That's where Inteca's Managed Keycloak comes in. We turn open-source freedom into a fully supported, production-ready IAM service **without the vendor lock-in**.

This guide compares 6 top enterprise IAM platforms so you can see where Keycloak fits, how it stacks up, and why a managed approach might be the best for you.



Who we're comparing

We evaluated 6 leading IAM vendors against Keycloak — all enterprise-ready:

Okta, Auth0, Ping Identity, ForgeRock, Microsoft Entra ID and OneLogin.

Each has strengths. Each has trade-offs.

Only Keycloak gives you full control — and with Inteca's Managed Keycloak, that control is simple, secure, and supported.



What we evaluated

We focused on what really matters to enterprise teams:

- Vendor lock-in risk
- SSO flexibility
- Multi-tenancy support
- Federation options
- MFA & passwordless login
- User self-service

Because choosing an IAM is a strategic decision.

Cloud-native IAM with strong integrations and fast deployment

Deployment Model

SaaS-only (fully cloud-based)

Okta is one of the most widely adopted IAM platforms for enterprises. It offers a broad feature set focused on ease of use, security, and fast integration with thousands of apps. It's ideal for organizations that want a fast, cloud-first IAM solution without managing infrastructure.

Vendor Lock-In

High. Okta is proprietary and fully cloud-hosted. Migration can be complex.

SSO Flexibility

Excellent. Thousands of pre-built integrations via the Okta Integration Network.

Multi-Tenancy

Supported through organizational units and policies, but limited compared to realm-based models like Keycloak.

Federation

Strong support for SAML, OIDC, and identity brokering across social and enterprise IdPs.

MFA & Passwordless

Built-in MFA with Okta Verify, WebAuthn, biometrics, and adaptive policies.

User Self-Service

Very user-friendly. Password resets, profile updates, MFA enrollment are all streamlined.

Best for: Enterprises seeking quick, low-effort deployment and deep app integration.

Limitations: No self-hosted option. Less flexibility for custom logic or on-prem scenarios. Higher total cost at scale.



Auth0

Developer-friendly CIAM with fast integration and flexible login flows

Deployment Model

SaaS-only (fully cloud-based, part of Okta)

Auth0 focuses on customer identity (CIAM) and developer experience. It's widely used to embed secure login, social auth, and identity federation into web and mobile apps. Ideal for product teams that want flexibility without building IAM from scratch.

Vendor Lock-In

Moderate to high. Proprietary SaaS with custom rule logic. Migration requires effort.

SSO Flexibility

Excellent. Full support for SAML, OIDC, OAuth2, and social logins. Easy integration with most apps.

Multi-Tenancy

Supported via the "Organizations" feature. Useful for B2B SaaS but less isolated than realm-based models.

Federation

Strong. Easily integrates with social and enterprise IdPs. Identity brokering is straightforward.

MFA & Passwordless

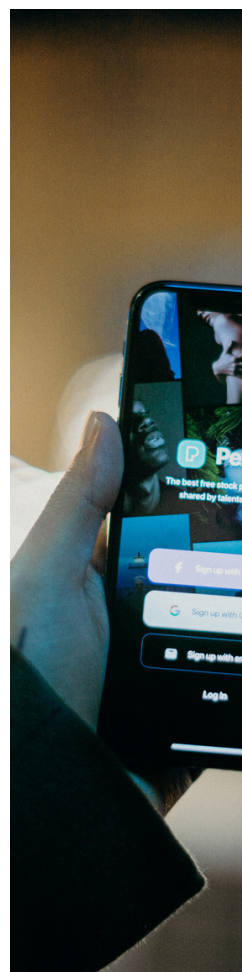
Built-in support for MFA, WebAuthn, SMS/email, and passwordless login. Adaptive policies available.

User Self-Service

Modern, customizable login and self-service pages. Great user experience out-of-the-box.

Best for: Product teams building customer-facing apps that need secure, fast login with rich customization.

Limitations: No self-hosted option. Costs rise quickly with scale. Complex logic tied to proprietary rules and actions.



Ping Identity

inteca.com

Flexible enterprise IAM with hybrid deployment and strong federation

Deployment Model

Both SaaS (PingOne) and self-hosted (PingFederate)

Ping Identity offers a modular IAM suite for large enterprises. Known for its strong federation capabilities, legacy protocol support, and deployment flexibility, Ping is often used in highly regulated industries and hybrid IT environments.

Vendor Lock-In

Moderate. Standards-based with flexible deployment options. Less lock-in if self-hosted.

SSO Flexibility

Strong. Supports SAML, OIDC, and even older protocols like WS-Fed and Kerberos. Works well in complex environments.

Multi-Tenancy

Limited. Possible via custom setups or multiple instances, but lacks a native realm-style model.

Federation

Excellent. One of Ping's core strengths. Acts as both IdP and SP, ideal for partner and enterprise federation.

MFA & Passwordless

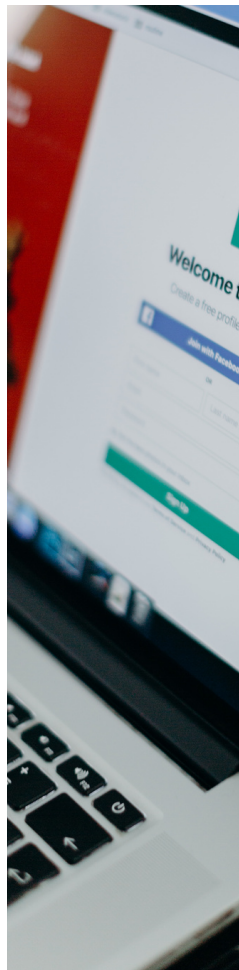
Available via PingID and adaptive authentication policies. Supports push, OTP, and passwordless options.

User Self-Service

Basic out-of-the-box. Can be extended but requires more setup than SaaS-first options.

Best for: Large enterprises with hybrid IT, complex federation needs, or strict compliance requirements.

Limitations: Higher complexity. Multi-component setup may require dedicated IAM expertise. UI and developer UX not as modern as newer SaaS platforms.



ForgeRock

Enterprise-grade IAM with full-stack capabilities and advanced customization

Deployment Model

Both SaaS (ForgeRock Identity Cloud) and self-hosted (on-prem or private cloud)

ForgeRock offers a IAM platform covering access management, identity provisioning, directory services, and consent management. It's built for complex environments and is highly extensible.

Vendor Lock-In

Moderate. Strong standards support, but advanced features and scripting rely on ForgeRock-specific tools.

SSO Flexibility

Strong. Full support for SAML, OIDC, OAuth2, and fine-grained access policies.

Multi-Tenancy

Good. Supports realms for tenant separation, similar to Keycloak. Suitable for multi-organization environments.

Federation

Excellent. Supports enterprise IdPs and identity brokering. Includes tools for consent and privacy management (UMA).

MFA & Passwordless

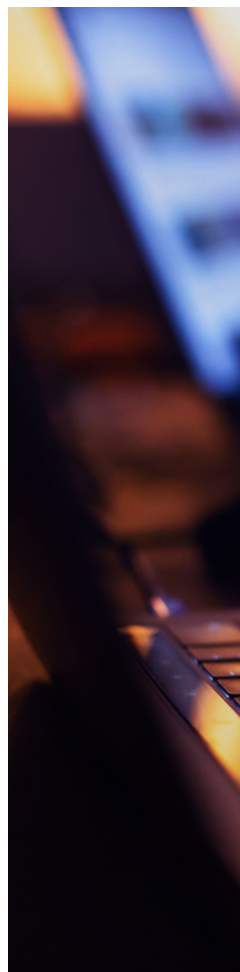
Built-in MFA, passwordless options, and adaptive access. Integrates with biometric and WebAuthn devices.

User Self-Service

Robust features including registration, password reset, consent control, and profile management.

Best for: Large enterprises needing full IAM stack, custom logic, and hybrid deployment flexibility.

Limitations: Complex to deploy and operate. Higher cost and steeper learning curve than lighter IAM solutions.



Microsoft Entra ID

inteca.com

IAM built into the Microsoft ecosystem with strong enterprise security

Deployment Model

SaaS (cloud-only, part of Microsoft Azure)

Formerly Azure Active Directory, Entra ID is Microsoft's identity platform for securing access across Microsoft 365, Azure, and thousands of third-party apps. It's deeply integrated into enterprise environments that rely on Microsoft infrastructure.

Vendor Lock-In

High. Tight integration with Microsoft services. Limited flexibility outside the Azure ecosystem.

SSO Flexibility

Strong, especially for Microsoft apps. Supports SAML, OIDC, OAuth2, and app integrations via Azure AD gallery.

Multi-Tenancy

Good. Each tenant is isolated. B2B collaboration and multi-tenant app registrations are supported.

Federation

Strong. Supports external IdPs and directory sync with on-prem AD via Azure AD Connect.

MFA & Passwordless

Robust. Includes Microsoft Authenticator, FIDO2, phone sign-in, and adaptive access via Conditional Access.

User Self-Service

Well-developed. Password reset, profile updates, MFA setup, and self-enrollment included.

Best for: Organizations using Microsoft 365, Azure, or hybrid AD environments. Ideal for workforce identity.

Limitations: Cloud-only. Less flexibility for custom auth logic or non-Microsoft ecosystems. Complex for external user scenarios.



OneLogin

inteca.com

Simple, cloud-based IAM with strong core features and ease of use

Deployment Model

SaaS (cloud-based) with connectors for on-prem directories

OneLogin offers a user-friendly IAM platform focused on ease of deployment, SSO, and adaptive MFA. Now part of One Identity, it serves mid-size to large enterprises looking for a cost-effective, cloud-first solution.

Vendor Lock-In

Moderate. Proprietary SaaS, but supports open standards and integration with external directories.

SSO Flexibility

Good. Supports SAML, OIDC, and thousands of apps via its connector catalog.

Multi-Tenancy

Basic. Multi-org scenarios possible through roles and policies but lacks true realm isolation.

Federation

Solid. Connects with enterprise IdPs and social providers, suitable for most SSO use cases.

MFA & Passwordless

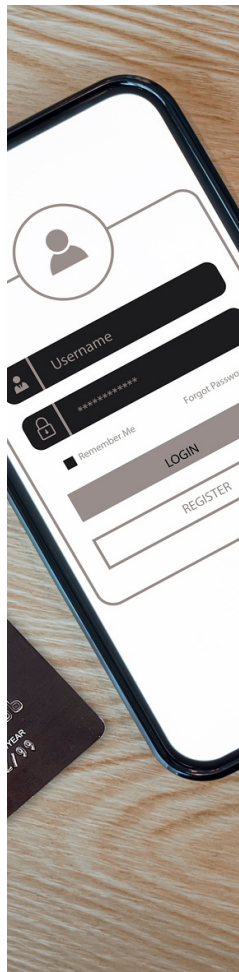
Built-in adaptive MFA (SmartFactor), push notifications, biometrics, and WebAuthn support.

User Self-Service

Intuitive. Users can reset passwords, update profiles, and manage MFA with minimal support.

Best for: Organizations seeking quick IAM deployment with solid SSO and MFA at a lower cost.

Limitations: SaaS-only. Less suited for complex multi-tenant or custom auth needs. Feature set not as deep as larger players.



Keycloak

Open-source IAM with full control — made simple, scalable, and supported

Deployment Model

Self-hosted or cloud-managed by Inteca

Keycloak is a powerful open-source IAM platform offering enterprise-grade features like SSO, federation, MFA, and user self-service — all without license fees. With Inteca's Managed Keycloak, you get expert support, enterprise reliability, and zero infrastructure overhead.

Vendor Lock-In

Low. Fully open-source and standards-based. Your data, your control — always.

SSO Flexibility

Strong. Supports OIDC, SAML, OAuth2, and fine-grained authorization policies. Easily integrates with custom and enterprise apps.

Multi-Tenancy

Excellent. Native realm-based isolation supports complex B2B or multi-org scenarios.

Federation

Robust. Connects to social logins, external IdPs, LDAP, Active Directory, and more.

MFA & Passwordless

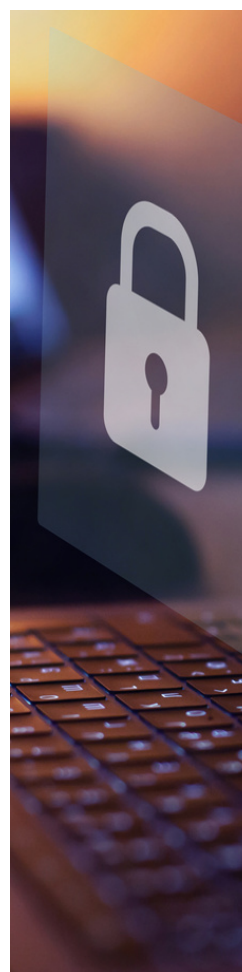
Built-in support for OTP, WebAuthn, FIDO2, and custom MFA flows.

User Self-Service

Customizable login pages, password resets, and user management. Fully themeable for your brand and UX.

Best for: Enterprises that want open-source freedom with commercial-level support. Perfect for custom IAM strategies, B2B platforms, and compliance-sensitive environments.

Limitations: Requires in-house expertise to deploy, secure, and scale. That's why we manage it for you.



Implementing Keycloak vs. Commercial Solutions



Factor	Red Hat – Keycloak	Commercial IAM (Okta, Auth0, One Login etc.)
Control & Customization	Full control over authentication flows, identity storage, and security policies	Limited customization; must adhere to the provider's framework
Cost	Open-source (free), but requires hosting, maintenance, and technical knowledge – you can outsource Keycloak as a managed service to companies like Inteca	Subscription-based pricing; can be costly because accumulates over time
Security	Adjustable to implementation of advanced practices (WebAuthn, FIDO2, MFA, SSO, passkeys policies) giving you zero trust security – you can adjust specific security measures to your organization's unique risks	Enterprise-grade security built-in, with continuous updates & compliance adherence
Scalability	No scale limit, but requires infrastructure management	Auto-scaling, managed service with global availability, cost increase significantly with scaling
Ease of Implementation	Requires setup, integration, and ongoing maintenance which can be covered by Keycloak Managed Service	Turnkey solution with ready-to-use integrations
Compliance	Compliance is self-managed (GDPR, NIST, PSD2) and adjustable to your regulations	Built-in compliance certifications

Who should choose which?

- **Keycloak** – Ideal for teams needing deep customization and control, or wanting to avoid per-user fees.
- **Commercial solutions** – Best for quick deployments, minimal maintenance, and built-in pre-set compliance.

Next steps



From analysis and design to implementation and constant maintenance, we provide your company with solutions to succeed

01

Schedule a consultation – reach out to our team for a personalized assessment of your current IAM landscape and passwordless strategy

Contact form



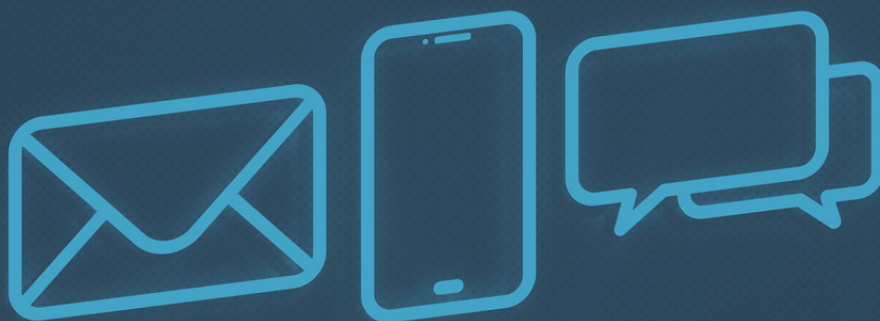
02

Explore custom solutions – let's discuss how Keycloak and our expertise can tailor a solution that meets your specific security and compliance needs.

03

Ongoing support – learn about our managed services to ensure continuous optimization and support throughout your passwordless journey.





Contact Information

Email :

contact@inteca.com

Phone Number :

+48 881 309 604

Contact form :

inteca.com/contact/

