

10 Ways Omada Simplifies IGA

Your environment is complex. Your Identity Governance shouldn't be.

Every new application, cloud service, and automation initiative adds identities and access to govern. When governance is fragmented or manual, access piles up, visibility fades, and complexity grows. Omada Identity Cloud takes a simpler approach: proven governance that is fast to deploy, easy to operate, and built to adapt across human, machine, and AI agent identities. Here are ten ways Omada makes IGA simpler.

01

One complete view of every identity

Identity and access data is often spread across directories, HR systems, cloud platforms, and applications, making it difficult to maintain a clear, current picture. Omada brings human, machine, and AI agent identities, accounts, roles, and entitlements into a single access model across hybrid environments. Orphaned accounts, excess privileges, and access that no longer fits policy become visible in business context, so teams can identify and act on issues faster.

02

Configure, don't code

Complex IGA deployments stall on custom code and specialized resources. Omada replaces that with drag-and-drop configuration you manage directly in the browser, so you build and adjust workflows without relying on developers. Deployments move faster, upgrades stay simple, and total cost of ownership comes down. Your team owns and operates the platform without depending on consultants.

03

Access that follows the business, automatically

Access should reflect what people actually do, not accumulate through historical exceptions. Omada grants and removes access as roles, projects, and regional requirements change, keeping least privilege in place without constant manual intervention. Requests and certifications carry business context, so decision-makers can approve with confidence. When the business need ends, access is removed through governed policy, with evidence captured at every step.

04

Intelligence that turns insight into action

Visibility alone does not reduce risk. Omada Access Intelligence connects discovery, analytics, machine learning role insights, and governed remediation in one coordinated process, so findings become controlled changes with full traceability rather than reports that sit unused. Cleaner data sharpens the intelligence, and sharper intelligence drives faster, more confident action. Over time, that means fewer orphaned accounts, fewer audit findings, and shorter certification cycles.

05

Certifications that focus on real risk

Periodic access certifications can turn into high-volume approval exercises that create friction without reducing exposure. Omada makes certifications risk-aware, so attention goes where it matters most. SMART Certifications group related items by real access patterns, while rolling, policy-driven campaigns keep reviews focused and manageable. Segregation of duties is enforced in workflow, and every decision is captured with context and timestamps, so audit-ready evidence is a byproduct of daily operation.

06

AI that speeds decisions, with people in control

Omada applies AI to scale governance while keeping people in control. It clarifies the intent behind access requests, recommends appropriate entitlements, and prioritizes the reviews that carry the most risk. AI assisted guidance helps managers make faster, more informed decisions while approvals, policy checks, and audit trails remain in place. Your team keeps final approval, and every decision stays inside a governed workflow.

07

Non-human identities governed with the same rigor

Service accounts, API keys, bots, and now AI agents are multiplying rapidly, and they often hold elevated privileges outside traditional governance frameworks. Omada governs machine identities as a distinct identity type, applying the same ownership, least privilege, dormant-access detection, and certification you apply to people. For AI agents, Omada Agent Governance, now in technical preview, extends this discipline to who owns each agent, what it can reach, and whether its access is used. Governance stays complete as automation and AI adoption grow.

08

Connectivity that extends reach, not your attack surface

Bringing on-premises systems under cloud-based governance can add connectivity complexity. Omada's Cloud Application Gateway uses outbound-only connectivity, so your firewalls do not need to accept inbound traffic from the cloud. Data is encrypted before it leaves your environment and decrypted only with keys you control. Pre-built connectors and support for the Shared Signals Framework help bring systems under governance quickly and exchange risk signals across your security ecosystem.

09

A platform that runs on your terms

Omada gives you deployment options to match your operational, regulatory, and data-control requirements, from SaaS to customer-controlled cloud and sovereign deployment models. You can choose the model that fits your organization while maintaining a consistent approach to identity governance. That flexibility helps you meet changing requirements without rethinking your governance strategy from the ground up.

10

A fast start, and a proven path to maturity

Modern IGA should not require a multi-year program or an army of consultants to get started. Omada delivers a production-ready governance foundation in a guaranteed 12 weeks, built on IdentityPROCESS+, a methodology informed by more than two decades of enterprise deployments. From there, Omada helps you advance your IGA maturity, using proven practices and use cases to expand governance over time as your priorities and requirements evolve.

Embrace IGA Simplicity.

Omada Identity Cloud delivers proven governance that is fast to deploy, easy to operate, and built to adapt, so your identity governance can keep pace as your organization changes.

Contact us to see how Omada can simplify your IGA.