

12 Best Identity Governance and Administration (IGA) Solutions for 2025

[According to User Reviews]



Looking for an IGA solution in 2025 feels overwhelming – too many options, lots of flashy features, and everyone claiming to be the best choice.

But here's the thing: choosing the wrong IGA solution isn't just frustrating – it can impact your entire organization's security and productivity.

In this guide, we'll break down the 12 best IGA platforms based on what matters most: ease of implementation, automation capabilities, user experience, and actual results.

What to Look for in Identity Governance and Administration (IGA) Solutions

Identity Lifecycle Management

Efficiently manages the [entire lifecycle](#) of identities, from onboarding to offboarding. This feature ensures employees have the right access from day one and lose access immediately upon departure, minimizing security risks. It also simplifies access changes during promotions, department shifts, or role changes.

Access Certification

Streamlines periodic reviews of [access rights](#). Validating that access permissions align with current roles and responsibilities lowers the risk of unnecessary or excessive access while meeting compliance requirements.

Dynamic Role-, Policy-, and Attribute-Based Access Control

Enhances security by assigning permissions [based on predefined job roles](#), policies, or attributes. This simplifies access management, ensuring users only have the access necessary for their responsibilities, reducing exposure to unauthorized activities.

Just-in-Time (JIT) Access Provisioning

Secures sensitive systems and critical data by limiting access to only the amount of time needed to perform necessary actions. The ability to enforce JIT access reduces or eliminates the need for standing privileges, thus reducing the likelihood of privilege compromise or abuse.

Access Request and Approval Workflows

[Automates](#) the resource access process. With this, users can easily request access while approval workflows ensure appropriate authorization, maintaining transparency and accountability in access provisioning.

Segregation of Duties (SoD)

Prevents conflicts of interest and reduces fraud by ensuring that critical tasks require multiple users to complete. [SoD](#) enforces separation of responsibilities, safeguarding sensitive operations from internal misuse.








Regulatory Compliance Management

Simplifies adherence to regulatory frameworks (e.g., SOX, GDPR, HIPAA) and internal policies through audit trails, automated access reviews, and detailed compliance reports. This keeps your organization [audit-ready](#) and reduces regulatory risks.

Integration Capabilities

Ensure seamless [compatibility with existing cloud and on-prem systems](#) such as directories, applications, and infrastructure, including homegrown and private systems. Robust integration capabilities create a unified identity governance ecosystem that minimizes friction and operational silos.

The Top 12 IGA Solutions for 2025

1.  **ConductorOne**
2.  **SailPoint**
3.  **Saviynt**
4.  **Omada**
5.  **Microsoft Entra**
6.  **Okta IGA**
7.  **Opal Security**
8.  **Lumos**
9.  **Oracle Identity Governance**
10.  **One Identity Manager**
11.  **IBM Security Verify Governance**
12.  **Ping Identity**

1. ConductorOne

ConductorOne is a modern identity governance platform that automates and secures how organizations handle human and non-human identity permissions.

It streamlines access requests and access reviews, enforces least-privilege principles, and provides clear visibility into permissions across cloud and on-premises systems.

ConductorOne connects smoothly with SaaS apps, cloud and on-prem infrastructure, and identity providers to simplify access management. It also automates the entire lifecycle of user access — from granting initial permissions (provisioning) to removing them when no longer needed (deprovisioning).

Key Features of ConductorOne's Identity Governance & Administration Solution

- **Unified Identity Graph.** Aggregates and visualizes access and identity data across cloud and on-premises systems, enabling comprehensive visibility and control over user permissions.
- **Just-in-Time Access.** Reduces standing permissions by granting temporary access to applications and infrastructure only when needed, minimizing security risks while ensuring operational continuity.
- **Automated Access Reviews.** Streamlines compliance by automating periodic and targeted access reviews, ensuring that permissions align with business needs and regulatory requirements without manual intervention.
- **Copilot AI.** Leverages AI-powered insights to assist with decision-making in identity governance, such as recommending appropriate permissions or flagging anomalies in access patterns.
- **Shadow IT Detection.** Identifies unapproved applications and monitors unauthorized tool usage, providing actionable insights to enforce governance policies and mitigate risks.
- **Identity Lifecycle Management.** Automates the management of identities throughout their lifecycle, from onboarding to offboarding, ensuring that access permissions remain appropriate at every stage.

What Makes ConductorOne Different?



Time-to-Value Measured in Hours, Not Months

Traditional IGA implementations can drag on for months or even years. ConductorOne flips this on its head with a deployment process that takes hours instead of months. The platform comes with prebuilt connectors for popular tools and services, and the modern API-first architecture means you can extend it to custom applications without the usual integration headaches.



No-Code Automation That Actually Works

We've all dealt with complex IGA tools that require specialized knowledge to automate even basic workflows. ConductorOne takes a different approach with true no-code automation that lets you build advanced access management workflows through an intuitive interface. You can set up everything from simple approval chains to complex conditional logic without writing a single line of code.



Cost-Effective and Predictable Pricing

Unlike traditional IGA vendors that lock you into complex, expensive contracts, ConductorOne offers transparent, usage-based pricing that scales with your needs. You don't pay for unused features, and there are no surprise costs hidden in professional services or implementation fees.

Why Do Customers Choose ConductorOne?

ConductorOne makes access management both secure and effortless.

Instead of adding more complexity, ConductorOne streamlines everything through intelligent automation and modern design.

- When a new engineer needs AWS access, they don't wait days—they get it in minutes through automated workflows.
- When someone leaves the company, their access isn't left lingering for weeks—it's revoked across every system.

What ConductorOne customers are saying:

→ *“What sets ConductorOne apart is their ability to balance security with accessibility. The platform incorporates multi-level configurable approval policies to ensure the right people make access decisions based on the resource itself.”* — Anthony S. ([Read full review](#)).

→ *“The biggest headache we had before ConductorOne was getting accurate data from our in-scope applications and ensuring the right procedures were followed for approving/denying access. We found with ConductorOne that setting up our integrations and approval policies was quick and gave us the configurability we needed to run campaigns.”* — ([Read full review](#)).

 [Read Case Study](#) → [How RRCU Cut Risk With Automated User Access Reviews and Jit Access](#)

2. SailPoint

SailPoint is an IGA platform that helps organizations control and protect user access across their IT systems. It automates the management of who can access what resources, ensuring access is granted appropriately and timely.

In terms of integration, SailPoint is compatible with SaaS, cloud, and on-premises systems, providing seamless governance in hybrid environments. There's also advanced analytic tools to help spot unusual access patterns and potential security risks before they become problems.

Additionally, SailPoint offers two core features; *Predictive Identity*, which uses AI to automatically adjust access policies based — and *Access Modelling*, which helps build and maintain least-privilege access frameworks.

Advantages

- Sailpoint offers advanced automation of access reviews and policy enforcement, making security management significantly more streamlined [\[*\]](#).
- The platform's deep backend accessibility gives users the ability to read and customize the backend code through Java decompiler for creating custom logic and events [\[*\]](#).
- Offers complete backend control, allowing for custom workflow modifications, with an easy learning curve [\[*\]](#).

Disadvantages

- SailPoint's setup and customization process can be complex — especially for new users, requiring expertise to configure it effectively [\[*\]](#).
- The recent decommissioning of the accelerator pack disappointed some users, as it previously streamlined configurations for lifecycle management events [\[*\]](#).
- SailPoint's large size leads to occasional unexpected behavior and cache issues, requiring additional effort to troubleshoot and resolve [\[*\]](#).

Pricing

- Not available. Please contact SailPoint for more information.

3. Saviynt

Saviynt is an all-in-one platform that manages and secures user access across organizations. It combines identity governance, privileged access management (PAM), and application access control in a single system that works across cloud and on-site systems.

The platform features *Identity-First Zero Trust*, which checks every access request against security policies in real-time. Same as its *Access Risk Exchange*, which continuously evaluates risk by monitoring user behavior and system vulnerabilities.

Advantages

- Offers numerous out-of-the-box connectors for system integration and highly useful APIs for custom UI experiences [\[*\]](#).
- Makes onboarding applications, managing dynamic attributes, and designing workflows seamless [\[*\]](#).

Disadvantages

- Lacks SSO capabilities for integrated applications and flexible MFA enrollment options [\[*\]](#).
- Despite the multi-tenant model, updates require extensive customer testing, often breaking existing functionalities, making the upgrade process difficult [\[*\]](#).
- Poor user experience particularly with the platform's user interface. For example, the small "View Detail" icon in the *Entitlement tab* is hard to locate [\[*\]](#).

Pricing

- Not available. Please contact Saviynt for more information.

4. Omada

Omada's IGA solution combines identity lifecycle management, access governance, and compliance management in a user-friendly package.

Its process-driven approach and strong focus on compliance, particularly with regulations like GDPR, make it a good fit for organizations seeking a streamlined and compliant IGA solution.

What makes Omada quite different is its *IdentityPROCESS+* framework, which applies proven best practices from years of industry experience. The platform offers detailed role management tools and *Smart Connectors* that easily integrate with existing business applications.

Advantages

- The *Assignment Policy* system offers several criteria for assigning access. It also comes with a robust survey system for GDPR-related tasks and a self-service flow with multiple approvers [*].
- Helps in automating account creation, handling SoD violations, managing technical identities centrally, and executing emergency lockouts [*].
- The clean interface, simple controls, and quick user permission editing make the platform easy and efficient to use [*].

Disadvantages

- Troubleshooting errors can be overly complex, with limitations around editing certain objects, such as updating usernames linked to display names, leading to outdated data [*].
- Lack of safety measures for HR data and no copy function for identity views [*].
- The survey function can overwhelm managers with attestation questions [*].

Pricing

- Not available. Please contact Omada for more information.

5. Microsoft Entra

Microsoft Entra is a comprehensive suite of IAM solutions designed to secure digital identities across an organization.

As part of Microsoft's ongoing commitment to identity security, Entra provides organizations with the tools (using *Workload Identities*) to authenticate, manage, and protect access to resources, applications, and environments. This ensures automated systems and IoT devices are authenticated and authorized, reducing potential attack vectors.

There's also '*Conditional Access Policies*' – that enables organizations to implement dynamic, context-aware access rules. These policies take into account factors such as user location, device health, and risk signals to grant or deny access, ensuring adaptive security measures without compromising user experience.

Advantages

- It's a reliable platform for *Spring Boot* development, offering smooth integration, comprehensive documentation, and a supportive community, making it an excellent choice for developers [*].
- The single sign-on feature simplifies user access by enabling login across multiple applications with one set of credentials [*].
- Its integration with Office 365 makes the platform highly effective for managing accounts and monitoring activity in environments that heavily rely on Microsoft's ecosystem [*].

Disadvantages

- The setup and configuration process is complex and challenging for organizations without a dedicated IT team, consuming significant time and effort [*].
- Some advanced features require paid subscriptions, increasing costs for larger organizations, and its integration with non-Microsoft applications can be complex and time-intensive [*].
- Community support and resources for Spring Boot developers are limited, making it difficult to find specific security solutions or timely assistance during the development process [*].

Pricing

- **Microsoft Entra ID P1.** \$6 per user/month.
- **Microsoft Entra ID P2.** \$9 per user/month.
- **Microsoft Entra Suite.** \$12 per user/month.

6. Okta IGA

Okta IGA simply streamlines the governance of digital identities across an organization. As part of Okta's extensive identity platform, IGA focuses on automating identity lifecycle management, simplifying access provisioning, and enforcing compliance through comprehensive access controls and reporting.

The platform also delivers a modern, cloud-native approach to governance that eliminates traditional complexities while enhancing security and operational efficiency.

Similar to other IGA solutions, Okta offers '*Adaptive Access Policies*' that dynamically adjust permissions based on contextual signals like location and device security. There's also pre-built integrations with thousands of applications that ensures quick deployment and broad compatibility.

Advantages

- Simplifies access to multiple applications through single login and two-factor authentication [\[*\]](#).
- Integrations and automation capabilities make workflows easier and more efficient, streamlining daily tasks [\[*\]](#).
- Ensures secure access through robust authentication while being simple to navigate on both web and mobile platforms [\[*\]](#).

Disadvantages

- It's not easy to check passwords for apps with integrated logins, which could be streamlined [\[*\]](#).
- The pricing structure is steep for smaller companies, making it less accessible for businesses with limited budgets [\[*\]](#).
- Recent changes to the mobile app authentication process on iOS add extra steps, making it less convenient compared to the earlier pop-up confirmation method [\[*\]](#).

Pricing

- **Light.** \$9 per user/month up to 50 flows.
- **Medium.** \$10 per user/month up to 150 flows.
- **Unlimited.** \$11 per user/month for unlimited flows.

7. Opal Security

Opal Security follows a simple approach — simplify access management and reduce the risks associated with over-privileged accounts.

The platform focuses on providing just-in-time access provisioning, dynamic role management, and comprehensive visibility into access permissions.

Opal Security also blends access management into daily workflows and DevOps pipelines by integrating natively with key tools like Terraform, Slack, Jira, and PagerDuty.

For example, the integration with Terraform enables organizations to manage access policies programmatically. With this, teams can define, deploy, and enforce access permissions as code, ensuring consistent configurations across environments while reducing manual intervention.

Advantages

- Minimizes privilege risks across engineering teams, offering easy admin access when needed and effectively integrating with Kubernetes, IAM roles, breakglass, and on-call schedules [\[*\]](#).
- Offers an intuitive UI and customizable workflows, including Terraform IaC configurations [\[*\]](#).
- Supports onboarding different access patterns, like Okta groups, AWS IAM roles, and SSH access [\[*\]](#).

Disadvantages

- While excellent for developers, Opal can be challenging for non-technical users [\[*\]](#).
- Webhook functionality works well for non-SSO apps but adds overhead for custom functions, slowing the onboarding of new applications [\[*\]](#).
- Limited custom integrations, making it harder to fully leverage internal API platforms [\[*\]](#).

Pricing

- Not available. Please contact Opal for more information.

8. Lumos

Lumos is a modern SaaS access management platform that helps organizations track and control employee access to cloud applications. It gives companies real-time visibility into their system, automates access requests and approvals, and helps enforce least-privilege security principles.

In addition, Lumos connects with an organization's cloud applications to automatically discover and map all user permissions. It streamlines the access request process through an employee self-service portal, where users can request and managers can approve access based on roles and business needs.

Lumos also features intelligent access recommendations and automated workflows. The platform suggests appropriate access levels based on employee roles and department patterns, while also automating routine access reviews and cleanup of unused licenses.

Advantages

- Slack-based notifications and simple action buttons enable end users, managers, and admins to seamlessly fulfill their roles [\[*\]](#).
- Offers time-saving features like one-click offboarding, transferring Google Drive contents, and rerouting emails [\[*\]](#).
- Bridges the gap in role-based access management for startups, uncovering shadow apps, enhancing visibility into IT spending, and providing excellent support [\[*\]](#).

Disadvantages

- Interface can be confusing at times, making it unclear what access users already have [\[*\]](#).
- Some application integrations are not fully connected to the one-click offboarding process, requiring manual audits [\[*\]](#).
- Lumos has a steep learning curve, requiring intense effort to fully understand the software [\[*\]](#).

Pricing

- Not available. Please contact Lumos for more information.

9. Oracle Identity Governance

Oracle Identity Governance solution drives enterprise-wide identity security through intelligent automation and risk-aware access controls.

The platform combines *Identity Cloud Service* (IDCS) with AI-powered workflows to handle everything from basic user access to complex role management. This is also combined with the platform's *Connector Framework*, which integrates with thousands of applications, from legacy systems to modern cloud services.

Beyond standard identity management, Oracle also offers features like *Segregation of Duties (SoD) engine* and *Access Orchestration* to prevent conflicting access grants and automate complex provisioning workflows.

Advantages

- Features like SSO and forced password changes during reset scenarios enhance security, while the self-service portal empowers end users to manage their identities [*].
- The platform prioritizes user data security, offering stability even with large datasets and applications [*].
- Automated provisioning, integrates with Oracle and third-party systems, and ensures strong compliance features [*].

Disadvantages

- Customization options are limited and do not always meet specific requirements, forcing reliance on out-of-the-box functionalities [*].
- Workflow and notification systems are limited to sending only three reminders, which may not be sufficient for some use cases [*].
- The platform is complex to set up, has a steep learning curve, and its high costs, including implementation and maintenance, can be expensive for some organizations [*].

Pricing

- Oracle doesn't offer 'exact' pricing details of the plans. However, you can request a bill comparison to see if it's a fit for you.

10. One Identity Manager

One Identity Manager provides a unified governance framework that provides a single platform for managing identities, roles and access rights. It also supports deployment on both cloud and traditional systems, making it particularly effective for organizations with complex IT environments.

The platform's built-in 'Attestation' capabilities speed up access reviews by focusing attention on high-risk changes while fast-tracking low-risk renewals. For organizations dealing with complex compliance requirements, One Identity's compliance dashboard provides real-time visibility into potential access violations.

Advantages

- Offers customizable scripts for role-based access management, quick deactivation of users across multiple systems with one click, and an object browser tool to manage frozen processes [*].
- Provides a unified view of multiple identities and entitlements, simplifies removal processes, and integrates easily with Azure, LMS, and ERP systems [*].
- Features a clean interface, multiple integration tools, and intuitive options like field definitions, making RBAC setups straightforward [*].

Disadvantages

- The database password change process, limited to every 42 days without user control, is inconvenient [*].
- On-premise IDM upgrades can cause performance issues, impacting functionality [*].
- Switching between environments (e.g., production vs. test) is complicated, with slow loading times and poor navigation [*].

Pricing

- Not available. Please contact One Identity for more information.

11. IBM Security Verify Governance

IBM Security Verify Governance (ISVG) is a comprehensive IGA solution that enables organizations to manage user access, enforce compliance, and mitigate security risks in hybrid IT environments.

Tailored for enterprises handling complex identity requirements, ISVG combines automation, analytics, and intuitive governance tools to streamline identity lifecycle management and ensure compliance with regulatory standards.

The platform features a watson-powered analytics engine, which processes identity data to spot risks and automate routine access decisions. This enables it to automatically adjust security controls based on user behavior and risk levels.

Advantages

- The platform is easy to set up and supports role lifecycle management, policy customization, and user access reviews [\[*\]](#).
- Ensures secure and trouble-free logins to multiple applications, offering robust protection for sensitive business data while integrating well with IBM's suite of products [\[*\]](#).
- Integrates with other security and identity access management solutions, enabling a unified security ecosystem [\[*\]](#).

Disadvantages

- Maintenance and updates for the platform can increase the total cost of ownership and demand significant resources [\[*\]](#).
- Role analysis is overly simplistic, and access provisioning occasionally experiences errors, with some requests being missed [\[*\]](#).
- Custom connector development requires skilled engineers, which are harder to find for IBM products [\[*\]](#).

Pricing

- Not available. Please contact IBM for more information.

12. Ping Identity

Ping Identity, through its unified *PingOne Cloud Platform*, unifies authentication, authorization, and intelligence capabilities.

The platform's signature *DaVinci* orchestration engine streamlines identity workflows across cloud and on-premises environments, while *PingIntelligence* uses AI to detect and respond to suspicious access patterns.

All of this is strengthened by the *PingFederate*, which manages complex authentication scenarios and enables secure identity federation across enterprise boundaries. *PingDirectory* is another core feature as it provides a scalable user directory service that can handle billions of identities and their attributes.

Advantages

- Ping Identity's cloud-based development ensures high scalability to meet varying business needs [*].
- The multi-factor authentication (MFA) feature enhances application security, supporting advanced authentication methods like biometrics, scanning, and smart cards for secure and efficient logins [*].
- The platform is easy to use and configure, with a highly responsive support team assisting during and after setup [*].

Disadvantages

- Frequent login session terminations are a recurring issue, disrupting user experience [*].
- Advanced features and functionalities in the premium tier are costly, making it less accessible for some organizations [*].
- Custom policies for access management require technical expertise, adding complexity for less-experienced teams [*].
- Some interfaces, like PingAuthorize and PingDirectory, are overly complex and not user-friendly [*].
- Software releases sometimes include bugs, leaving customers to report issues post-deployment [*].

Pricing

- Not available. Please contact Ping Identity for more information.

ConductorOne – Simplify Access Control with Modern IGA



It's evident traditional IGA solutions aren't making identity governance easier or more secure. They promise automation but deliver complexity. They talk about efficiency but require months of implementation and training.

Here's where ConductorOne is different:

- **Implementation in Days, Not Months.** Get up and running quickly with no complicated setup required.
- **Intelligent Automation That Works.** Stop drowning in manual tasks. Our AI-powered workflows handle the heavy lifting.
- **Complete Visibility, Zero Complexity.** See who has access to what, and why – all from one intuitive dashboard.
- **Seamless Integration.** Works with your existing stack right out of the box. No custom coding needed.
- **Built for Humans.** So intuitive that your team will actually use it, not avoid it.

 [ConductorOne Overview](#)

Here's the thing: every day you spend wrestling with outdated IGA tools is a day you could be running smoother, safer, and more efficiently.

Companies like [Ramp](#) have already transformed their identity governance with ConductorOne – why not join them?

Tired of Complex IGA? *We get it* 🙌

[Switch to ConductorOne →](#)

FAQs

What is Identity Governance and Administration and How Does It Work?

Identity Governance and Administration (IGA) is a comprehensive framework that helps organizations manage digital identities, access rights, and compliance requirements across their IT environment.

It ensures that the right individuals have access to the right resources at the right times for the right reasons while maintaining compliance with regulatory and internal policies.

IGA focuses on two core aspects:

- **Identity Governance.** Enforcing policies and controls to ensure access is granted appropriately and monitored consistently.
- **Identity Administration.** Managing the lifecycle of user identities and access permissions, including provisioning, updating, and deprovisioning.

How Does IGA Work?

- **Managing User Access.** When someone joins the organization, IGA assigns them the appropriate access based on their role. If their role changes, their access is updated accordingly. When they leave, all access is revoked automatically to maintain security.
- **Controlling Access.** The system implements role-based access controls and conducts regular reviews to validate user permissions. Managers participate in these reviews to ensure employees only have access to resources they need for their current roles. Additionally, employees can request additional access through automated workflows that ensure proper approval.
- **Protecting Privileged Access.** Sensitive privileges are given extra protection, such as time-based access, stricter authentication, and monitoring, to [reduce risks of data breaches](#) or misuse.
- **Ensuring Compliance.** IGA keeps track of who accessed what and when, generating reports to help organizations stay compliant with regulations like GDPR or HIPAA.
- **Integrating with Systems.** It connects with all major systems and applications to enforce identity policies consistently across the organization.

In short, IGA works by automating identity and access management, protecting sensitive data, and ensuring compliance, all while keeping processes smooth and efficient.

What Are the Benefits of Using an IGA Solution?



Enhanced Security

IGA strengthens an organization's security posture by enforcing the principle of least privilege, ensuring users only have access to resources necessary for their roles.

It prevents unauthorized access through automated controls and quickly revokes access when employees leave, reducing the risk of security breaches from dormant accounts or excessive permissions.



Improved Operational Efficiency

By automating identity-related tasks and workflows, IGA significantly reduces the manual effort required for user provisioning, access requests, and reviews.

This automation accelerates access delivery, reduces IT support tickets, and allows IT teams to focus on more strategic initiatives rather than routine administrative tasks.



Regulatory Compliance

IGA helps organizations meet various compliance requirements by providing comprehensive audit trails, access certification processes, and detailed reporting capabilities.

It maintains documentation of who has access to what resources and why, making it easier to demonstrate compliance during audits and reducing the risk of non-compliance penalties.



Better User Experience

Employees benefit from faster access to required resources through self-service portals and automated provisioning.

This reduces waiting times and productivity losses while maintaining appropriate security controls. The streamlined process for requesting and receiving access helps maintain workforce productivity.



Reduced Operational Costs

Automation reduces the need for manual access management tasks, freeing up IT resources. It also minimizes costs related to security incidents caused by improper access.

How is IGA Different From Identity and Access Management (IAM)?

IAM primarily focuses on managing day-to-day user authentication and access. It handles immediate access needs like login processes, password management, and access enforcement.

IGA, on the other hand, provides broader governance and oversight of identity management. It answers questions like “who should have access to what” and “why do they have this access,” focusing on policy enforcement, compliance, and risk management.

Talk to our team.

Or take a [self-guided tour](#) to learn more!

Try ConductorOne now

Get a demo