

Identity Manager

Take the risk out of enterprise identity governance and administration



Overview

Traditional identity governance & administration (IGA) frameworks are expensive to build and time-consuming to implement and maintain. They are burdens on most IT departments as IT typically handles all user identity lifecycle management. To meet the varied IGA needs of different business units, IT often works with a siloed set of narrowly focused tools and security policies and relies on manual processes for enforcement. This leaves the environment vulnerable, increases risk and makes it difficult to meet SLAs.

You can increase security and productivity by giving users access to the data and applications they need to do their jobs—and nothing more.

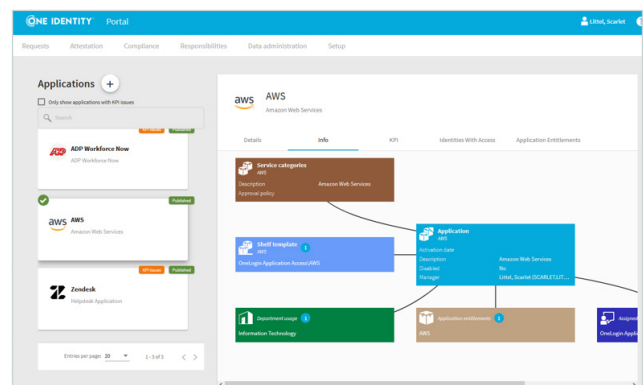
Identity Manager governs and secures your organization's data and users, meets uptime requirements, reduces risk and satisfies compliance by giving users access to data and applications they need - and only what they need - whether on-premises, hybrid or in the cloud. Now, identity security can be driven by business needs, not by IT capabilities. With Identity Manager, you can unify security policies and satisfy governance needs — today and long into the future.

You can do this while improving business agility today and in the future with a modular and scalable IGA solution.

Mitigate risk. Control access.
Govern identities. Secure data.

Benefits

- **Deploy** an identity-centric Zero Trust model
- **Govern** access to on-premises, cloud and hybrid resources from request through fulfillment for users and data
- **Reduce risk** by ensuring users have only the access they need to do their jobs
- **Satisfy audit and compliance** initiatives with attestation/recertification policies
- **Put access decisions** where they belong – in the hands of the business
- **Build** on existing investments and infrastructure and grow from there



Application Governance streamlines application onboarding and visibility

Now, identity governance and administration (IGA) can be driven by business needs.

Features

Identity Lifecycle

Identity management software that secures user access and automates enterprise provisioning to any target on-premises or in the cloud.

SAP Certified

Provide certified deep-SAP-integration with fine-grained capabilities to enhance existing SAP security models — and connect accounts under governance.

Risk Reducer

Make better security decisions by combining security information and policies from multiple sources to reduce exposure and eliminate information silos.

Cloud

Extend investment in identity governance beyond on-premises applications to hybrid and SaaS applications.

Governance

Single framework for governance for visibility to who has access to data and applications, when that access was granted and why. Provide auditors with detailed, real-time governance reports that include information about what resources are in your environment, who has access to them and when and why that access was granted and terminated.

Access Done Right

Enhance security by providing employees, contractors, partners, customers, students, alumni, constituents and patients with only the access they absolutely need - nothing more and nothing less.

Compliance Reporting

Satisfy compliance regulations with user- and privileged-access reporting.

Data Governance

Get control and visibility of your data.

Self-Service Access Portal

Enable the business to save time and help themselves. Reduces IT effort via a customizable

online intuitive “shopping cart” portal. This enables users to request access to security assets such as physical assets, groups and distribution lists and control access rights and permissions for their entire identity lifecycle with predefined approval processes and workflows.

Privileged Access Governance

Close the gap between privileged access and standard user identities across the enterprise.

Attestation

Empower line of business personnel to approve or deny user and group access and entitlements. Display the status of group and distribution list in a clear dashboard view.

Integrations and Connectors

Extend identity governance capabilities to the cloud and reduce cloud application onboarding time.

Application Governance

Streamline application-access decisions and enable line-of-business managers to make decisions without IT input.

Password Reset

Reset user-account passwords and set user-policy preferences that mirror your organization's password rules and requirements. You can institute multiple and granular password policies that depend on user roles.

About One Identity

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Our Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Identity and Access Management (IAM), Privileged Access Management (PAM) and Active Directory Management and Security (ADMS) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale – managing more than 500-million-plus identities for more than 11,000 organizations worldwide. For more information, visit www.oneidentity.com.