

OneLogin Delegated Administration



Enable Zero Trust, increase efficiency, and reduce the risk of high-privileged accounts

For organizations to adopt a Zero Trust framework, they must embrace the concept of “least privilege access”, which grants users the minimum level of access needed to perform their job. However, maintaining this baseline is challenging when organizations must balance the operational needs of the business and maintaining a strong security posture.

Not only is granting, removing, and enforcing privileges an operational headache, but continuously expanding user permissions increases the risk of a security breach. Today’s IT and Security teams need access to a highly flexible and customizable set of admin privileges that they can control and define, without incurring additional security risks.

OneLogin Delegated Administration

OneLogin Delegated Administration enables organizations to adopt the Zero Trust principle of least privilege access. By empowering admins to easily delegate access on a granular level, organizations can balance productivity requirements with the need to aggressively protect their organization against security threats.

How OneLogin Delegated Administration Works

Privileges are very simple records that grant users access to perform one or more operations on an object or collection of objects, such as an app, role, or user. Access can be granted for individual users or via roles. Each privilege consists of an effect, action, and scope to achieve the desired level of access for an admin user.

Key Benefits of OneLogin Delegated Administration

- **Customize and automate user privileges**

Grant users the ability to perform one or more administrative functions to a subset of users, roles, or applications. Define the specific actions admins are able to perform, like reset passwords for only a certain set of users or add users to a particular role.

- **Combat privileged account takeover**

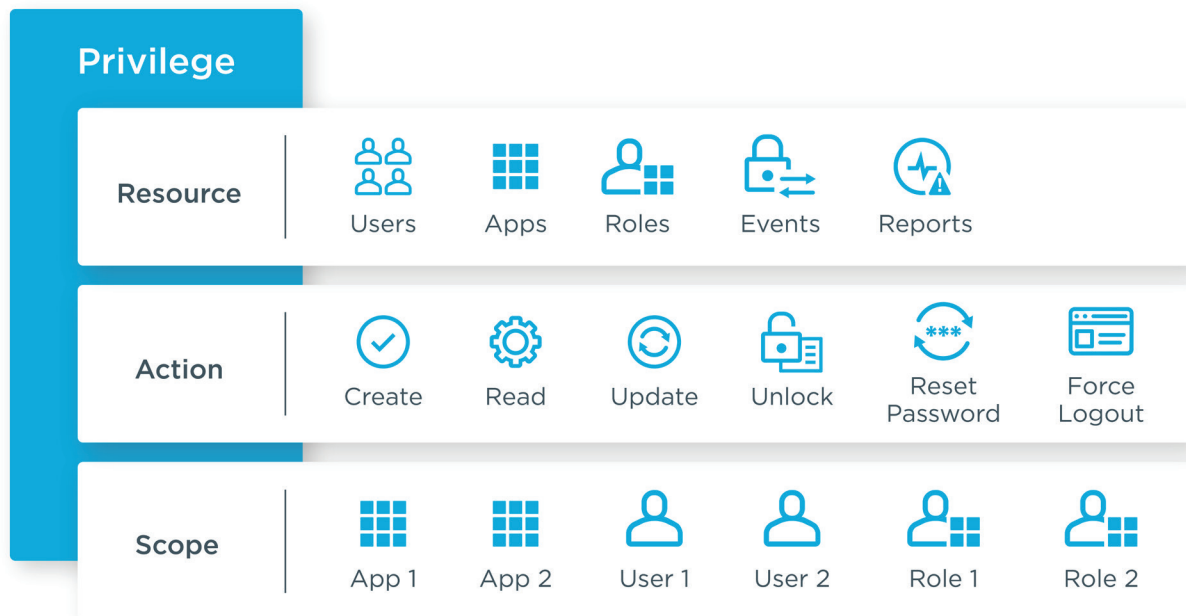
Reduce the threat and cost of account takeover for high-privileged users. With a granular list of privilege options, reduce the number of users or roles associated with a specific privilege to eliminate the risk of granting users more access than needed.

- **Enforce the principle of least privilege**

Only grant privileges for actions and users that are truly necessary and prevent unintended security consequences as a result of bloated privileges. Meet regulatory compliance requirements by providing granular access for auditing events and reports.

- **Alleviate access requests for Central IT**

Save time, reduce costs, and eliminate bottlenecks by allowing lower tier, less expensive support teams or departments to manage access for specific apps. Our robust privileges model allows you to flexibly combine different statements for a user or role in order to create a granular level of access.



FEATURE CAPABILITY	Description
Privileges Enforcement for Apps, Users, Roles, Events, and Reports	Grant users access to perform one or more operations on an object or collection of objects, including apps, users, roles, events, and reports
Programmatic Assignment of Privileges through Roles	Save time and reduce costs with automated role-based privilege assignment
Custom Granular Privileges	Create custom privilege sets for users with the ability to reduce permissions to specific users, roles, apps, events, and reports
API for Privileges CRUD Operations	Make changes via API to conveniently create, read, update, and delete privileges

Over 2,500 enterprise customers globally secure their applications with OneLogin



AIRBUS

pandora

Steelcase

STITCH FIX

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), Access Management (AM), 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.