ConductorOne

User Access Management: Everything You Need to Know

UAM involves the lifecycle management of user access rights, which includes provisioning, modifying, and de-provisioning permissions to ensure authorized users have the appropriate access to resources for the required period.

What is User Access Management?

User Access Management (UAM) is the process of managing and controlling individual users' access permissions to specific systems, applications, or data based on their roles and responsibilities.

UAM is a subset of IAM solution [1] that focuses specifically on controlling and monitoring individual users' access to resources. It ensures users have the right level of access to perform their roles without overstepping boundaries.

The main purpose of UAM is to address three key questions:

1. **Who is the user?** (User authentication and identity verification)
2. **What can they access?** (Access control)
3. **When and how can they access it?** (Contextual permissions)

[1] 💡 **What is IAM?**

Identity and Access Management (IAM) is a critical framework of policies, processes, and technologies designed to manage and secure digital identities within an organization. The aim here is to govern **who** has access to systems, data, and applications, as well as **what** they can do once access is granted.

For example, many organizations implement IAM through solutions like Microsoft Active Directory, which serves as a centralized identity provider for managing user access across the enterprise.

Related → 10 Best Identity and Access Management (IAM) Tools in 2024

Key Components of UAM

UAM relies on a structured approach to ensure secure and efficient access management.
The primary components include:

User Provisioning and De-Provisioning:

→ **Provisioning**. The process of granting users secure access to systems, applications, or data when they join the organization or change roles. Automated provisioning ensures immediate access to necessary resources.

→ **De-Provisioning**. The reverse process, where access is revoked when a user leaves the organization or no longer needs specific resources. Prompt de-provisioning prevents cybersecurity risks such as orphaned accounts, which can be exploited by malicious actors.

Related → The User Access Provisioning & Deprovisioning Process

Access Modification

Handles changes in a user's permissions as they transition between roles or projects.

For example, a promoted employee may require additional access while relinquishing permissions associated with their previous role.

Authentication and Authorization:

→ **Authentication** is the process of verifying a user's identity. Methods include:

- **Single-Factor Authentication (SFA)**. Basic credentials like username and password.
- **Multi-Factor Authentication (MFA)**. Combines two or more verification factors, such as a password and a fingerprint.
- **Passwordless Authentication**: Uses methods like biometrics or one-time codes sent to a trusted device (e.g., code sent to your authentication app)

→ **Authorization**: After authentication, authorization determines what actions a user can perform and what resources they can access. It works on predefined policies and models, such as:

- **Role-Based Access Control (RBAC)**. Assigns permissions based on roles.
- **Attribute-Based Access Control (ABAC)**. Dynamically grants permissions based on user attributes (e.g., job title, location, device type).

Authorization ensures the principle of least privilege (PoLP)—users get the minimum access required to perform their roles — and implements separation of duties (SoD) (preventing conflicts of interest in user activities).

Role and Policy Management

→ Establishes roles that group users with similar access needs.

→ Policies define the rules and conditions under which access is granted or denied.

Access Reviews and Auditing

→ Periodic reviews ensure that user permissions remain aligned with job responsibilities.

→ Auditing tracks all access activities to maintain compliance with regulations and detect anomalies.

Related → User Access Reviews: Process & Best Practices Checklist

How UAM Works: Practical Example

Let's say a company hires a contractor for a project that requires access to specific tools and data.

→ **Access Request**:

- First, the contractor submits a request through the organization's access management portal, specifying the needed systems and duration of access.

→ **Identity Verification**:

- The contractor's identity is verified via email or phone confirmation.
- MFA is enabled to enhance data security.

→ **Access Approval (Conditional)**:

- Based on the contractor's job description, access is granted using a predefined role template (e.g., "Project Contractor").
- Permissions are restricted to only project-related systems (*based on the principle of least privilege*).

→ **Access Provisioning**:

- The system automatically provisions access to relevant applications, such as file-sharing platforms and project management tools.
- Temporary access expiration is set based on the project timeline (*based on Just-in-time-Access (JIT)*).

→ **Continuous Monitoring**:

- The contractor's usage is monitored in real-time for compliance with organizational policies.
- Alerts are also set up for any unusual activity, such as attempts to access unauthorized files.

→ **Access Deprovisioning**:

- At the end of the project, the system automatically revokes the contractor's access based on the expiration date set during provisioning.
- An exit checklist ensures all credentials, tokens, and devices are returned or deactivated.

→ **Post-Access Audit**:

- Logs of the contractor's activities are reviewed to confirm no data breaches or policy violations occurred.
- Audit findings are documented for compliance purposes.

This process ensures the contractors only access necessary systems during their engagement, minimizing any form of cyber threat and maintaining the organization's security posture.

Benefits of a User Access Management System

Enhanced Security

The primary objective of UAM is to protect sensitive resources and minimize security risks. By restricting access to critical files, databases, and applications based on user roles and responsibilities, UAM shields sensitive information from unnecessary exposure.

For instance, in healthcare settings, UAM systems carefully control access to patient records, allowing only authorized medical personnel to view sensitive health information while maintaining strict HIPAA compliance.

There's also the case of '*privilege creep*' — when users accumulate excessive permissions over time — increasing security risks. UAM prevents this by conducting regular access reviews and implementing automated de-provisioning.

Recommended → Top 9 User Access Review (UAR) Software List for 2024

Improved Productivity and Efficiency

Modern UAM systems enhance business operations by automating time-consuming tasks like user provisioning and de-provisioning. Instead of relying on manual processes to grant or revoke access, UAM systems use predefined workflows to ensure users have the necessary permissions from day one.

This is particularly important for organizations with high employee turnover or frequent role changes as automation accelerates onboarding and offboarding processes.

Another aspect is with self-service portals. UAM enables them to request additional access or reset passwords without involving IT support. This reduces help desk workloads and improves user satisfaction.

Ensuring Compliance with Regulations

Businesses handling user data are in a heavily regulated environment — and for the right reasons.

Back in 2019, Meta announced they accidentally stored hundreds' of millions of its users' passwords in 'plain text'. Following a five-year investigation by the Irish Data Protection Commission (DPC), Meta was found to have violated the EU's GDPR policy, leading to a €91 million ($101 million) fine [*].

On the flip side, organizations can avoid facing fines and penalties by using UAM to simplify compliance. This helps you maintain a centralized log of all access activities, including who accessed what and when.

These logs provide visibility into access patterns and serve as evidence during audits, ensuring that organizations can demonstrate their commitment to regulatory requirements.

For example, during a GDPR audit, a company can use UAM-generated reports to prove that only authorized personnel accessed customer data.

Cost Savings

Security breaches are expensive. First, you have to pay the attacker if you've been attacked with ransomware. Next you have to incur the cost of fixing your security infrastructure, several legal actions, fines, penalties, — and worse, reputational damage.

Meanwhile, deploying UAM systems prevents these costly scenarios through proactive protection methods.

Consider these:

→ Reduced IT support costs through self-service capabilities

→ Lower risk of costly data breaches and associated penalties

→ Decreased administrative overhead for access management

→ Minimized downtime from security incidents

Additionally, UAM systems optimize software license usage by tracking inactive user accounts and reallocating licenses to active users. This ensures organizations only pay for what they need.

Better User Experience

Balancing security with user convenience is what defines a well-designed UAM system. Features like Single Sign-On (SSO) and self-service portals simplify the user experience by reducing the number of credentials users need to remember and enabling them to manage access independently.

For remote workers, adaptive access management ensures that users can access the resources they need without unnecessary delays. By providing seamless access to trusted devices and requiring additional verification for unknown ones, UAM maintains a balance between security and user satisfaction.

Adaptability and Scalability

As businesses expand and adopt new technologies, UAM adapts to accommodate additional users, roles, and resources.

This scalability is particularly valuable for organizations transitioning to hybrid or multi-cloud environments, where access management can become complex without centralized control.

Integration capabilities further enhance adaptability. UAM systems can connect with legacy applications, SaaS platforms, modern cloud services, and even external partner systems, providing a unified view of access management across the enterprise.

Common Challenges With User Access Management (and How to Solve Them)

Balancing Security Needs With User Convenience

Balancing strong security measures with seamless usability is a persistent issue for organizations.

One one hand, the **overly restrictive** access policies, while effective at preventing unauthorized access, can frustrate employees who face delays in obtaining the permissions they need. This frustration often leads to risky workarounds, such as sharing credentials or storing sensitive passwords insecurely, further compromising security.

On the other hand, **overly lenient** access policies can result in users having excessive permissions, creating vulnerabilities that increase the risk of insider threats, privilege creep, and unauthorized data access.

For organizations with remote workforces or dynamic operational needs, this challenge becomes even worse. Employees need access to tools and systems across various devices and locations, yet granting unrestricted access exposes the organization to significant risks.

> 💡 **Solution →** Adopt risk-based access controls that dynamically adjust security requirements based on contextual factors like user location, device, or behavior.
> For example, access may be seamless for users on corporate networks but require additional authentication for remote or unusual login attempts.
> Combine this with **Just-in-Time (JIT)** provisioning to provide temporary access for specific tasks, automatically revoking permissions once the task is complete.

Credential Overload Issues

Managing multiple, complex passwords across various systems often leads to password fatigue among users.

As organizations expand their digital ecosystems, employees are required to remember and maintain credentials for numerous platforms, tools, and applications.

This results in users adopting risky behaviors like reusing passwords, writing them down, or choosing weak, easy-to-remember passwords. Practices like these significantly increase the risk of credential theft, unauthorized access, and data breaches.

Additionally, frequent password resets or account lockouts can frustrate users and burden IT support teams with a high volume of password-related queries.

> 💡 **Solution →** Implement Single Sign-On (SSO) solutions that enable users to access multiple applications with a single set of credentials, reducing the need to remember numerous passwords.
>
> Complement this with MFA to enhance security without overburdening users. Also encourage using password managers to securely store and generate strong, unique passwords for non-SSO-enabled systems.

Data Oversight Complexities

Integrating UAM systems with data governance initiatives is often complex. This is because organizations must ensure that access rights are aligned with data classification policies and comply with privacy regulations like GDPR and HIPAA.

Without proper integration, access controls may become inconsistent, leading to sensitive data being overexposed or underutilized.

Additionally, siloed systems make it difficult to enforce unified access policies, complicate audits, and hinder effective tracking of data usage across the organization.

> 💡 **Solution →** Establish clear data governance policies that classify data based on sensitivity and define corresponding access controls.
> Use data access governance tools to enforce these policies automatically and ensure that permissions are consistently applied across all systems.
> Integrate UAM with existing governance frameworks to provide centralized visibility into data access and activity.

Related → 11 Best Access Governance Software for Identity Management in 2024 [+User Feedback]

Securing Access for Remote and Hybrid Workforces

The shift to remote work has introduced unique access management challenges. Employees often connect to organizational systems from different locations, devices, and networks, many of which may not meet enterprise security standards.

This increases the risk of unauthorized access, data breaches, and compromised endpoints. Traditional access controls designed for on-premises environments struggle to handle the dynamic and decentralized nature of remote work, creating vulnerabilities in security policies and disrupting workflows.

💡 **Solution →** Implement *Zero Trust Network Access (ZTNA)*, which requires continuous verification of both user identity and device health before granting access.
Pair this with endpoint security solutions that enforce device-level controls, such as ensuring antivirus protection and encryption.
Secure remote access tools, such as Virtual Private Networks (VPNs) or secure application gateways, can further protect communication channels.

Managing Excessive Privileges

Over time, users often accumulate excessive permissions as their roles or responsibilities change.

These unused or unnecessary privileges increase the organization's attack surface and pose significant security risks.

Similarly, orphaned accounts, which are accounts left active after an employee leaves the organization or changes roles, create another vulnerability.

Such accounts can be exploited by malicious actors, leading to unauthorized access or data breaches. Both issues often arise due to inadequate monitoring and inconsistent de-provisioning practices.

💡 **Solution →** Conduct regular access reviews to ensure that user permissions align with their current roles and responsibilities.

You can do this by granting users only the minimum access required to perform their tasks.

Also, automate de-provisioning processes to immediately revoke access for departing employees or redundant accounts, ensuring that no orphaned accounts remain.

How to Set Up Access Management Systems in 4 Easy Steps

Step 1: Define and Configure Access Levels

The foundation of an effective user access management system lies in clearly defining different levels of access. These determine what users can do within your systems and ensure permissions align with organizational needs.

Here's how to set it up:

→ Catalog all resources (files, databases, applications, and systems) within your organization.

→ Classify these resources based on sensitivity (e.g., public, confidential, highly confidential) and criticality to operations.

→ Define granular access levels, such as:

- **Read-Only**: Users can view data but cannot modify it.
- **Read/Write**: Users can both view and edit data but cannot delete it.
- **Full Control**: Users have complete control, including the ability to delete, share, or configure settings.

→ Align these levels with the organization's risk tolerance and data governance policies.

→ Implement compliance requirements like GDPR or HIPAA into your access levels to ensure sensitive data is adequately protected.

💡 **Pro Tip →** Run scenarios to ensure access levels provide the right permissions without overexposing sensitive data.
For example, ensure a marketing intern with "*Read-Only*" access cannot edit customer data but can view analytics reports.

Step 2: Establish User Roles and Role Hierarchies

After defining access levels, create user roles to streamline the assignment of permissions.

Here's how to set it up:

→ List all job functions within your organization, from entry-level staff to senior executives.

→ Group roles by department or function to ensure permissions reflect responsibilities (e.g., HR Manager, IT Administrator, Sales Representative).

Define role-based permissions. For example:

- **HR Manager**: Full control over HR software but read-only access to finance data.
- **IT Administrator**: Full control over network configurations but no access to marketing tools.

→ Avoid overlapping permissions to prevent excessive privileges.

→ Create a structure where higher-level roles inherit permissions from lower-level roles. For example:

- A "*Department Head*" role might inherit all permissions from a "*Team Lead*" role, plus additional privileges like approving access requests.

→ Maintain a detailed document listing each role, its associated permissions, and the reasoning behind its configuration for reference during audits or updates.

Step 3: Automate User Access Management Processes

Provisioning

→ Automate account creation and permission assignment when new users are onboarded. Integrate with HR systems to trigger provisioning as soon as employees are hired.

- **Example**: An employee hired as a "*Finance Analyst*" is automatically granted access to budgeting software, payroll tools, and financial reports upon onboarding.

De-Provisioning

→ Implement automated workflows to revoke access immediately when users leave the organization or change roles.

- **Example**: When an IT contractor's engagement ends, their administrative privileges are revoked, and their account is disabled.

Access Requests

→ Use self-service portals for access requests. Automate approval workflows to route requests to managers or system owners for quick decision-making.

- **Example**: A content writer requests access to a new analytics tool, and the system routes the request to their manager for approval.

Regular Access Reviews

→ Automate periodic reviews where managers validate permissions for their team members.

- **Example**: Every quarter, department heads receive automated reminders to review access for their teams and revoke unnecessary permissions.

Password Management

→ Enable self-service password reset capabilities to reduce help desk workload.

→ Enforce strong password policies with automatic reminders for expiration and updates.

Step 4: Monitor Access and Ensure Compliance

→ Implement tools to track user activity, including login times, accessed resources, and unusual behavior.

- For example, set an alert when a user attempts to access files outside their permissions or logs in from an unusual location.

→ Maintain detailed logs of all access-related activities to ensure accountability. These logs should include:

- Who accessed the resource.
- What action they performed.
- When the access occurred.
- Where the request originated from (e.g., IP address or device).

→ Generate reports for regulatory audits, showing how access aligns with policies and standards.

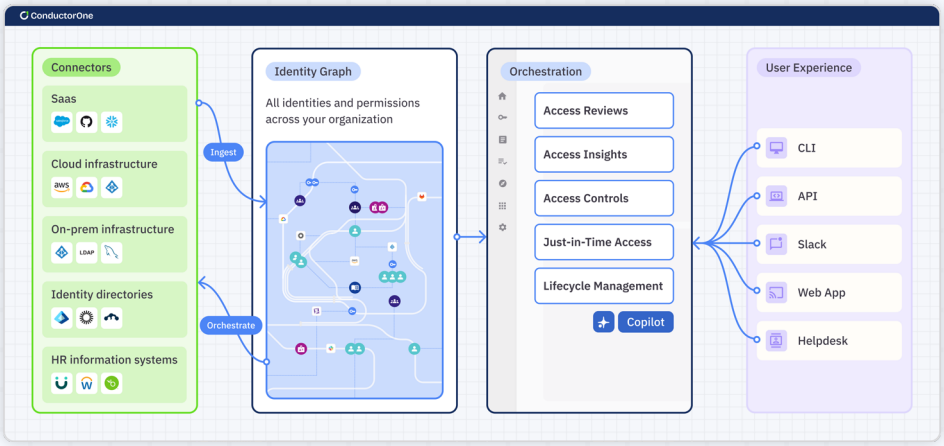
- For example, for GDPR compliance, demonstrate that only authorized employees accessed customer data during a specific time frame.

→ Use AI-powered tools to identify suspicious activity, such as a user downloading large amounts of data or accessing resources at unusual hours.

→ Regularly update access policies to reflect changes in technology, regulations, or business operations.

→ Conduct periodic training for employees to ensure they understand access policies, best practices, and their role in maintaining security.

Rethink User Access Management: From Chaos to Control with ConductorOne

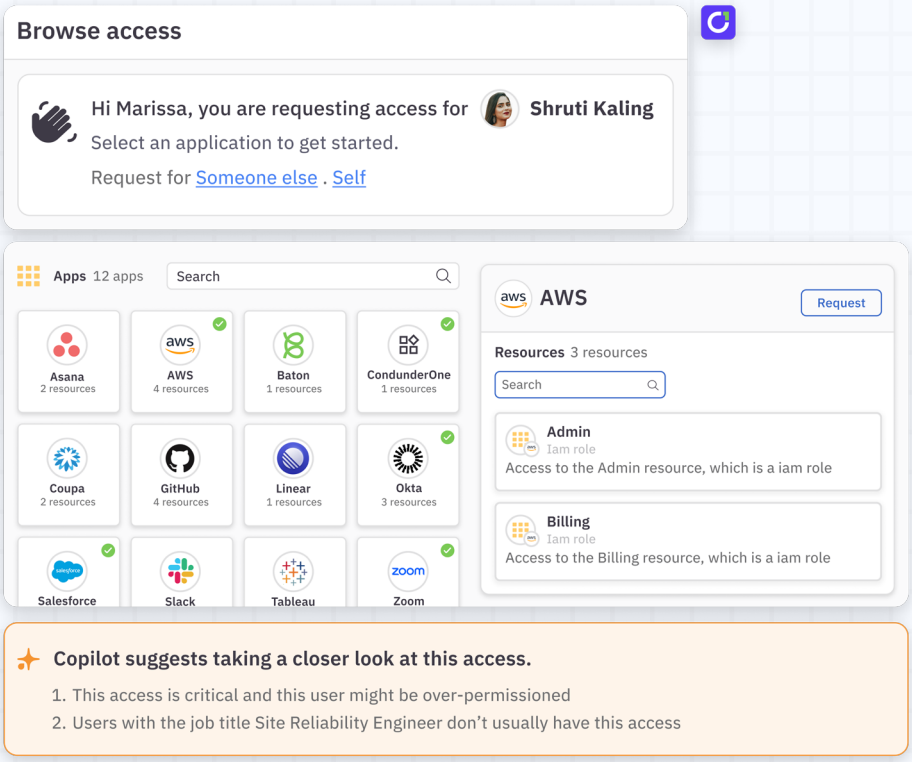


The old ways of managing user access have become a liability. Scattered spreadsheets, endless email chains, and manual approval processes aren't just inefficient—they're putting your organization at risk.

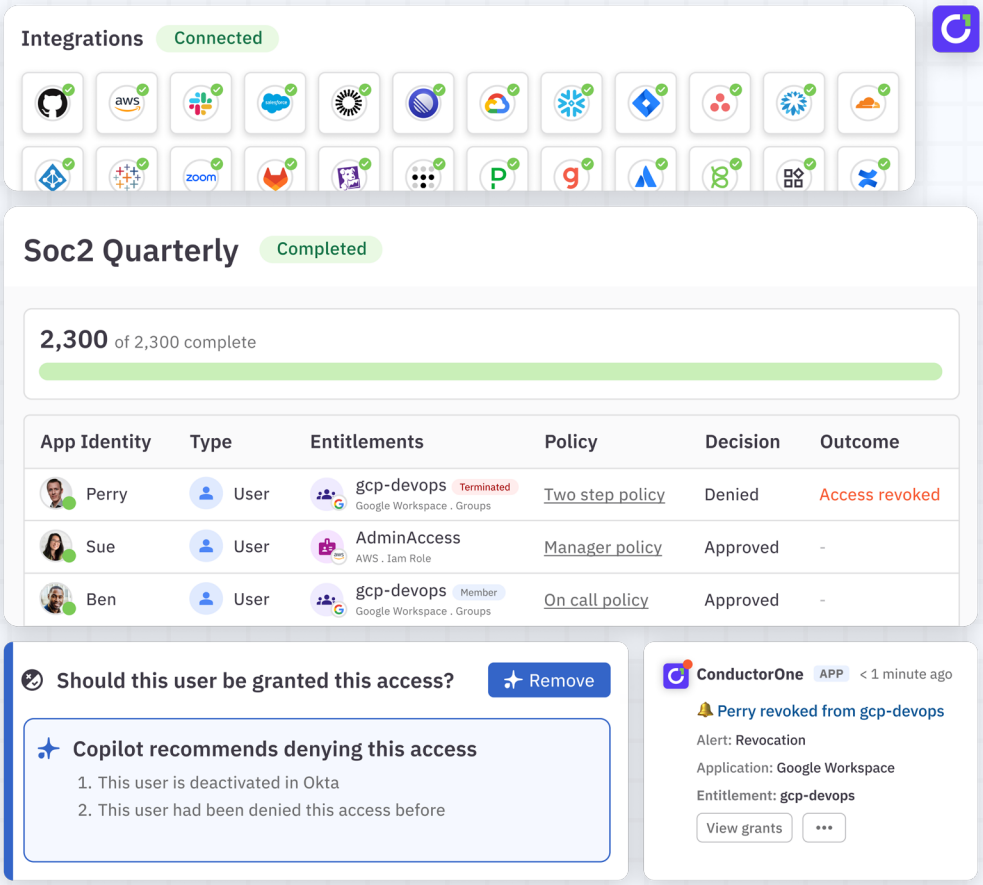
→ Every delayed access request isn't just a frustration; it's lost productivity.

→ Every overlooked permission isn't just an oversight; it's a potential security breach waiting to happen.

ConductorOne transforms this complexity into clarity. By automating the right processes at the right time, it ensures your team gets the access they need when they need it, while maintaining the security standards your organization demands.

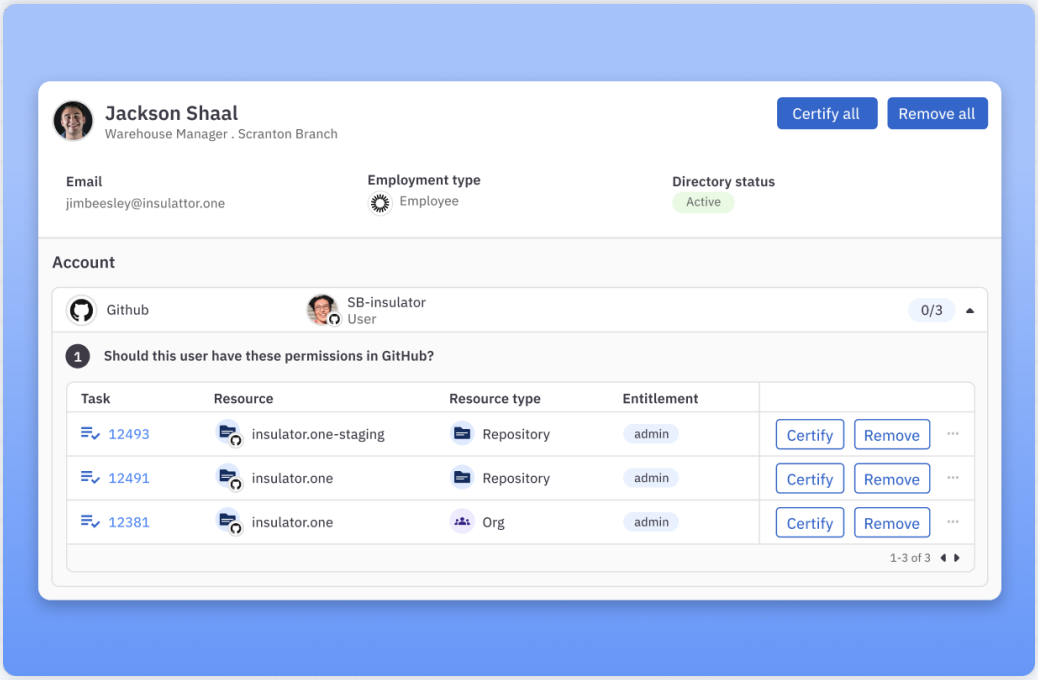


No more Monday morning access request pileups. No more frantic searches through email threads to track down approvals. Just smooth, secure, and auditable access management that scales with your organization.



What makes ConductorOne different is its understanding that access management isn't just about control—it's about enablement.

While other solutions focus solely on restrictions, ConductorOne learns, adapts, and streamlines approvals.



Access reviews that once took weeks now take hours. Approvals that once required multiple follow-ups now flow smoothly through intelligent workflows. And security teams finally get the comprehensive visibility they need without becoming a bottleneck.

🔗 Automate Access Reviews in Minutes → **See How**

Learn more about our identity security platform for modern workforces

Get a demo

ConductorOne