ConductorOne

Understanding Identity and Access Provisioning Lifecycle

The Access Provisioning Lifecycle is a crucial part of **Identity and Access Management (IAM)**. It's the process of managing user access to an organization's resources, like applications, systems, and data, throughout their entire "lifecycle" within the organization.

Why is access provisioning important?

Access provisioning is a critical process for any organization that wants to maintain a secure and efficient IT environment. Here's why it's so important:

Enhance security

- → **Protecting sensitive data**: Access provisioning ensures that only authorized individuals have access to sensitive information, systems, and applications. This helps prevent data breaches, unauthorized access, and other security incidents.
- → **Minimizing insider threats**: By controlling and monitoring access, organizations can reduce the risk of insider threats, whether intentional or accidental.
- → **Enforcing least privilege**: Access provisioning allows organizations to implement the principle of least privilege, granting users only the minimum necessary access to perform their job duties. This limits the potential damage in case of a security breach.

Improve efficiency

- → **Streamlining processes**: Automated access provisioning speeds up the process of granting and revoking access, reduces manual effort, and saves time for IT teams.
- → **Improving productivity**: When users have timely access to the resources they need, they can be more productive and efficient in their work.
- → **Reducing IT support costs**: Automated provisioning and self-service features can reduce the number of help desk requests related to access issues.

Ensure compliance

- → **Meeting regulatory requirements**: Access provisioning helps organizations comply with various data privacy and security requirements, such as GDPR, HIPAA, and SOX.
- → **Providing audit trails**: Detailed logs of access provisioning activities provide evidence of compliance and support audits.
- → **Enforcing access policies**: Access provisioning helps organizations define and enforce consistent access policies across all systems and applications.

Support business agility

- → **Supporting business growth**: Good access provisioning helps companies adapt to changing business needs, such as new hires, role changes, and organizational restructuring.
- → **Facilitating collaboration**: Proper access provisioning enables seamless collaboration between employees, partners, and contractors.
- → **Improving user experience**: A streamlined access provisioning process provides a positive user experience, especially for new employees and external users.

Who is responsible for access provisioning?

IT Department

The IT department usually plays the central role in access provisioning. They are responsible for:

- → Managing user accounts and access rights: Creating, modifying, and deleting user accounts in various systems and applications.
- → Implementing and maintaining access control systems: Setting up and configuring tools and technologies that govern user access.
- → Enforcing security policies: Ensuring that access provisioning aligns with organizational security policies and regulatory requirements.
- → Troubleshooting access issues: Resolving any problems users encounter with accessing resources.

Security team

The security team often has an oversight role, ensuring that access provisioning processes are secure and compliant. They may be responsible for:

- → **Defining access control policies**: Establishing rules and guidelines for granting and revoking access.
- → **Conducting security audits**: Regularly reviewing access rights and identifying potential vulnerabilities.
- → **Monitoring user activity**: Tracking user actions to detect suspicious behavior and prevent security breaches.

Human resources (HR)

- → **Initiating access requests**: HR often initiates access requests for new users based on their roles and responsibilities. They provide information about the employee's job title, department, and required access levels.
- → **Managing employee lifecycle**: HR plays a key role in triggering access provisioning and deprovisioning events based on employee onboarding, role changes, and terminations.

Business unit managers

- → **Approving access requests**: Managers often have the authority to approve access requests for their team members. They ensure that employees have the necessary access to perform their job duties. Managers may also sometimes request access on behalf of their team members.
- → **Reviewing access rights**: Managers may participate in periodic access reviews to confirm that their team members have appropriate access levels.

End Users

- → **Requesting access**: End users can request access to specific resources they need for their work.
- → **Managing their accounts**: Users may have some responsibilities for managing their own accounts, such as resetting passwords or updating personal information.

Effective access provisioning requires collaboration between these different stakeholders. Clear communication and well-defined processes are essential to ensure that access is granted efficiently and securely.

Many organizations use identity governance tools to streamline access provisioning, helping to:

- → Automate user provisioning and deprovisioning
- → Enforce access policies
- → Conduct access reviews
- → Monitor user activity

Risks associated with inadequate access provisioning control

Access creep

Access creep happens gradually over time. As employees change roles, take on new responsibilities, or move between departments, they often retain access to systems and data they no longer need. This accumulation of unnecessary permissions can create security vulnerabilities.

Why it's dangerous:

- → **Unauthorized access to sensitive data**: Employees may have access to confidential information that is not relevant to their current role.
- → **Increased risk of insider threats**: Disgruntled employees or malicious actors can exploit excessive access to steal data, sabotage systems, or disrupt operations.
- → **Compliance violations**: Organizations may fail to comply with data privacy regulations if they cannot demonstrate that access is limited to authorized personnel.

Privilege abuse

Privilege abuse occurs when users with elevated access rights misuse their privileges for personal gain, malicious intent, or even unintentionally cause harm. This could involve accessing confidential data, modifying system settings, or installing unauthorized software.

Why it's dangerous:

- → **Data breaches**: Sensitive information can be stolen or leaked, leading to financial losses, reputational damage, and legal repercussions.
- → **System disruptions**: Critical systems can be compromised, causing downtime, service interruptions, and operational disruptions.
- → **Fraud and financial loss**: Users with excessive privileges may be able to manipulate financial data or commit fraud.

Third-party data breaches

Third-party data breaches occur when vendors, partners, or other external entities with access to an organization's systems or data experience a security breach. This can expose sensitive information and compromise the organization's cybersecurity posture.

Why it's dangerous:

- → **Supply chain attacks**: Attackers may target third parties with weaker security controls to gain access to the organization's systems.
- → **Data leakage**: Sensitive information shared with third parties may be exposed in a breach, leading to privacy violations and reputational damage.
- → **Compliance issues**: Organizations may be held liable for data breaches involving third parties if they fail to implement adequate security controls.

Key stages in the access provisioning lifecycle

The access provisioning lifecycle outlines the journey of a user's access to an organization's resources, from the initial request to the eventual revocation. Here's a breakdown of the key stages:

Access request

→ The process begins with a request for access. This can be triggered by a new employee needing access to start their job, an existing employee requiring new permissions for a project, or even an external user like a contractor needing temporary access.

→ The request can come from various sources, including the user themselves, their manager, an HR system, or even automatically based on predefined rules and roles.

Access review and approval

→ Once a request is made, it needs to be reviewed and approved by the appropriate authority. This could be a manager, an app owner, an IT administrator, or a security team, or the request could even be automatically approved, all depending on the organization's policies and the sensitivity of the resources requested.

→ This step is crucial to ensure that access is granted only to those who genuinely need it, adhering to the principle of least privilege and preventing unauthorized access.

Access provisioning

→ After approval, the actual granting of access takes place. This involves creating user accounts in relevant systems, assigning roles and permissions, and configuring access settings in applications and databases.

→ This stage can be complex, especially in organizations with diverse IT systems. Automation tools can streamline the process, reduce manual effort, and minimize human errors.

Monitoring and review

Access provisioning requires continuous monitoring and periodic reviews to ensure that:

→ **Access remains appropriate**: Users have the right level of access for their current roles and responsibilities, and haven't accumulated excessive permissions over time.

→ **Compliance is maintained**: Access rights adhere to security policies, industry standards, and regulatory requirements.

Access revocation and deprovisioning

→ When an employee leaves the organization, changes roles, or no longer needs access to specific resources, their access must be revoked promptly.

→ This involves disabling or deleting accounts, removing access permissions, and ensuring that ex-employees or those with changed roles cannot access sensitive data. Failing to deprovision properly can lead to significant security risks and compliance violations.

Three key best practices for managing user access

Access governance

Access governance is a structured framework for managing and controlling user access to an organization's resources. It involves establishing policies, procedures, and roles to ensure that access is granted appropriately, monitored effectively, and revoked when necessary.

Key components:

- → **Access request and approval processes**: Defining clear procedures for requesting, approving, and granting access.
- → **Role-based access control (RBAC)**: Assigning permissions based on user roles and responsibilities.
- → **Access certification**: Regularly reviewing and validating user access rights.
- → **Policy enforcement**: Ensuring that access provisioning adheres to organizational policies and regulatory requirements.

Access controls

Access controls are the technical measures used to enforce access governance policies. They regulate who can access what resources and what actions they can perform.

Examples:

- → **Authentication**: Verifying user identities through passwords, multi-factor authentication, or biometrics.
- → **Authorization**: Determining what resources and actions a user is allowed to access based on their roles and permissions.
- → **Network security**: Using firewalls, intrusion detection systems, and other tools to protect network resources from unauthorized access.
- → **Data encryption**: Protecting sensitive data by encrypting it both in transit and at rest.

Regular access reviews

Regular access reviews are a critical process for ensuring that user access remains appropriate and aligned with business needs. They involve periodically reviewing user permissions and revoking any unnecessary access.

Key steps:

- → **Identify users and their access rights**: Gather information about all users and their current access privileges.
- → **Review access against roles and responsibilities**: Determine if users have the appropriate level of access for their current roles.
- → **Revoke unnecessary access**: Remove any permissions that are no longer required.
- → **Document the review process**: Maintain records of the review process for audit and compliance purposes.

ConductorOne

How ConductorOne can help you streamline the access provisioning lifecycle

ConductorOne can significantly streamline the access provisioning lifecycle by automating key tasks, improving visibility, and enforcing stronger security controls. Here's how we help at each stage:

Access request

→ **Simplified request process**: ConductorOne provides a user-friendly interface for employees and managers to request access to applications and resources. This eliminates the need for manual forms or emails, making the process faster and more efficient.

→ **Automated role- and attribute-based requests**: Our platform can automatically suggest or prepopulate access requests based on the user's role or specific attributes, reducing errors and saving time.

Access Approval

→ **Streamlined approval workflows**: ConductorOne automates approval workflows, routing requests to the appropriate approvers based on highly customizable rules that can enable auto, conditional, and multistep approvals. This eliminates bottlenecks and ensures timely access granting.

→ **Delegated approvals**: Approval authority can easily be delegated to managers, app owners, or other designated individuals, improving efficiency and control.

Provisioning

→ **Automated account creation**: ConductorOne can automatically create user accounts in various applications and systems, eliminating manual processes and ensuring consistency.

→ **Just-in-time provisioning**: Automated time-bound access can be configured to grant access to resources only when needed, further minimizing the risk of unauthorized access.

→ **Zero-touch provisioning**: ConductorOne can automatically provision access without any human intervention, saving time and resources.

Reviewing and risk mitigation

→ **Centralized access visibility**: ConductorOne provides a single dashboard to view and manage user access across all applications, giving administrators a clear overview of permissions and entitlements.

→ **Automated access reviews**: The platform facilitates regular access reviews, allowing managers and security teams to easily identify and remove unnecessary permissions.

→ **Risk detection and remediation**: ConductorOne's security dashboard proactively alerts admins to potential risks like overprivileged and orphaned accounts. High-risk access is easily detected and can be remediated in a few clicks.

Deprovisioning

→ **Automated deprovisioning**: When an employee leaves or changes roles, ConductorOne can automatically revoke access to applications and systems, preventing security risks associated with stale accounts.

→ **Comprehensive deprovisioning**: It ensures that access is revoked across all connected applications, including both cloud-based and on-premises systems.

Why customers choose ConductorOne for access provisioning lifecycle management

ConductorOne helps organizations automate and orchestrate the full access provisioning lifecycle across every application and identity in their environment. Our customers see immediate business impact across the following areas:

Reduced manual effort

ramp

Ramp experienced a 95% reduction in IT effort to process tickets for access requests after implementation.

SYSTEM1

System1 reduced the time spent preparing user access reviews from weeks or months to under a day, all while reducing excessive privileges and unused licenses.

Improved accuracy

Automated, policy-based provisioning ensures access changes are applied consistently and correctly.

Teams gain complete visibility into access across systems, enabling precise and informed provisioning decisions.

Automation reduces reliance on spreadsheets and manual processes that often introduce errors.

Enhanced Security

Stronger controls and proactive risk detection help prevent unauthorized access and data breaches. Customers frequently identify and remove risky, unnecessary access that was previously undetected.

instacart

Instacart transitioned 100% of privileged access to policy-based just-in-time access.

RRCU

RRCU reduced its inherent risk assessment by $1 million, equating to a 2,000 percent ROI, from implementing ConductorOne.

Increased Efficiency

Streamlined workflows speed up access requests and revocations, improving responsiveness and agility.

ConductorOne

In ConductorOne, fully automated access requests can be completed in as little as 1 minute from submission to approval to provisioning.

DigitalOcean

DigitalOcean completed 1,200 access reviews across seven departments with 85 percent less effort and achieved a 100 percent on-time reviewer completion rate.

Improved Compliance

Automated workflows and robust audit trails help organizations meet regulatory requirements and reduce audit preparation time.

igsenergy

With ConductorOne, IGS Energy significantly improved their documentation and reporting for SOC 2 and ISO compliance.

Customers consistently meet internal and regulatory SLAs for access campaign completion.

To learn how ConductorOne can automate and streamline your access provisioning lifecycle, book a demo.

Try ConductorOne now

Get a demo