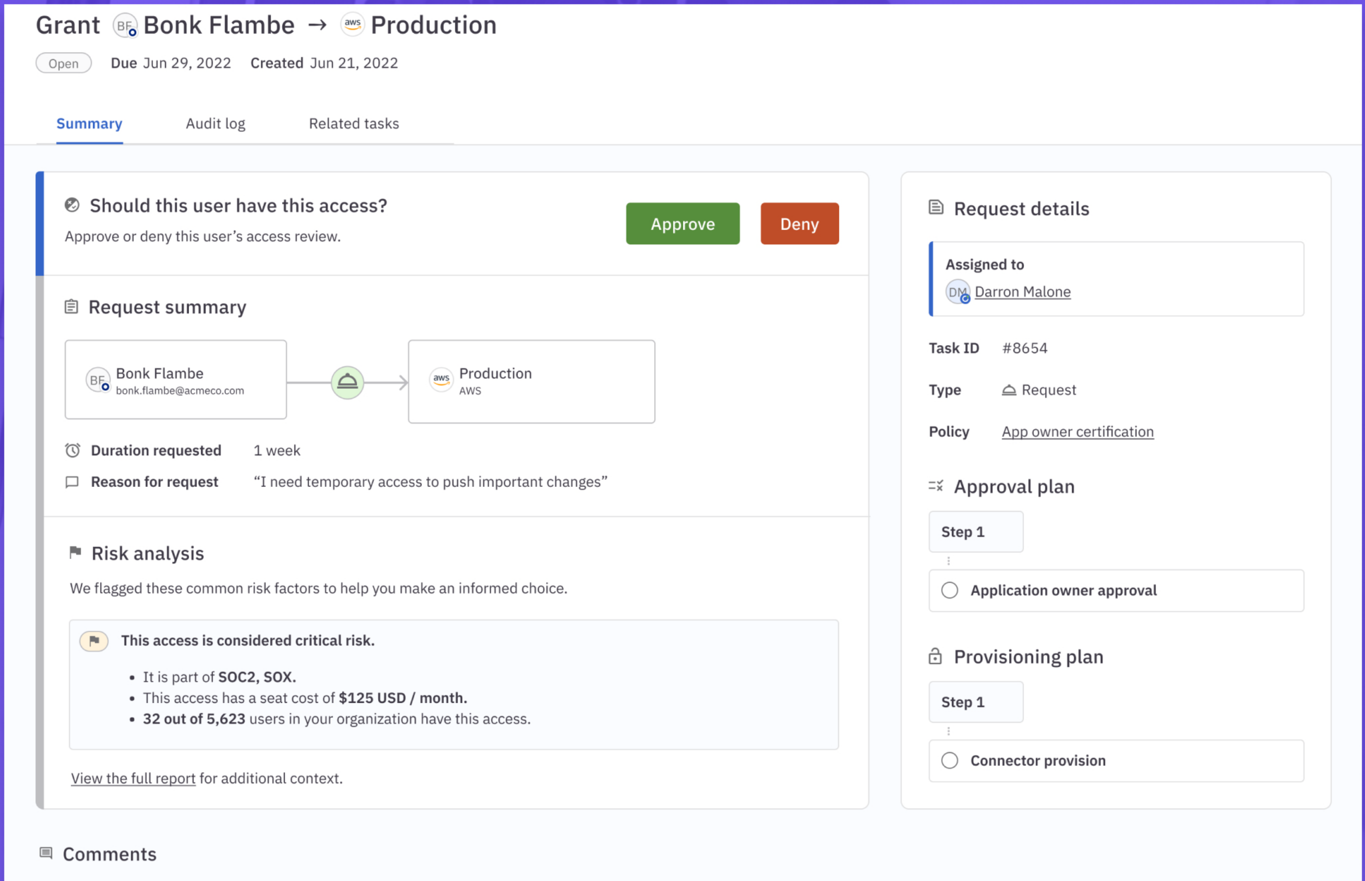
ConductorOne

The Principle of Least Privilege & Best Practices

GUIDE | July 2022



Grant BF Bonk Flambe → aws Production

Open **Due** Jun 29, 2022 **Created** Jun 21, 2022

Should this user have this access?

Approve or deny this user's access review.

Request summary

Bonk Flambe
bonk.flambe@acmeco.com → Production
AWS

Duration requested	1 week
Reason for request	"I need temporary access to push important changes"

Risk analysis

We flagged these common risk factors to help you make an informed choice.

This access is considered critical risk.

- It is part of **SOC2, SOX.**
- This access has a seat cost of **$125 USD / month.**
- **32 out of 5,623** users in your organization have this access.

View the full report for additional context.

Comments

Request details

Assigned to
DM Darron Malone

Task ID	#8654
Type	Request
Policy	App owner certification

Approval plan

Step 1

○ **Application owner approval**

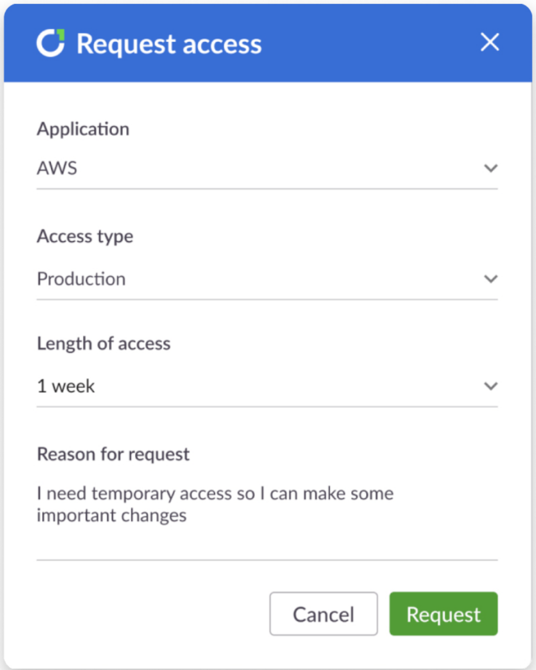
Provisioning plan

Step 1

○ **Connector provision**

Modern companies have unique identity security needs driven by high adoption of SaaS and IaaS applications, permissions sprawl, and decentralized admins for each application or infrastructure account.

In this white paper, you'll find a set of best practices for streamlining security and reducing the risk of compromise by implementing the principle of least privilege access.



Application
AWS

Access type
Production

Length of access
1 week

Reason for request
I need temporary access so I can make some important changes

What is the Principle of Least Privilege (POLP)?

The Principle of Least Privilege, one of the core elements of zero trust security, is defined as giving people access when they need it to complete a job, and for no longer than they need it. By enforcing least privilege access, you reduce the chances of account compromise by eliminating unused or unnecessary accounts, and reduce the potential impact of a compromised account or insider threat.

It's a simple principle, but in practice, understanding and achieving least privilege access across today's sprawling, complex identity environments can be enormously difficult. Despite the challenge, working toward least privilege is crucial for security teams who want to protect their infrastructure and users. In a 2022 IDSA report, 80% of firms surveyed reported suffering from an identity-related breach in the previous year, and many blamed "inadequately managed privileges," "compromised privileged identity," or "excessive privileges leading to an insider attack" for those breaches. Least privilege is also important to compliance —most security-centric compliance regulations require some level of access management controls and policies and recommend least privilege access as a top level guiding principle.

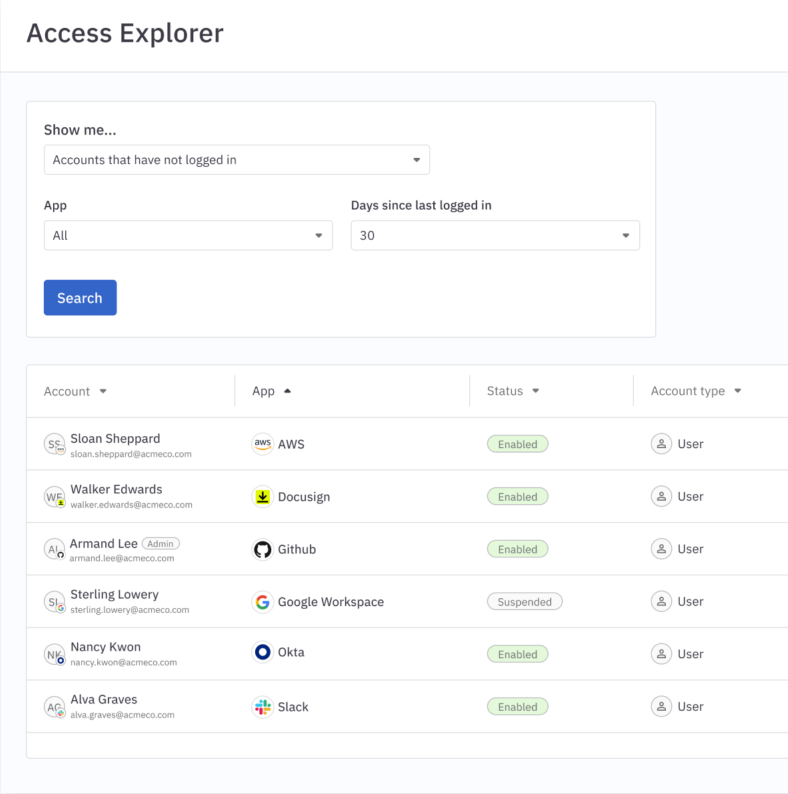
Though systems and sensitivities vary, every company can benefit from incorporating least privilege access best practices into their identity security and access control processes.

Here's how to get started.

Least Privilege Strategies & Tactics

01 Move sensitive access to time-based access

The first step to achieving least privilege is to identify which of your systems are mission critical. Once you have cataloged these systems, identify who has access and what permissions, roles, and group members provide privileged access. As a final step, shift these entitlements to a time-bound or contextually provisioned model, assuming by default that users don't need this type of access on a regular basis. You can think of granting access in these situations as a "privileged action" escalation. Users who need elevated privileges to perform privileged actions can request just-in-time access that fits their needs.



Show me... Accounts that have not logged in

App: All

Days since last logged in: 30

Account	App	Status	Account type
Sloan Sheppard sloan.sheppard@acmeco.com	AWS	Enabled	User
Walker Edwards walker.edwards@acmeco.com	Docusign	Enabled	User
Armand Lee Admin armand.lee@acmeco.com	Github	Enabled	User
Sterling Lowery sterling.lowery@acmeco.com	Google Workspace	Suspended	User
Nancy Kwon nancy.kwon@acmeco.com	Okta	Enabled	User
Alva Graves alva.graves@acmeco.com	Slack	Enabled	User

Not all access situations need to be time-based, but transferring sensitive permissions, applications, and roles to just-in-time access ensures users will always have the access they need, when they need it, without being overprovisioned.

02 Control sensitive access with appropriate policies and approvals

Establishing clearly defined, appropriate access policies and approval protocols for sensitive roles and permissions will ensure provisioning is handled consistently and with the correct checks and balances. Create standards for how employees in different roles will be onboarded, making least privilege the default for all new accounts, and decide how role changes and offboarding will be communicated and managed to make deprovisioning quick and comprehensive.

Educate all stakeholders on your new standardized access request and approval procedures, especially those that pertain to sensitive, just-in-time access, to make sure policies are clear and easy for everyone to follow.

03 Automate gaining visibility over who has sensitive access

The basis of securing any environment is to understand the environment. With the proliferation of SaaS and IaaS applications and the centralization of management of these environments, it can be a massive challenge to simply understand what roles and access exists, what identities and accounts have been created, and who has access to what. Security teams need to be able to answer these questions quickly and easily to achieve least privilege and this depends on automating the collection of data and the centralization of the information.

With this in mind, do all that you can to get full visibility of access, permissions, and group memberships across your system and keep this information centralized, up to date, and easy to reference. Once you have your system inventory in place, develop a schema for tagging roles, groups, and permissions within applications that are most sensitive so they're instantly identifiable.

04 Keep a comprehensive catalog & audit trail

When users are granted sensitive access, log the decision, approvals, and the context under which the access is granted so that it can be easily audited. This is useful information when reviewing whether access is still necessary and may be essential proof for external compliance requirements. The catalog of current sensitive access should be easily accessible by IT, Security, and GRC teams.

Actively maintain this catalog as part of your access review process—a user's or identity's status should be automatically updated in the catalog as part of the provisioning and deprovisioning processes.

05 Periodically review sensitive access

Defining least privilege access policies and keeping an up to date catalog of active sensitive access will go a long way toward achieving least privilege, but it's still crucial to regularly review sensitive access to ensure that currently provisioned access is still necessary. These reviews should not just depend on your catalog of access from any manually maintained audit trail, but ideally should poll the applications and accounts directly to ensure that the latest and most up to date information is used for review. This ensures that access was not provisioned outside of your business processes, but more importantly, if it was, that it is reviewed and recertified.

Following a few best practices for user access reviews can make the process more seamless and accurate. Collaborate with your company's managers and/or system administrators on periodic access reviews to certify that users have the correct levels of access.

06 Make access reviews timely and contextual

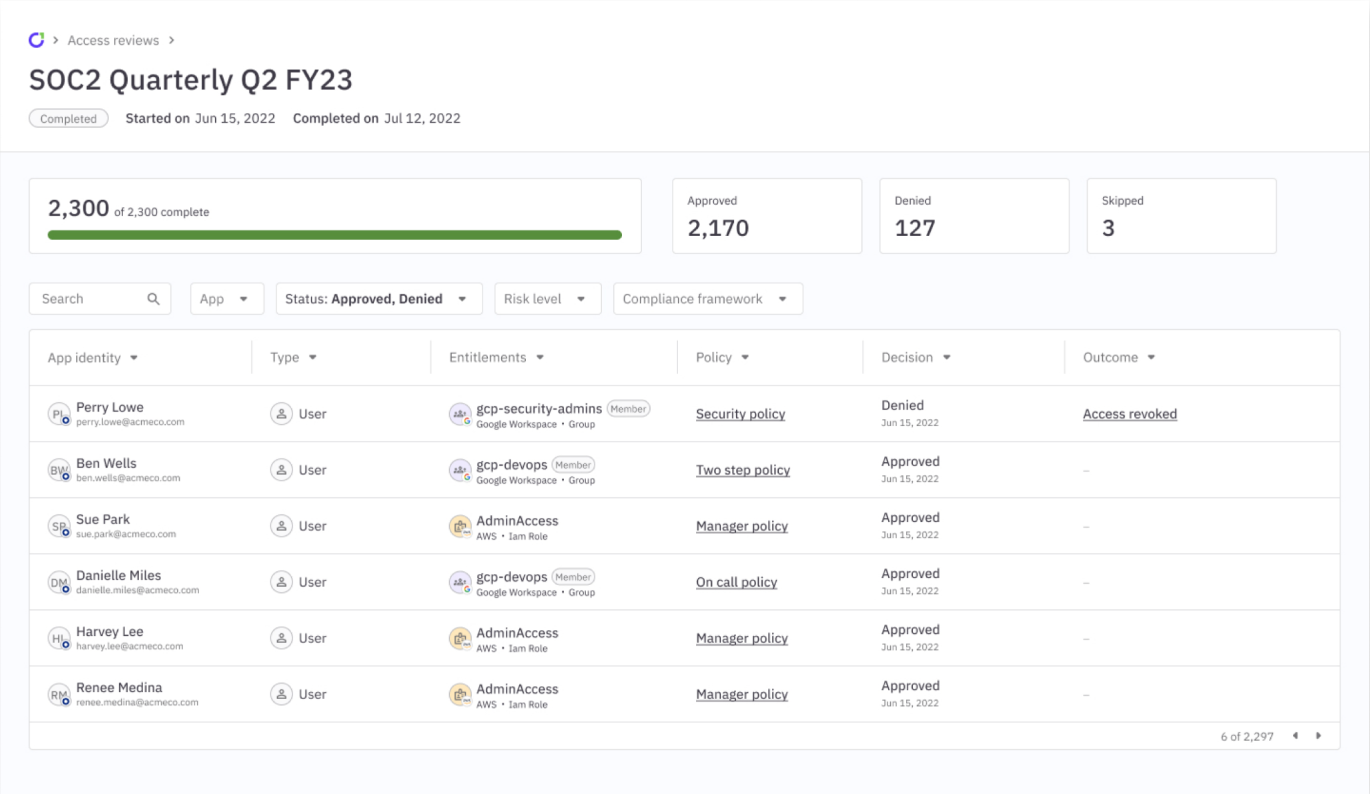
Access reviews are necessary for meeting compliance requirements, but they should also be seen as a critical tool for maintaining security by regularly identifying and removing unnecessary access. To maintain least privilege, access reviews should occur on a frequent and timely basis (at least once a quarter for privileged access) and be contextual (e.g., upon a significant role change). This level of on-going effort necessitates automation or the manual processes may become prohibitively expensive.

Create a regular schedule for user access reviews, defining the scope of each review scheduled, and share it with your supporting teams so they can prepare for and resource reviews appropriately.

07 Include context on access decisions

It's important to understand the security implications of any granted access, permission, or group membership. Downstream authorization implications of access may not always be clear to approvers or reviewers. Group memberships, for example, may have significant knock on effects of granted permissions on resources and/or roles which can be challenging to understand. This effective access is important context when making access decisions.

Regular access reviews should include context around risk, the account with the access, and downstream implications of the grant. Help those who grant and certify access to understand the security implications of their decisions so they can make the best decision.



SOC2 Quarterly Q2 FY23

Completed **Started on** Jun 15, 2022 **Completed on** Jul 12, 2022

2,300 of 2,300 complete

Approved 2,170

Denied 127

Skipped 3

Status: **Approved, Denied**

App identity	Type	Entitlements	Policy	Decision	Outcome
Perry Lowe perry.lowe@acmeco.com	User	gcp-security-admins Member Google Workspace • Group	Security policy	Denied Jun 15, 2022	Access revoked
Ben Wells ben.wells@acmeco.com	User	gcp-devops Member Google Workspace • Group	Two step policy	Approved Jun 15, 2022	–
Sue Park sue.park@acmeco.com	User	AdminAccess AWS • Iam Role	Manager policy	Approved Jun 15, 2022	–
Danielle Miles danielle.miles@acmeco.com	User	gcp-devops Member Google Workspace • Group	On call policy	Approved Jun 15, 2022	–
Harvey Lee harvey.lee@acmeco.com	User	AdminAccess AWS • Iam Role	Manager policy	Approved Jun 15, 2022	–
Renee Medina renee.medina@acmeco.com	User	AdminAccess AWS • Iam Role	Manager policy	Approved Jun 15, 2022	–

6 of 2,297

Least Privilege Realized

Working toward least privilege is an essential goal for security, IT, and GRC teams who want to help keep the access control secure and compliant. The proliferation of SaaS and IaaS applications, and permutations of permissions and roles within those systems, can make managing access unwieldy and risk prone.

At ConductorOne, we believe modern workforces require modern solutions for governance and access control. We help companies meet their compliance and security objectives, including least privilege, with a quick time-to-value, and an experience that users love and understand.

Want to learn more about our identity security platform for modern workforces?

ConductorOne, Inc.
548 Market St.
PMB 88486
San Francisco, CA 94104

team@conductorone.com

Chat with us