

Data Access Controls

Amplitude's granular access controls empower you to precisely manage who sees what data, ensuring compliance and minimizing risk.



Finding the balance between data accessibility and security is a critical challenge. Providing the right teams with the insights they need while protecting sensitive customer information can feel like an uphill battle. If your organization is grappling with this dilemma, you're not alone.

The stakes are even higher with the increasing complexity of data privacy regulations. Stringent laws like GDPR and CCPA demand a robust approach to data protection, with severe consequences for non-compliance.

Navigating this landscape can be overwhelming, but Amplitude's Data Access Controls (DAC) offer a powerful solution.

Data Access Controls empower you to take control of your data governance, ensuring that only authorized personnel have access to the information they need.

With granular permissions and customizable access, you can strike the perfect balance between data accessibility and security, fostering a culture of collaboration while mitigating risk.

Lockdown your data, unlock your insights

Amplitude's granular access controls empower you to precisely manage who sees what data, ensuring compliance while minimizing risk. Feel confident that your data is secure, your teams are empowered, and your organization is well-positioned for continued growth and success.

Key capabilities



Granular permissions

Control access at a highly detailed level, even down to specific data points within charts, user lookups, syncs, and event streams.



Customizable access

Tailor data access to to your teams and their responsibilities, ensuring each team member has precisely the information they need.



Sensitive data classification

Safeguard PII, revenue, and other sensitive data with additional layers of protection.

PERFORMANCE-DRIVEN TEAMS CHOOSE AMPLITUDE



With Data Access Controls you can:

Foster secure collaboration: Enable teams to work together effectively while maintaining data security and privacy.

Drive data-driven decision making: Empower your teams with the insights they need to fuel innovation and growth, all without compromising data security.

Adapt to your needs: Manage access at scale with an easy to navigate overview page and make adjustments on the fly with improved APIs.

Reduce risk: Minimize the risk of data breaches, accidental exposure, and non-compliance with data privacy regulations.

The screenshot displays the Amplitude Data Access Controls interface. On the left is a navigation sidebar with options like Home, Activity, Assistant, Visual Labeling, Events, Properties (selected), Filters, Groups, Connections Overview, Sources, Destinations, and Catalog. The main area is titled 'Properties' and shows a table of 500 user properties. The table has columns for NAME, STATUS, and REQUIRED. The 'plan' property is highlighted. To the right, a detailed view of the 'plan' property is shown, including its description, visibility, classification (Sensitive), and type (PII, Revenue, Sensitive).

NAME	STATUS	REQUIRED
Country	Live	Required
Device family	Live	Required
Device ID	Planned	Required
Device type	Planned	Required
email	Planned	Optional
IP address	Blocked	Required
Library	Blocked	Required
Latitude	Blocked	Required
Longitude	Live	Optional
OS	Live	Optional
plan	Live	Required
Platform	Live	Required
Region	Live	Required
Start Version	Live	Required

plan Details:

- Description: A user's plan type
- Visibility: Visible
- Classification: Sensitive
- Required: PII, Revenue, Sensitive
- Type: Sensitive
- Min Value: Not set
- Max Value: Not set
- Regex: Not set

[Explore Data Access Controls >](#)