Cross App Access (XAA)
Internal FAQs & Resources

Top 10 GTM FAQs – At a Glance

1. **What is XAA?**
   Cross App Access (XAA) is an open protocol (not a product) that extends OAuth to secure app-to-app and agent-to-app interactions by shifting control from individual apps to the enterprise IdP, giving IT centralized visibility and governance.

2. **Why now?**
   AI agents are driving a surge in autonomous, app-to-app communication that bypasses traditional identity controls. Without XAA, enterprises face blind spots, over-privileged tokens, and unmanaged integrations.

3. **How does it work?**
   XAA establishes trust between a requesting app and a resource app through the IdP. The requesting app first gets an ID-JAG token from the IdP, then presents the token to the resource app. The resource app validates it, and then mints a scoped access token—moving trust decisions into enterprise policy.

4. **How does XAA differ from OAuth?**
   OAuth was designed for user consent. XAA extends OAuth with enterprise authorization, moving consent from individuals to organizations, and using token exchange to secure app-to-app and agent-to-app flows.

5. **What risks does XAA solve?**

   - Token sprawl from static service accounts
   - Over-privileged credentials
   - Invisible app-to-app data sharing
   - Ungoverned AI agent actions

6. **What are the benefits for customers?**

- Centralized visibility and control over human + AI identities
- Consistent security policies across all integrations
- Reduced user consent fatigue and better UX
- Stronger compliance with auditable data sharing

7. **What are the benefits for ISVs and Auth0 B2B SaaS builders?**

- Out-of-the-box support in Auth0 (Jan 2026 for requesting apps; Q2 FY27 resource apps later)
- Faster enterprise adoption and trust
- Build once, integrate everywhere via standards

8. **Which ISV are supporting XAA today?**
   XAA is still in the network-building stage. 13 ISVs pledged support at Oktane 2025, validating its importance. Not all have begun building integrations yet. Please encourage any B2B SaaS partners you speak with to adopt it.

9. **Is XAA available for customers now?**
   Yes. XAA is in Early Access in Okta Platform with sample apps for testing. No third-party apps yet—the value grows as ISVs adopt. Auth0 out-of-the-box support begins Jan 2026. Encourage customers to ask their SaaS providers for XAA integrations.

10. **How does XAA fit into Okta's AI strategy?**
    XAA is a cornerstone of Okta Secures AI and part of Okta Secures AI Agents, an offering that will be available EA in Jan. 2026. It's key to securing the full lifecycle of AI agents and non-human identities across the identity fabric.

Deep Dive FAQs

Basics

1. **What is Cross App Access (XAA)?**
   Cross App Access is an open protocol (not a product) that extends OAuth to secure app-to-app and agent-to-app interactions. It shifts access control from individual apps

and end users to the identity provider (IdP), allowing enterprises to centrally govern data sharing between SaaS apps, AI agents, and other non-human identities.

2. Why was XAA created, and why now?

AI agents are driving a surge in autonomous, app-to-app communication that bypasses traditional identity controls. Most existing protocols were built for human-to-app interactions, not for autonomous agents. Without XAA, enterprises face blind spots, over-privileged tokens, and unmanaged integrations. XAA provides the visibility, governance, and security needed to keep pace with agentic AI.

3. How does XAA differ from OAuth?

OAuth was originally designed to enable third-party apps to access a user's data. OAuth has been extended over the years to add many new capabilities and use cases. XAA is a further extension of OAuth that adds enterprise-level authorization controls, shifting consent from individuals to organizations. It uses the OAuth Token Exchange and JWT Authorization Grant (JAG) frameworks to leverage the common relationship two apps have with an enterprise IdP, enabling the IdP to govern the connection between apps.

4. How does XAA relate to other identity standards like MCP and IPSIE?

XAA is complementary. MCP (Model Context Protocol) focuses on how agents can connect to external applications and is an authorization extension of XAA, while the emerging IPSIE standard sets broader interoperability standards between IdPs and SaaS apps. If an MCP client and server support XAA, the application gets the same value of centralized visibility and control for their enterprise customers. XAA provides the authorization layer that governs which agents and apps can connect to each other, under enterprise control. Together, these standards form the foundation for secure agentic AI.

5. How does XAA work?

XAA works by establishing trust between two apps — a requesting app and a resource app — through the IdP.

- The requesting app requests an ID-JAG from the enterprise IdP using an ID Token it previously obtained for the user.
- The requesting app presents the ID-JAG token to the resource app, representing the statement that the enterprise IdP has validated it’s ok for the requesting app to access this user's resources on the resource app.
- The resource app validates the ID-JAG and creates its own access token that grants only the appropriate level of access.

This flow shifts trust decisions away from end-user clicks and into centrally managed enterprise policy, ensuring secure, auditable app-to-app and agent-to-app connections.

Security & Value

6. What security risks does XAA solve for enterprises?

XAA closes a major blind spot in enterprise security: unmanaged app-to-app and agent-to-app communication. It prevents risks like token sprawl, over-privileged service accounts, invisible data sharing, and ungoverned AI agent actions.

7. How does XAA help with AI agents and other non-human identities (NHIs)?

XAA treats AI agents and non-human identities as first-class, with the same visibility, lifecycle management, and policy controls as humans. Enterprises can apply least privilege, audit behavior, and revoke access centrally, reducing risks from unpredictable or malicious agent activity.

8. How does XAA address token sprawl and over-privileged service accounts?

Instead of relying on static service accounts with broad scopes, XAA replaces them with scoped, short-lived tokens governed by the IdP. This minimizes exposure, reduces attack surfaces, and gives admins visibility into every integration.

9. How does XAA improve enterprise visibility and control over app-to-app communication?

By centralizing consent and authorization in the IdP, XAA gives IT and security teams one place to see which apps and agents are connected, what data is being shared, and enforce policies around those interactions.

10. How does XAA reduce risk for enterprises while improving user experience?

Users no longer face endless OAuth consent prompts. Instead, admins pre-approve integrations, reducing friction while ensuring safer, consistent access decisions. Enterprises gain oversight without disrupting workflows.

Benefits by Audience

11. What are the main benefits of XAA for Okta customers?

Improved security posture & UX:

- Visibility into which apps & agents are sharing data between each other
- Centralized control over which apps can connect and what data they can access
- Improved UX & reduced risk by eliminating repetitive OAuth prompts, preventing users from accidentally over-granting access

12. What are the main benefits of XAA for Auth0 B2B SaaS builders?

Faster enterprise adoption, less dev effort:

- Provide control and visibility to their enterprise customers without writing custom logic—XAA will soon be offered out-of-the-box in Auth0
- Let IT admins manage connections, while you focus on your product
- Provide expedited adoption of AI features by removing long-lived tokens, user consent fatigue, and integration friction

13. What are the main benefits of XAA for ISVs and partners?

Faster enterprise adoption, better user experience:

- Improved trust & faster sales cycles by meeting security and compliance requirements
- A smoother user experience by eliminating repetitive OAuth prompts
- Build once and use with all participating IdPs

14. What use cases are the best fit for XAA?

- AI agent governance across SaaS apps
- Service access where long-lived tokens are risky
- Enterprise SaaS data sharing (e.g., Slack <-> Zoom <-> Atlassian)
- App-to-app consent and control in B2B SaaS

15. Are there use cases that are not a good fit for XAA?

- Highly regulated environments like FedRAMP/HIPAA (not supported in Phase 1)

- Consumer/B2C scenarios where end-user consent is the primary model

Adoption & Ecosystem

16. How do ISVs adopt XAA?

Auth0 B2B SaaS Builders: Starting in January 2026, Auth0 will provide out-of-the-box XAA support for requesting apps. This means developers can enable their apps to request access tokens via the new ID+JAG flow without custom code. Support for resource apps will follow later in the year. Builders simply configure their integrations in Auth0, and XAA handles the secure exchange.

Other ISVs: ISVs integrating outside of Auth0 can adopt XAA by visiting Cross App Access Get Started Blog and updating their authorization servers to support the protocol. This involves:

- Accepting ID+JAG tokens from requesting apps
- Validating those tokens with the IdP (e.g., Okta)
- Minting scoped, user-bound access tokens for downstream APIs
- Registering their integrations via the Okta Integration Network (OIN) or other IdPs as they adopt, so enterprises can discover and centrally manage them

17. Which ISVs are already supporting or piloting XAA?

Several ISVs have started building the integration and the following have pledged their support for the protocol as of Oktane 2025, validating the importance of XAA.

- AGNCY
- Automation Anywhere
- AWS
- Boomi
- Box
- Cloudflare
- Glean
- Grammarly
- Google Cloud

- Miro
- Workday
- WRITER
- Zoom

18. How does XAA fit into Okta's broader "Okta Secures AI" strategy?

XAA is a cornerstone of Okta's identity fabric for securing agentic AI. Alongside Auth for GenAI, OPA, ISPM, and OIG, it enables Okta to secure the full lifecycle of AI agents and non-human identities.

Product & Roadmap

19. Is XAA available for customers today, and in what form?

Yes. XAA is currently in Early Access (EA) in the Okta Platform. Customers can enable it and test the protocol using Okta-provided sample apps that demonstrate how requesting and resource apps exchange tokens via the new ID+JAG flow. However, since we are still in the ISV recruitment phase, there aren't third-party apps in production that support XAA yet. The value for enterprises will grow as more SaaS vendors adopt the protocol. Customers can see the Cross App Access (XAA) Demo Walk Through video for more information.

Auth0 Roadmap:

- **Requesting apps** will be supported out of the box in Auth0 in January 2026.
- **Resource apps** support will follow *later in 2026*.

Competitive & Market Positioning

20. How is XAA different from traditional OAuth token exchange?

OAuth token exchange was designed for machine-to-machine calls, independent of a user session. XAA ties authorization directly to user SSO sessions and enterprise policies, giving organizations visibility and control over what data flows between apps.

21. How is XAA different from alternatives like MCP or Agent2Agent?

- MCP standardizes context-sharing but doesn't define authorization.

- Agent2Agent extends MCP with authentication but leaves authorization open — XAA fills that gap.

22. Why is Okta uniquely positioned to lead with XAA?

Okta already secures identity for thousands of enterprises and has a trusted ISV integration network. As a neutral IdP, Okta can rally ISVs, enterprises, and standards bodies around XAA as an open protocol. In fact, the IETF OAuth Working Group has already adopted the Identity Assertion Authorization Grant spec – the basis of XAA. This is an important step in helping XAA move from a protocol into an official standard.

23. How does XAA help Okta compete in the AI and identity standards landscape?

XAA positions Okta as the leader in securing agentic AI by solving a critical enterprise problem—governing agent-to-app interactions. This establishes Okta as the default identity provider for AI-driven applications.

24. What's the long-term vision for XAA as part of the identity fabric?

XAA will become the standard authorization framework for securing all non-human interactions across SaaS apps and AI agents. Over time, it will integrate into the identity security fabric alongside governance, threat protection, and posture management.

25. What resources are available to send to customers, ISVs and Auth0 B2B SaaS builders?

Cross App Access Get Technical Presentations in Highspot

Identity Summit: Securing Agentic AI Event Replay

Cross App Access Landing Page

Cross App Access Newsroom Blog: Byline by Arnab

Cross App Access Product Announcement PR

Integrate your ISV Tools with XAA Blog

Cross App Access Get Started Blog

Why Adopt XAA: Presentation for Enterprise SaaS Builders & AI Platforms

XAA in MCP: High-Level Overview for ISVs

26. What is XAA in the context of MCP?

Cross App Access (XAA) is the enterprise-managed authorization layer for MCP. MCP defines *how* AI agents connect to tools; XAA defines *who* is allowed to access what, under enterprise policy. Together, they give enterprises secure, governed agent-to-app connectivity.

27. How do MCP roles map to XAA?

MCP Client → Requesting App
(the AI agent or LLM, like ChatGPT or Claude)

MCP Server → Resource App
(the tool or SaaS app the agent wants to access)

How does the flow work?

1. The MCP Client obtains an enterprise-issued ID-JAG token from the IdP.
2. It presents that token to the MCP Server.
3. The MCP Server validates it and issues a scoped access token, enforcing the enterprise's policies.
4. No prompts, no user consent screens — authorization is fully handled by the IdP.

This shifts trust decisions away from end users and into centralized, auditable enterprise policy.

29. Does every MCP Server need to adopt XAA?

Not always. If the MCP Server implements its own authorization, it should adopt XAA directly. If the MCP Server uses an external authorization server (e.g., Auth0) that already supports XAA, then the MCP Server automatically benefits and does not need to implement XAA itself.

30. Why XAA in MCP Is Better for ISVs (Requesting & Resource Apps)

Benefits for MCP Servers (Resource Apps / Tools)

- Enterprise-ready out of the box: No need to build complex OAuth or consent flows.
- Higher security with lower complexity: IdP enforces policy; the server avoids managing credentials or custom authorization.
  Faster enterprise sales cycles: Aligns with enterprise governance and reduces procurement friction.
- Standards-based integrations: "Build once, integrate with any IdP that supports XAA."

Benefits for MCP Clients (Requesting Apps / AI Agents)

- **One unified authorization flow:** No more integrating with dozens of different OAuth implementations.
- **Zero user friction:** Agents connect to XAA-enabled servers automatically — no pop-ups or manual setup.
- **Enterprise trust built in:** ID-JAG tokens prove the agent is acting under enterprise policy.

31. How ISV Adoption Changes Now That XAA Is in the MCP Spec

- **MCP gains a standardized enterprise authorization model:** Makes MCP viable for security-sensitive use cases.
- **SDK updates simplify adoption:** TypeScript and Java SDKs bring XAA support with minimal engineering effort.
- **Enterprise expectations shift:** “MCP + XAA” becomes the default requirement for secure AI integrations.

32. Benefits for Customers (Why Enterprises Will Push ISVs)

Security & Risk Reduction:

- Centralized IdP policy control
- Eliminates static service accounts
  Full auditability of agent-to-app access

IT & Governance:

- Visibility into all AI-agent connections
- Eliminates shadow integrations
- Fits directly into existing IdP governance workflows

End Users:

- No configuration of MCP clients
- Zero consent fatigue
  Smooth, policy-backed agent experiences

XAA in MCP Resources

[XAA as an Auth Extension of MCP GitHub Repo]

XAA as an MCP Auth Extension: Internal Announcement

Cross App Access extends MCP to bring enterprise-grade security to AI agent interactions

Client Registration and Enterprise Management in the November 2025 MCP Authorization Spec