Enterprise-ready Auth for MCP With Cross-App Access (XAA)

Paul Carleton & Max Gerber

Who We Are

Paul Carleton, Anthropic

Max Gerber, Twilio

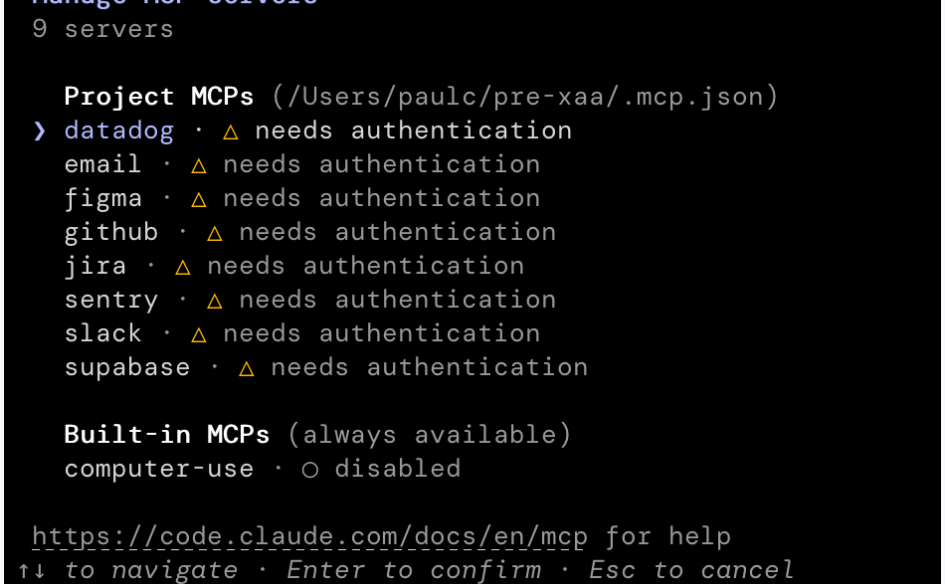
What We're Covering

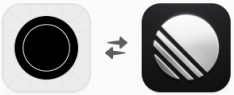
- Problems with OAuth Today
- How XAA fixes it
- Demos

Day 1 at Acme


Paul-Carleton-MacBook ~/pre-xaa
claude
Claude Code v2.1.89
Welcome back Paul!
Opus 4.6 (1M context) · Claude Max · Paul Carleton
~/pre-xaa
Tips
Run
Rece
No r
* Voice mode is now available · /voice to enable

Day 1 at Acme


9 servers
Project MCPs (/Users/paulc/pre-xaa/.mcp.json)
❯ datadog · △ needs authentication
email · △ needs authentication
figma · △ needs authentication
github · △ needs authentication
jira · △ needs authentication
sentry · △ needs authentication
slack · △ needs authentication
supabase · △ needs authentication
Built-in MCPs (always available)
computer-use · ○ disabled
https://code.claude.com/docs/en/mcp for help
↑↓ to navigate · Enter to confirm · Esc to cancel



Claude is requesting access

Details

Name:	Claude
Redirect URIs:	https://claude.ai/api/mcp/auth_callback

This MCP client is requesting to be authorized. If you approve, you will be redirected to authenticate with your Linear workspace.

Cancel Approve

Figma MCP in Claude would like to access your account and be able to:

- ✓ Connect to Figma's remote MCP server

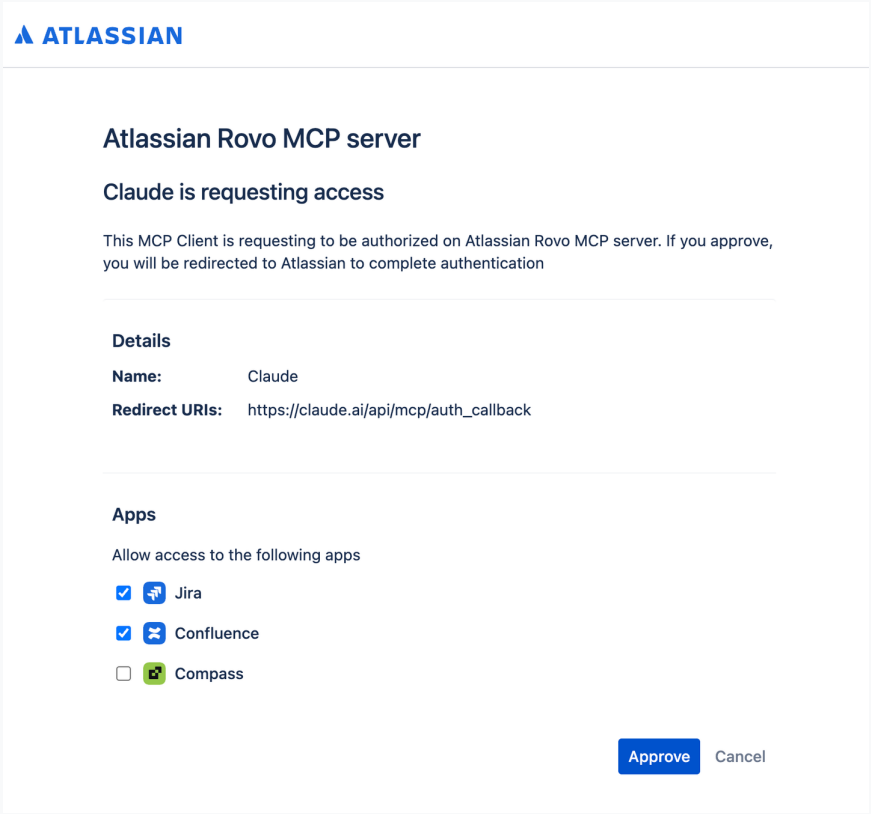
If you click "Agree & Allow Access" below, this MCP connection will provide **Figma MCP in Claude** read and write access to your Figma account.

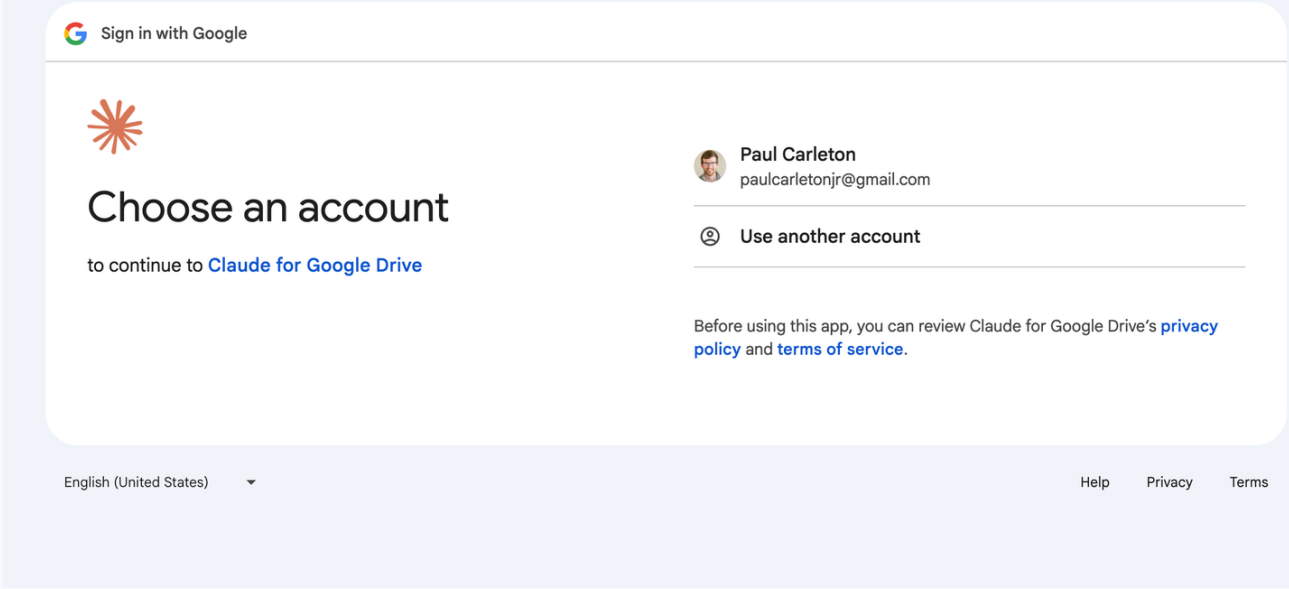
Any information you bring into the Figma platform via this MCP connection is subject to your existing agreement with Figma. Likewise, information you bring into **Figma MCP in Claude** from the Figma platform will be processed in accordance with your existing agreement with **Figma MCP in Claude**.

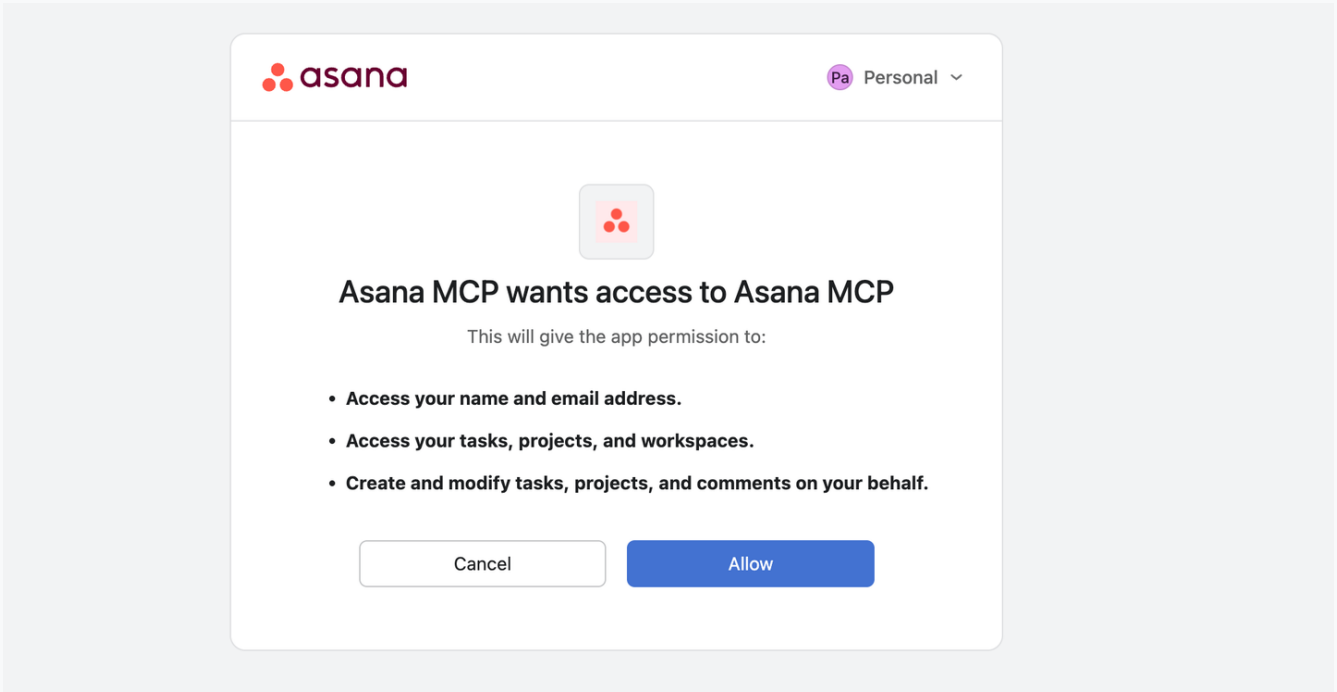
Review the Figma Developer Docs to learn more.

You may receive product, service, and events email updates from Figma and can opt-out at any time.

Agree & Allow Access


ATLASSIAN
Atlassian Rovo MCP server
Claude is requesting access
This MCP Client is requesting to be authorized on Atlassian Rovo MCP server. If you approve, you will be redirected to Atlassian to complete authentication
Details
Name: Claude
Redirect URIs: https://claude.ai/api/mcp/auth_callback
Apps
Allow access to the following apps
Jira
Confluence
Compass
Approve
Cancel


Sign in with Google
Choose an account
to continue to Claude for Google Drive
Paul Carleton
paulcarletonjr@gmail.com
Use another account
Before using this app, you can review Claude for Google Drive's privacy policy and terms of service.
English (United States)
Help
Privacy
Terms


asana
Pa Personal
Asana MCP wants access to Asana MCP
This will give the app permission to:
Access your name and email address.
Access your tasks, projects, and workspaces.
Create and modify tasks, projects, and comments on your behalf.
Cancel
Allow

What if there was a better way?

Day 1000 at Acme

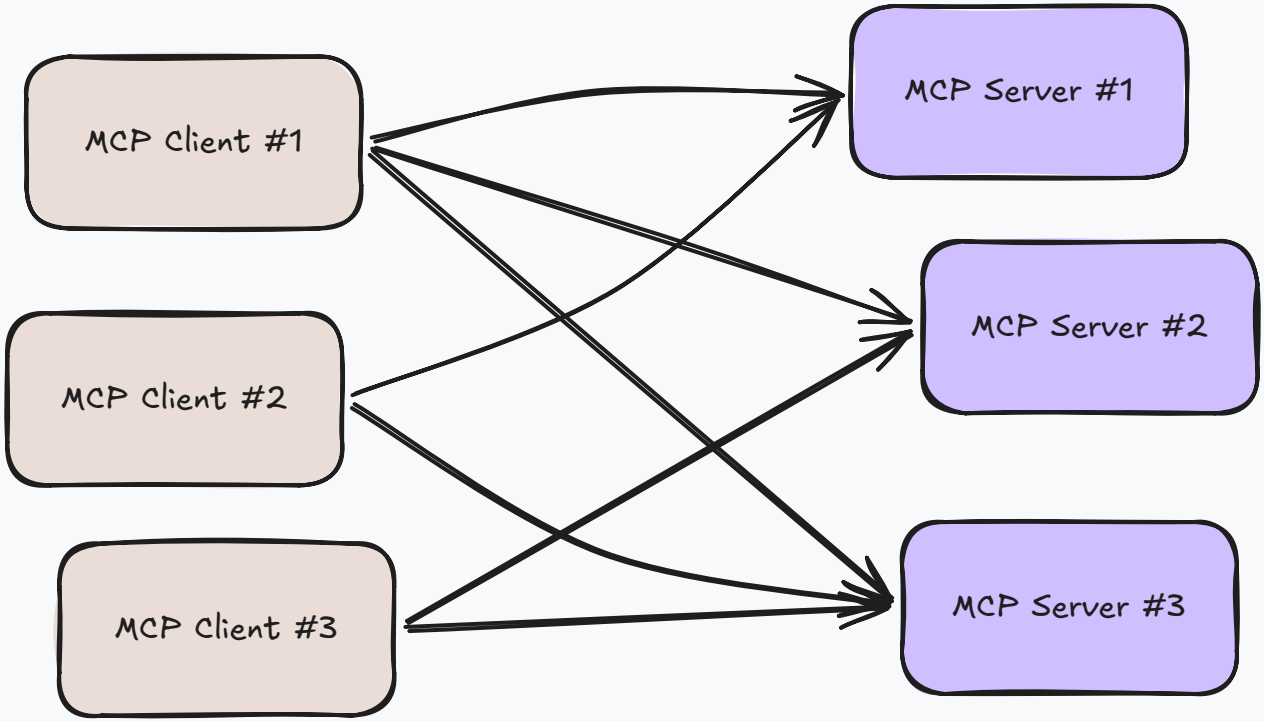
Yesterday

6:28 PM **max** How was the meeting?

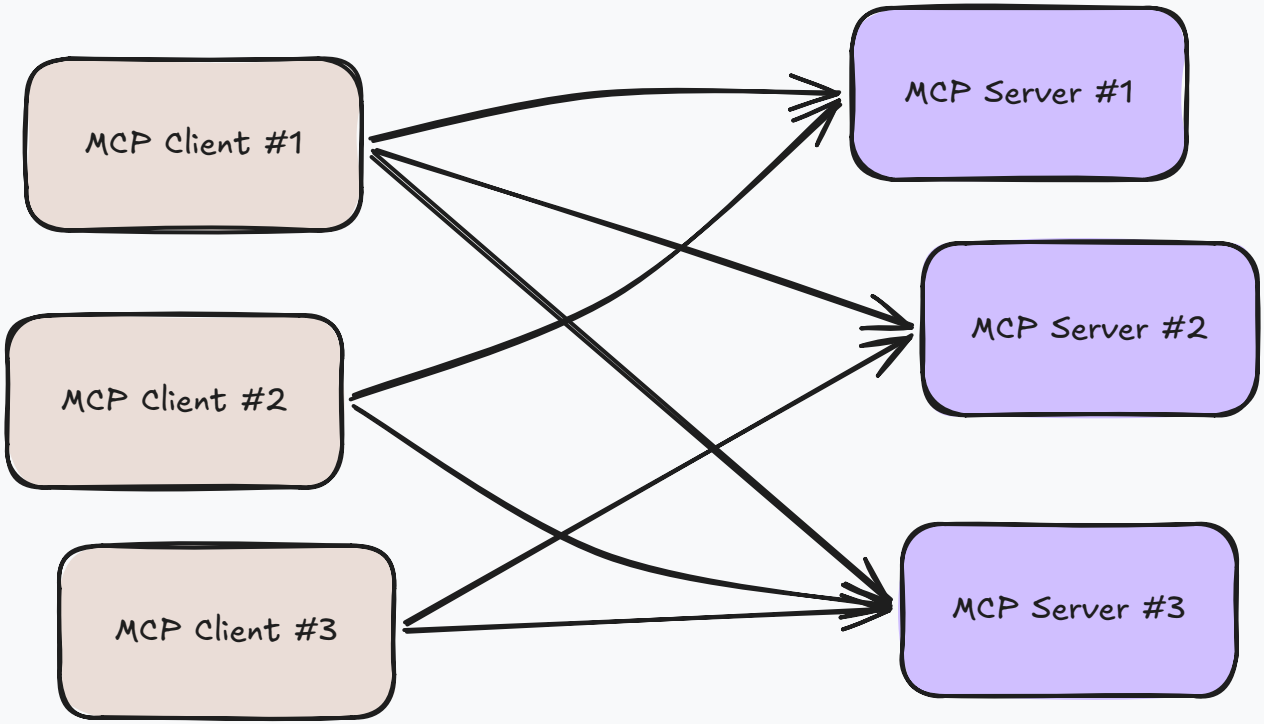
Not too bad I hope?

6:28 PM **Howard Limburg** No it was pretty bad. CISO is really concerned. We need to make sure all the coding agents have only read-only access to prod data.

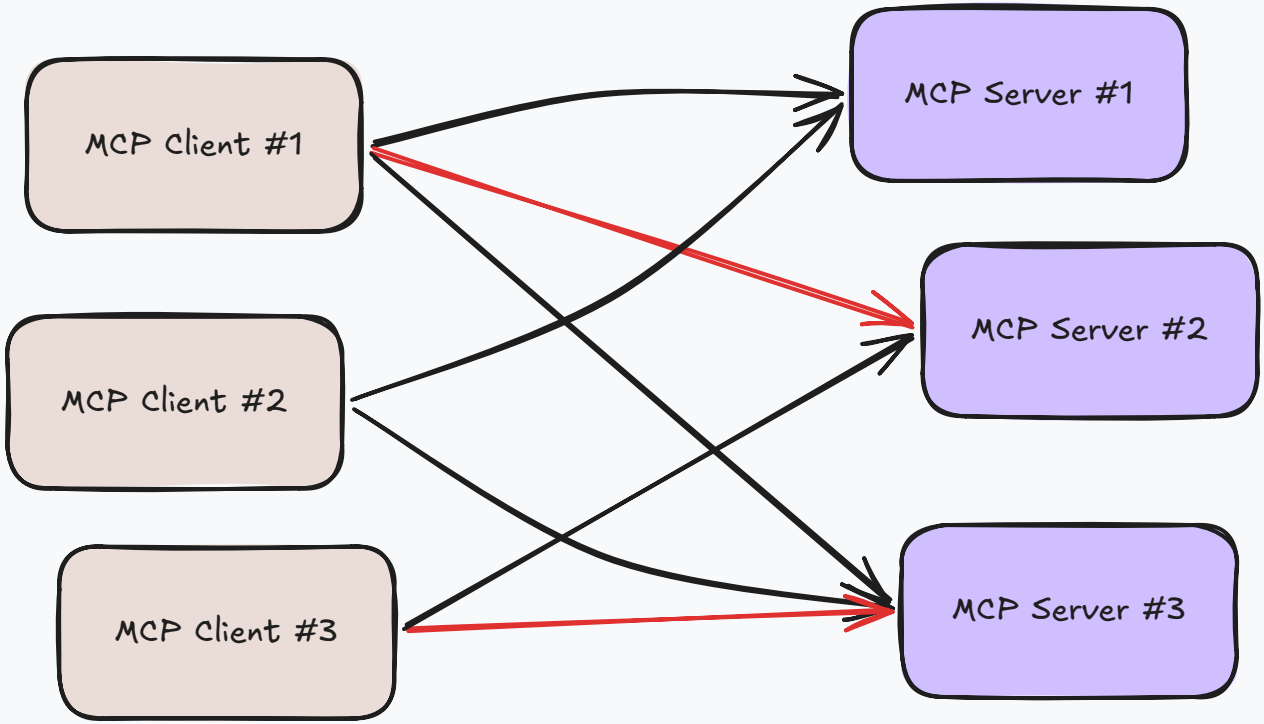
oh jeez... this is going to take forever


MCP Client #1
MCP Client #2
MCP Client #3
MCP Server #1
MCP Server #2
MCP Server #3

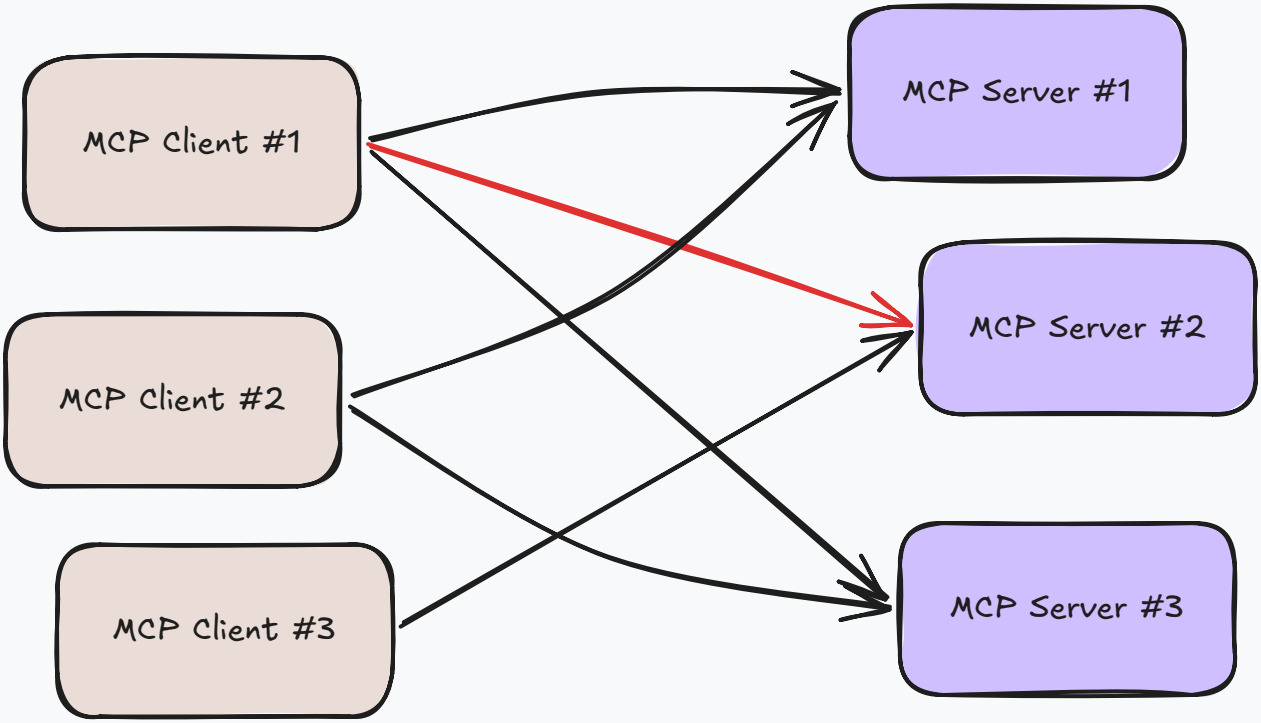
⚠ Read-Only Access



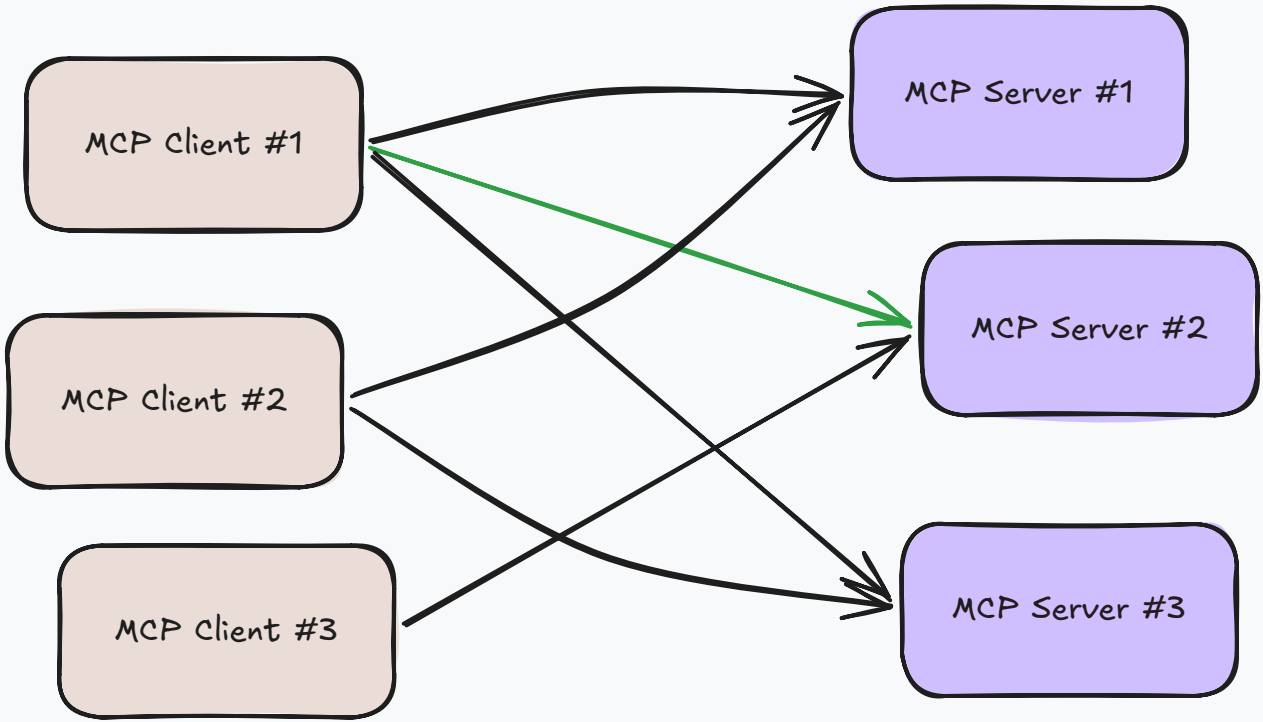
⚠ Read-Only Access



⚠ Read-Only Access



⚠ Read-Only Access



Google Account

Third-party apps & services

Keep track of your connections

You shared data with these third-party apps and services. Learn more

58 total apps & services

Search by name

Filter by:

Sign in with Google (58) | Access to (4) | Linked account (0)

- Calendly
- Claude
- Clerk
- Cloudflare Dashboard
- Devpost
- Figma

Manage

Resolutions

Installed Apps

Custom Integrations

Deactivated Apps

Connected Accounts

Muted Apps

Installed apps

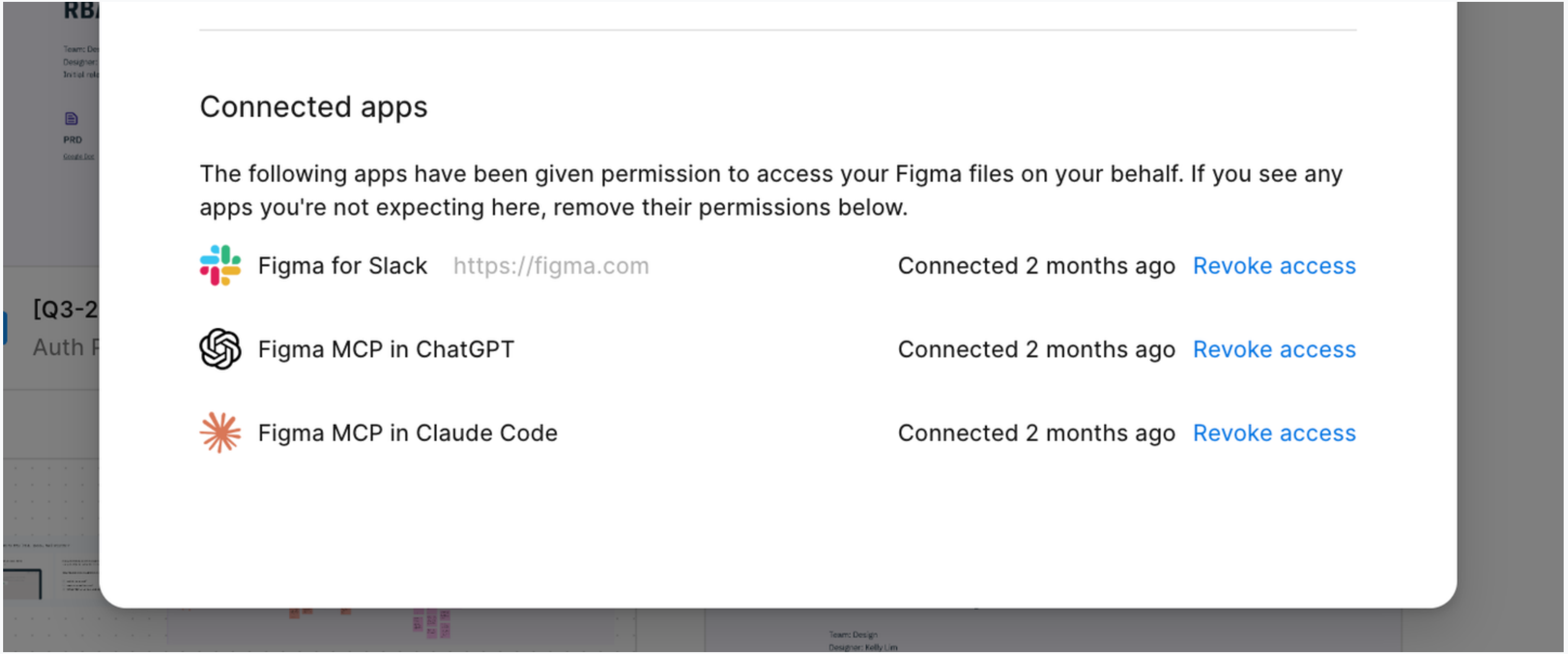
Manage the apps and services that are available to people in your organization. Learn more

Description includes: e.g. GitHub

Access type: All

Installed by: Anyone

Name	Steps	App resolution
Gusto	0	Approval required
Hex	0	Approved
Hightouch	0	Approval required
Honeycomb	0	Approval required
HubSpot	0	Approved
Instatus	0	Approved
Jira Cloud	0	Approved
LaunchDarkly	0	Approval required
LaunchNotes Announce	0	Approval required
Linear	0	Approved
Loom	0	Approved
Notion	0	Approved


Connected apps
The following apps have been given permission to access your Figma files on your behalf. If you see any apps you're not expecting here, remove their permissions below.
Figma for Slack https://figma.com Connected 2 months ago Revoke access
Figma MCP in ChatGPT Connected 2 months ago Revoke access
Figma MCP in Claude Code Connected 2 months ago Revoke access

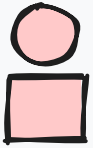
What if there was a better way?

Enterprise State of Mind

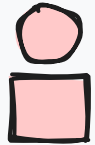
- In consumer usecases, the USER decides what to share and with whom

- In the enterprise, data belongs to the COMPANY

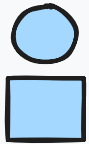
- The IT Admin is responsible for this



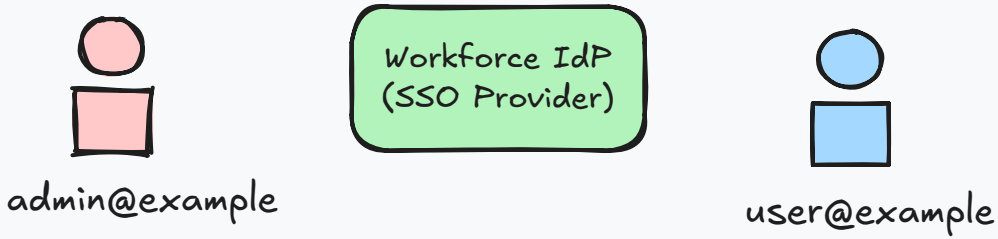
admin@example



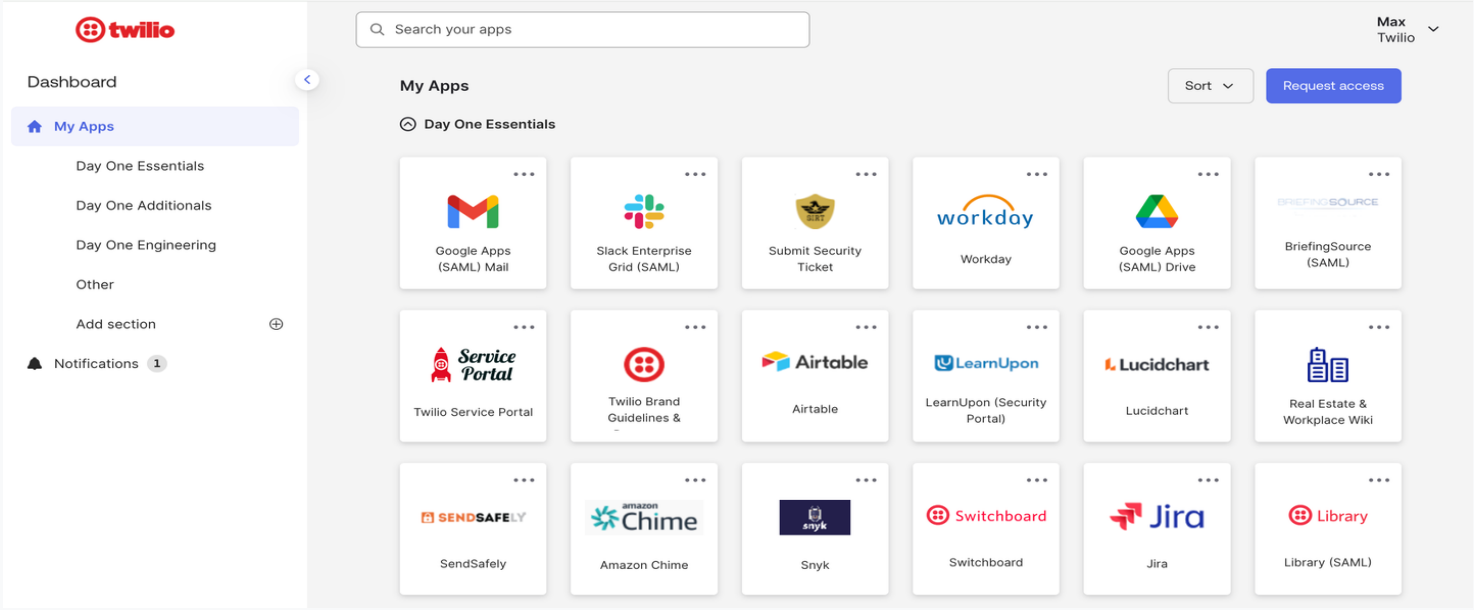
admin@example



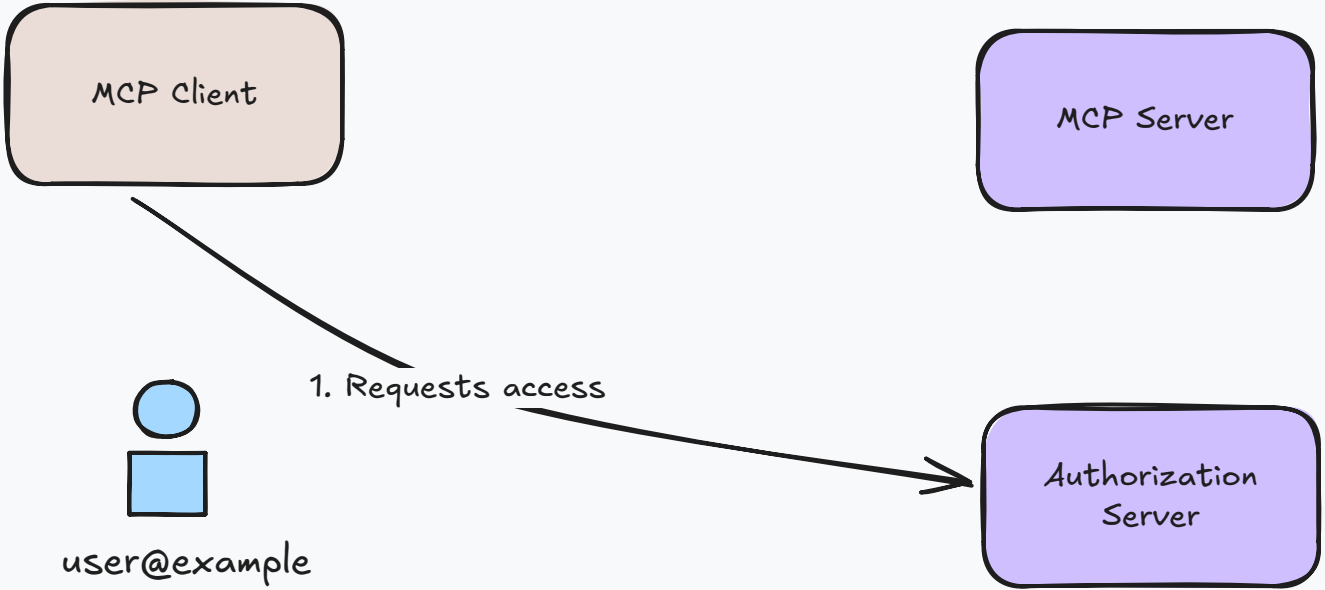
user@example

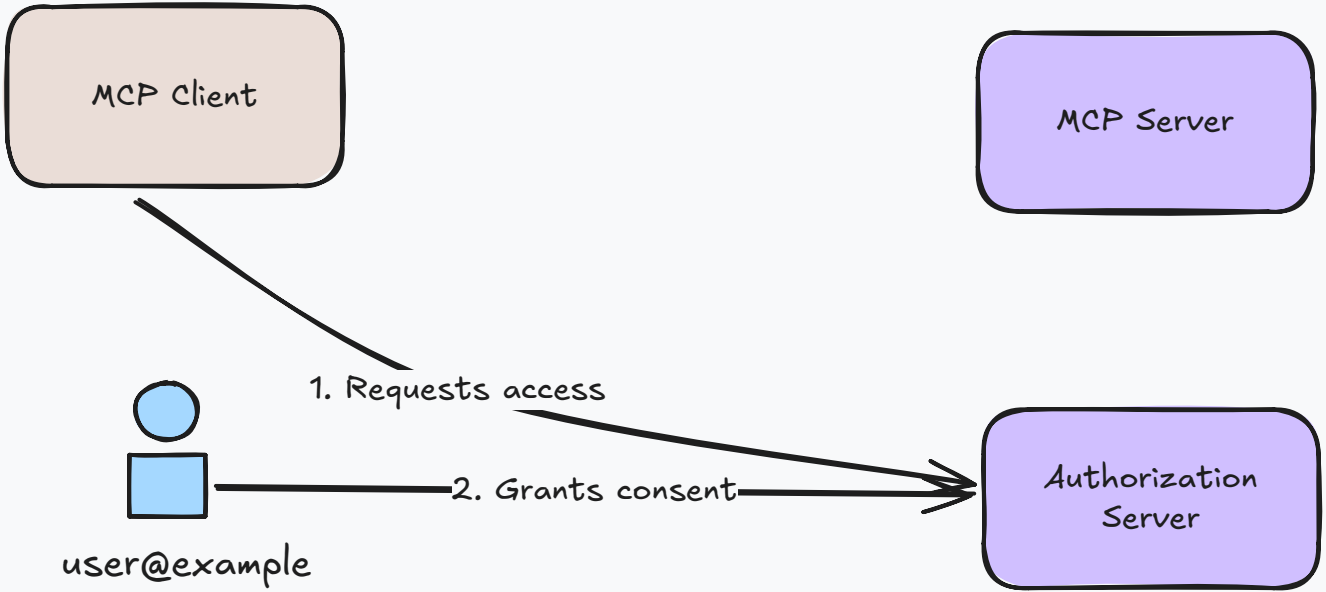

Workforce IdP
(SSO Provider)
admin@example
user@example

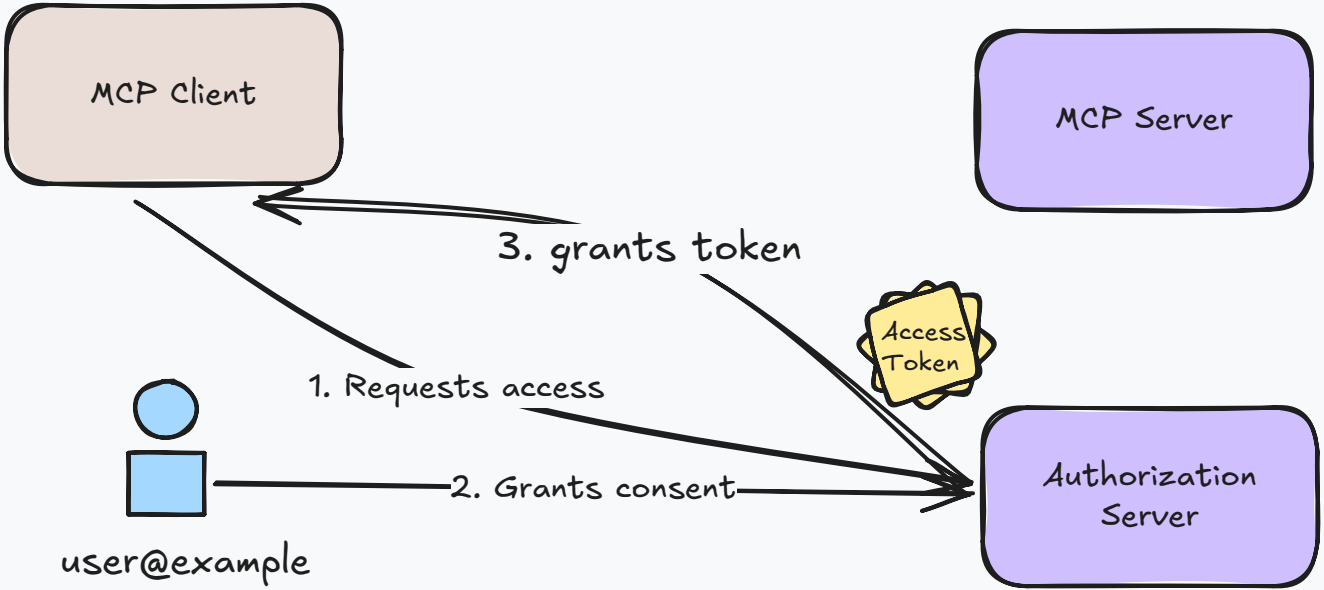

Workforce IdP
(SSO Provider)
admin@example
user@example

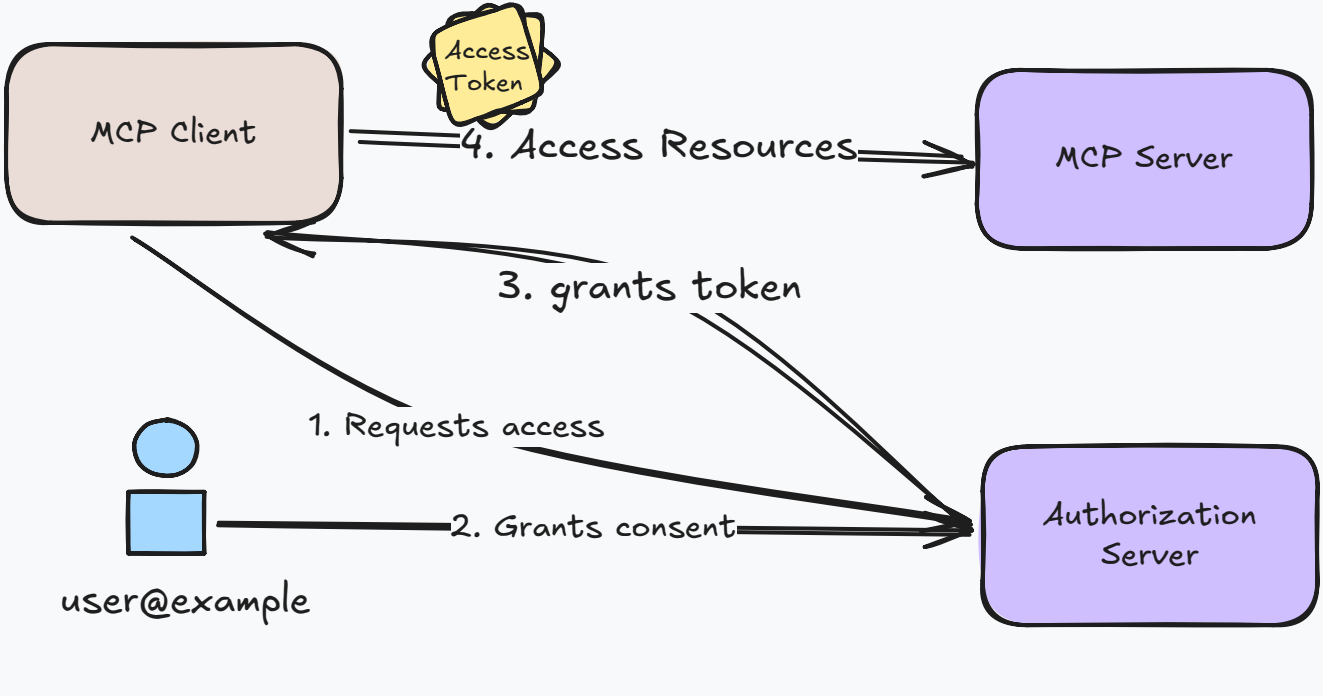

twilio
Search your apps
Max
Twilio
Dashboard
My Apps
Day One Essentials
Day One Additionals
Day One Engineering
Other
Add section
Notifications 1
My Apps
Sort
Request access
Day One Essentials
Google Apps (SAML) Mail
Slack Enterprise Grid (SAML)
Submit Security Ticket
Workday
Google Apps (SAML) Drive
BriefingSource (SAML)
Twilio Service Portal
Twilio Brand Guidelines &
Airtable
LearnUpon (Security Portal)
Lucidchart
Real Estate & Workplace Wiki
SendSafely
Amazon Chime
Snyk
Switchboard
Jira
Library (SAML)

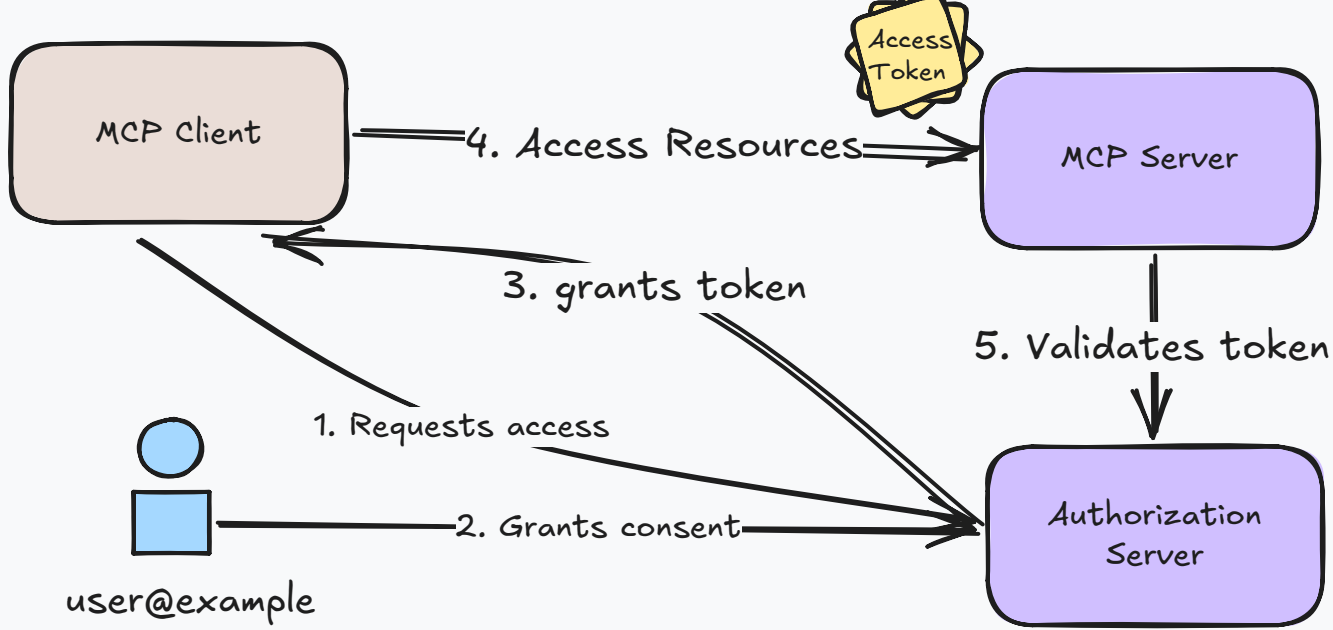

MCP Client
MCP Server
OAUTH
OAUTH
user@example
Authorization Server

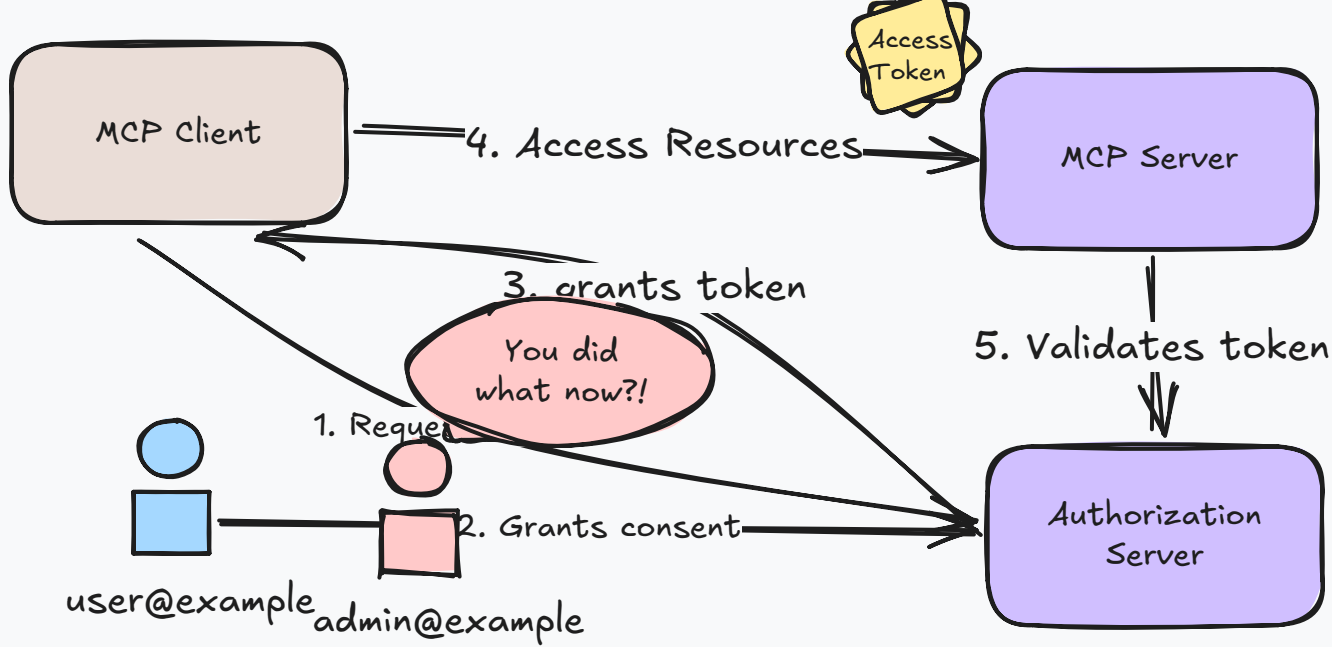

MCP Client
MCP Server
1. Requests access
Authorization Server
user@example

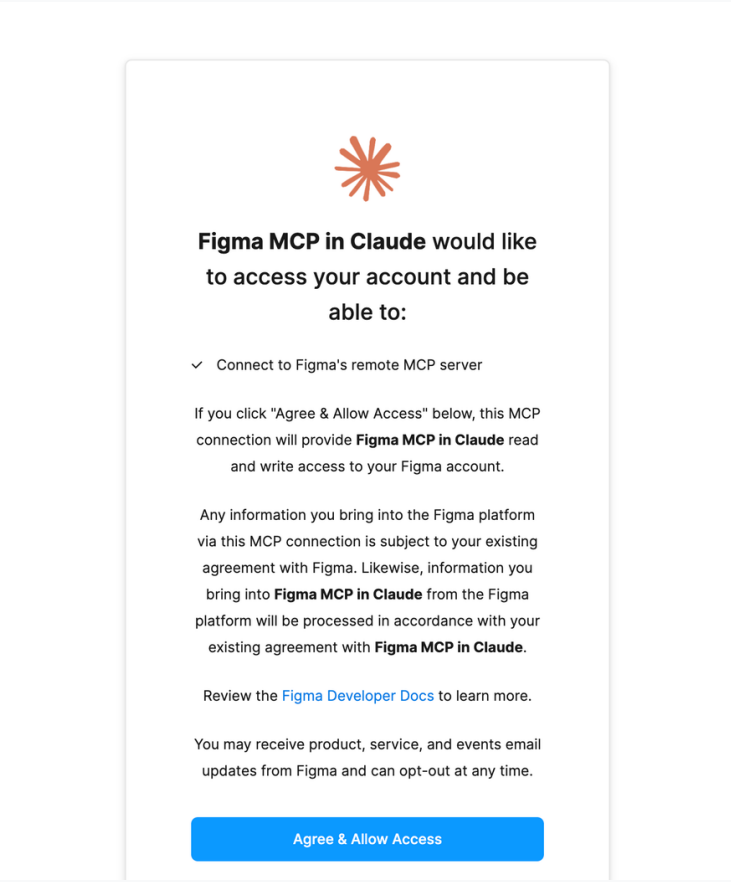

MCP Client
MCP Server
1. Requests access
2. Grants consent
Authorization Server
user@example


MCP Client
MCP Server
3. grants token
Access Token
1. Requests access
2. Grants consent
Authorization Server
user@example

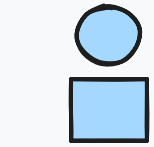

MCP Client
Access Token
4. Access Resources
MCP Server
3. grants token
1. Requests access
2. Grants consent
Authorization Server
user@example


Access Token
MCP Client
4. Access Resources
MCP Server
3. grants token
5. Validates token
1. Requests access
2. Grants consent
Authorization Server
user@example


Access Token
MCP Client
4. Access Resources
MCP Server
3. grants token
You did what now?!
5. Validates token
1. Reque
2. Grants consent
Authorization Server
user@example
admin@example

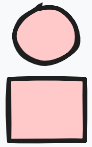


This consent screen matters less

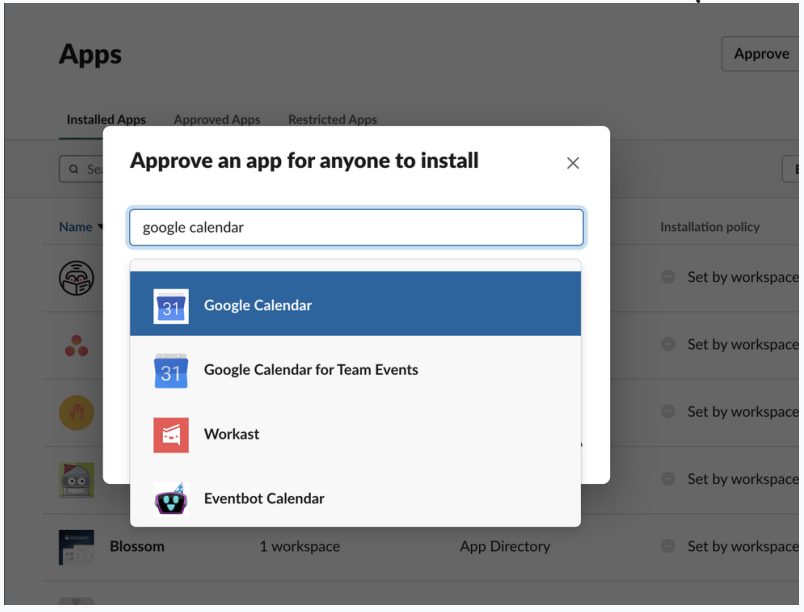


user@example

Than this config screen



admin@example



Workgroup: Web Authorization Protocol
Internet-Draft:
draft-ietf-oauth-identity-assertion-authz-grant-02
Published: 2 March 2026
Intended Status: Standards Track
Expires: 3 September 2026

A. Parecki
Okta
K. McGuinness
Independent
B. Campbell
Ping Identity

Identity Assertion JWT Authorization Grant

Abstract

This specification provides a mechanism for an application to use an identity assertion to obtain an access token for a third-party API by coordinating through a common enterprise identity provider using Token Exchange [RFC8693] and JWT Profile for OAuth 2.0 Authorization Grants [RFC7523].

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://drafts.oauth.net/oauth-identity-assertion-authz-grant/draft-ietf-oauth-identity-assertion-authz-grant.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-oauth-identity-assertion-authz-grant/.

Discussion of this document takes place on the Web Authorization Protocol Working Group mailing list (mailto:oauth@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/oauth/. Subscribe at https://www.ietf.org/mailman/listinfo/oauth/.

Source for this draft and an issue tracker can be found at https://github.com/oauth-wg/oauth-identity-assertion-authz-grant.

Workgroup: Web Authorization Protocol
Internet-Draft:
draft-ietf-oauth-identity-assertion-authz-grant-02
Published: 2 March 2026
Intended Status: Standards Track
Expires: 3 September 2026

A. Parecki
Okta
K. McGuinness
Independent
B. Campbell
Ping Identity

Discussion of this document takes place on the Web Authorization Protocol Working Group mailing list (mailto:oauth@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/oauth/. Subscribe at https://www.ietf.org/mailman/listinfo/oauth/.

Source for this draft and an issue tracker can be found at https://github.com/oauth-wg/oauth-identity-assertion-authz-grant.

Authorization Extensions

Enterprise-Managed Authorization

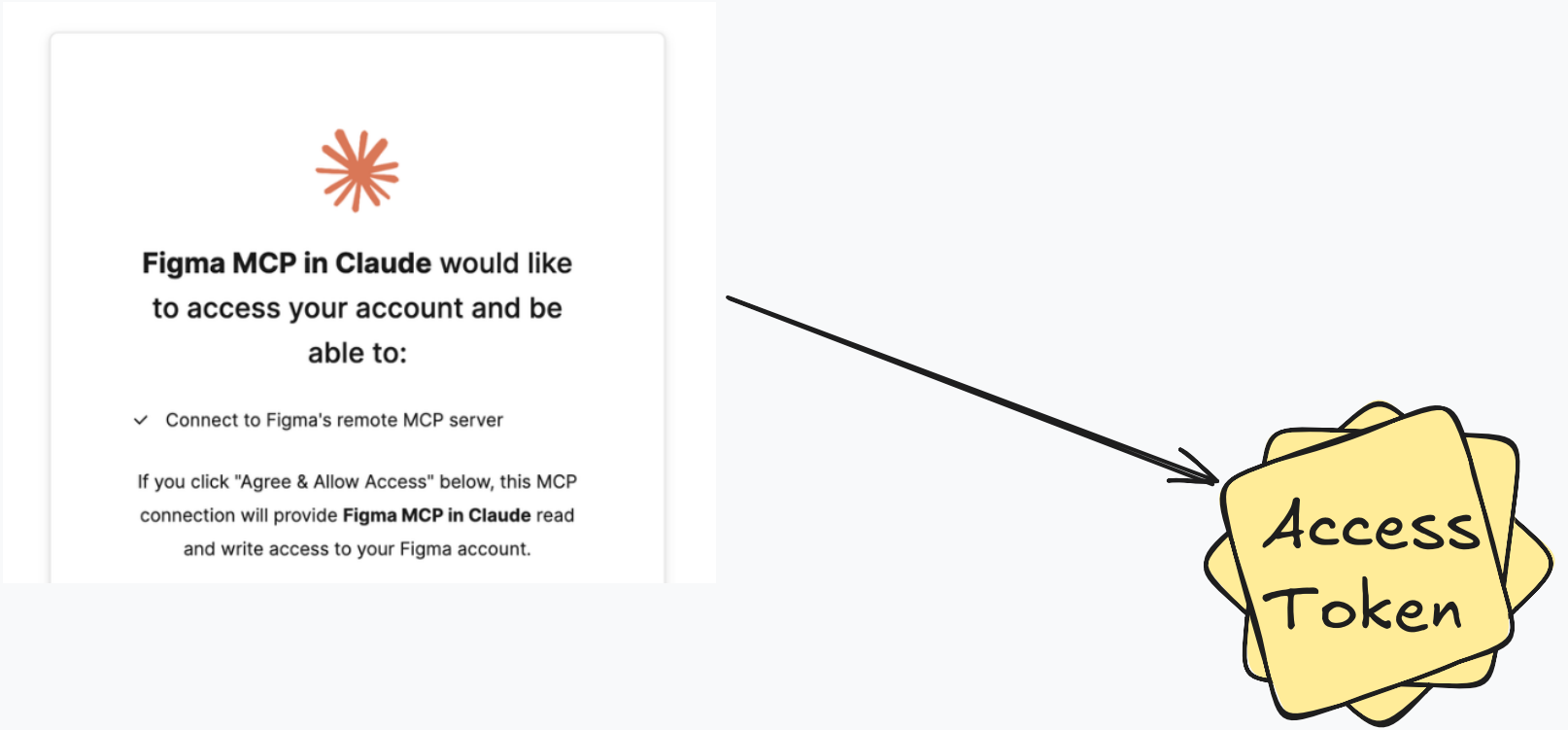
Copy page

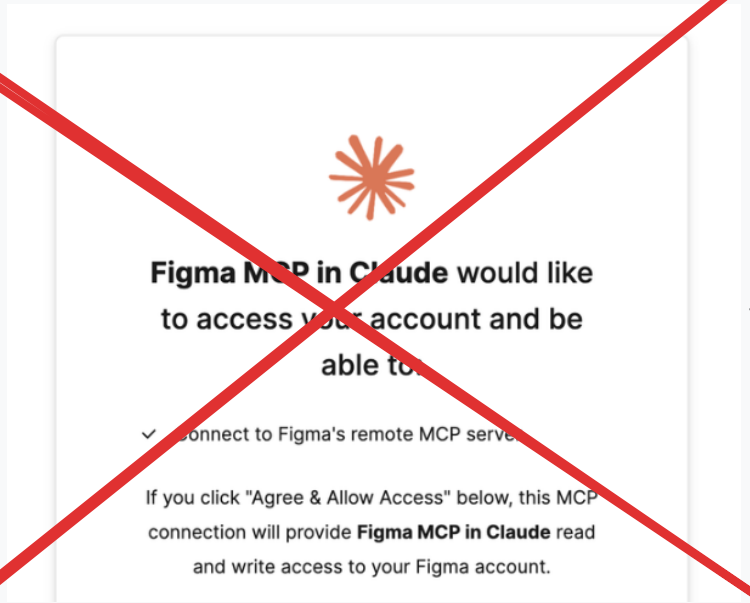
Centralized access control for MCP in enterprise environments via identity providers

The Enterprise-Managed Authorization extension (`io.modelcontextprotocol/enterprise-managed-authorization`) enables organizations to control MCP server access centrally through their existing identity provider (IdP). Instead of each employee authorizing each MCP server individually, the organization's IT or security team manages access policies in one place.

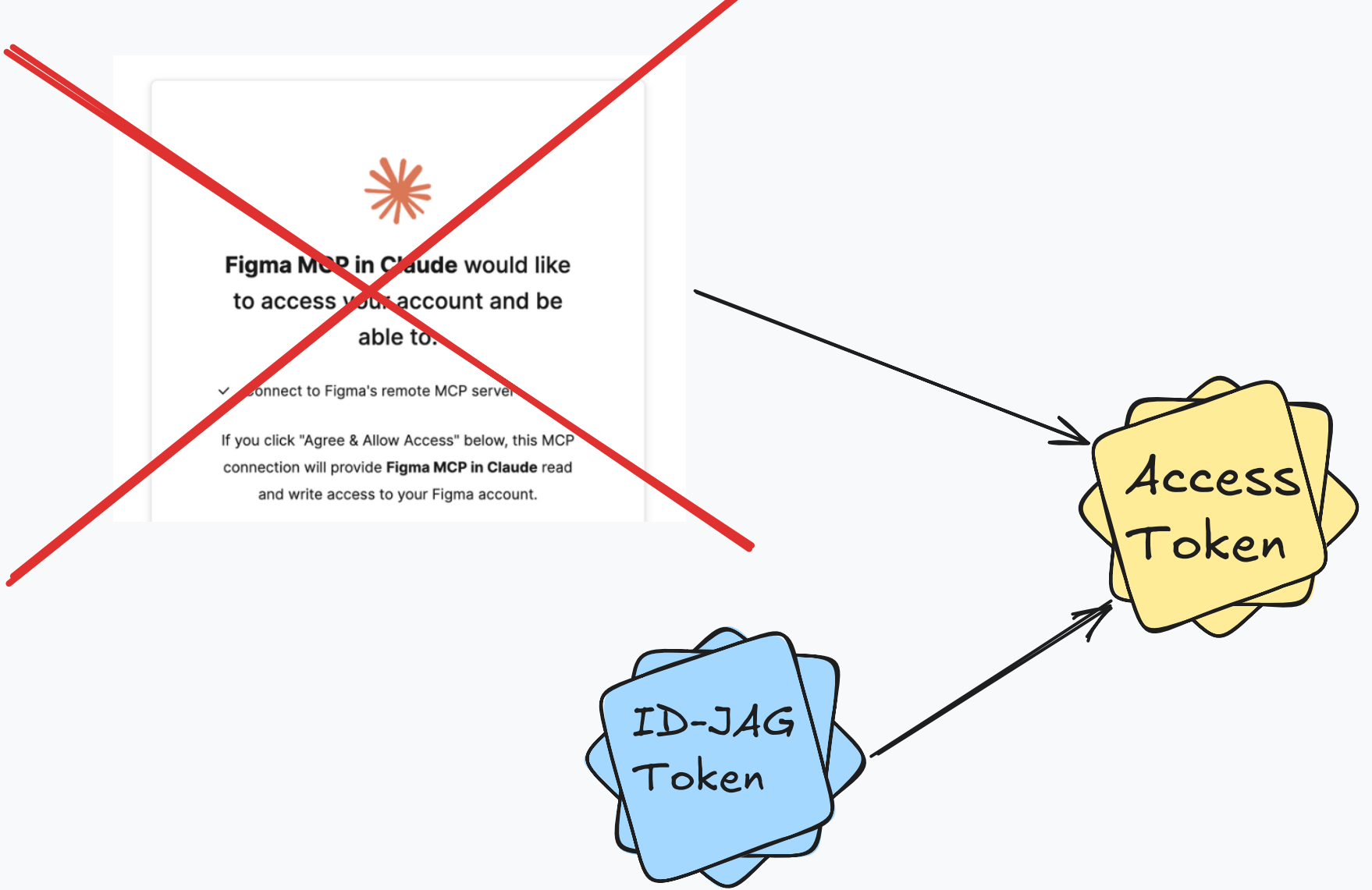
Specification

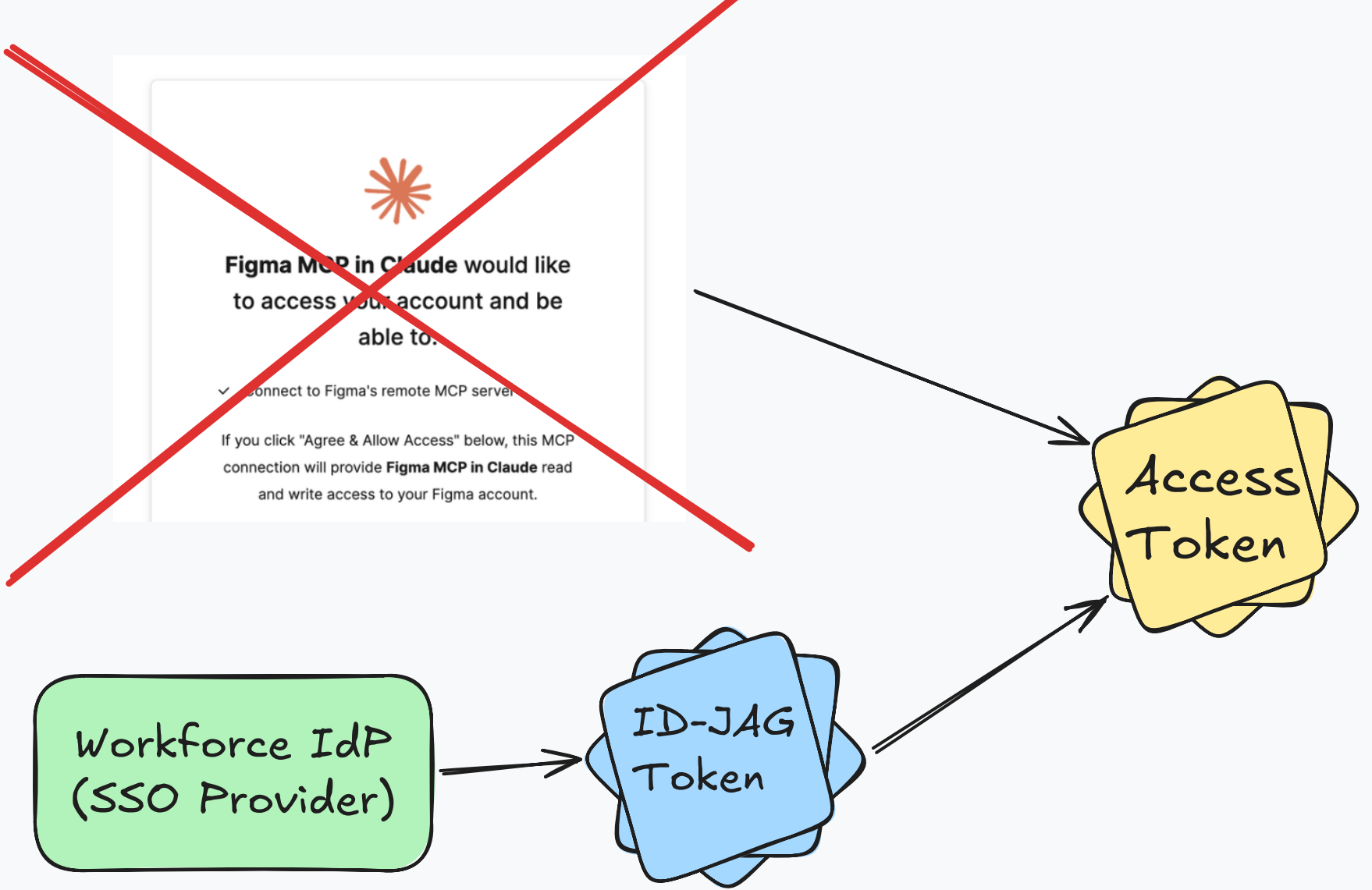
Full technical specification for the Enterprise-Managed Authorization extension.


Figma MCP in Claude would like to access your account and be able to:
Connect to Figma's remote MCP server
If you click "Agree & Allow Access" below, this MCP connection will provide Figma MCP in Claude read and write access to your Figma account.
Access Token

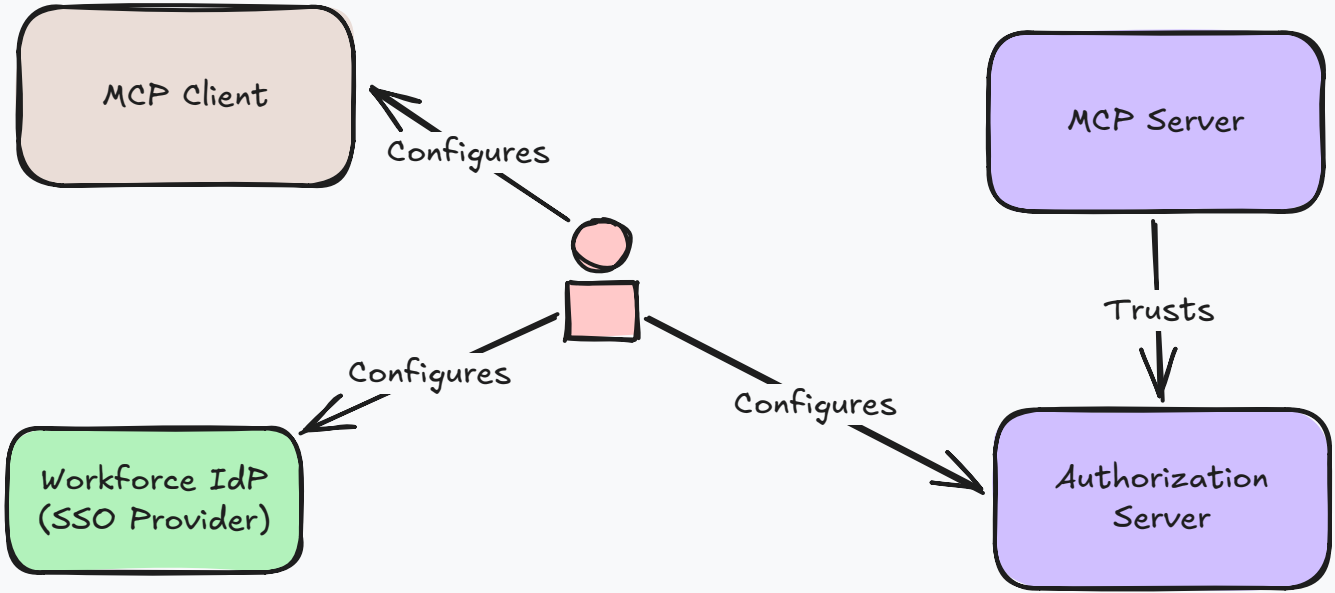

Figma MCP in Claude would like
to access your account and be
able to:
Connect to Figma's remote MCP server
If you click "Agree & Allow Access" below, this MCP connection will provide Figma MCP in Claude read and write access to your Figma account.

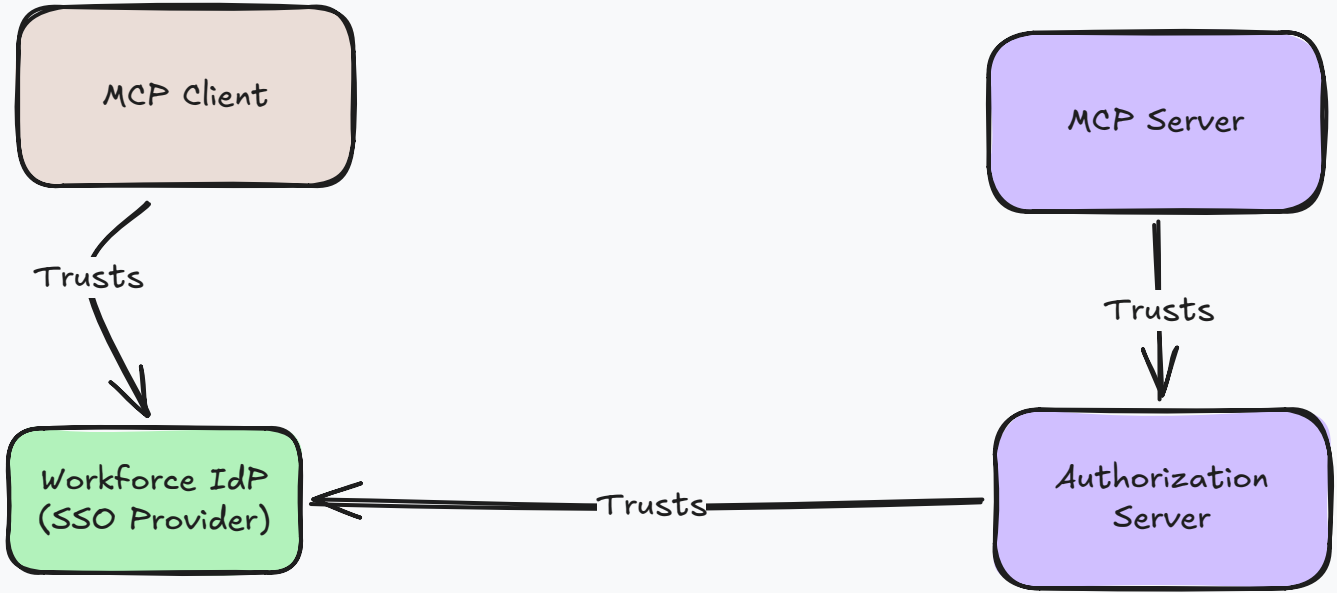

Access Token

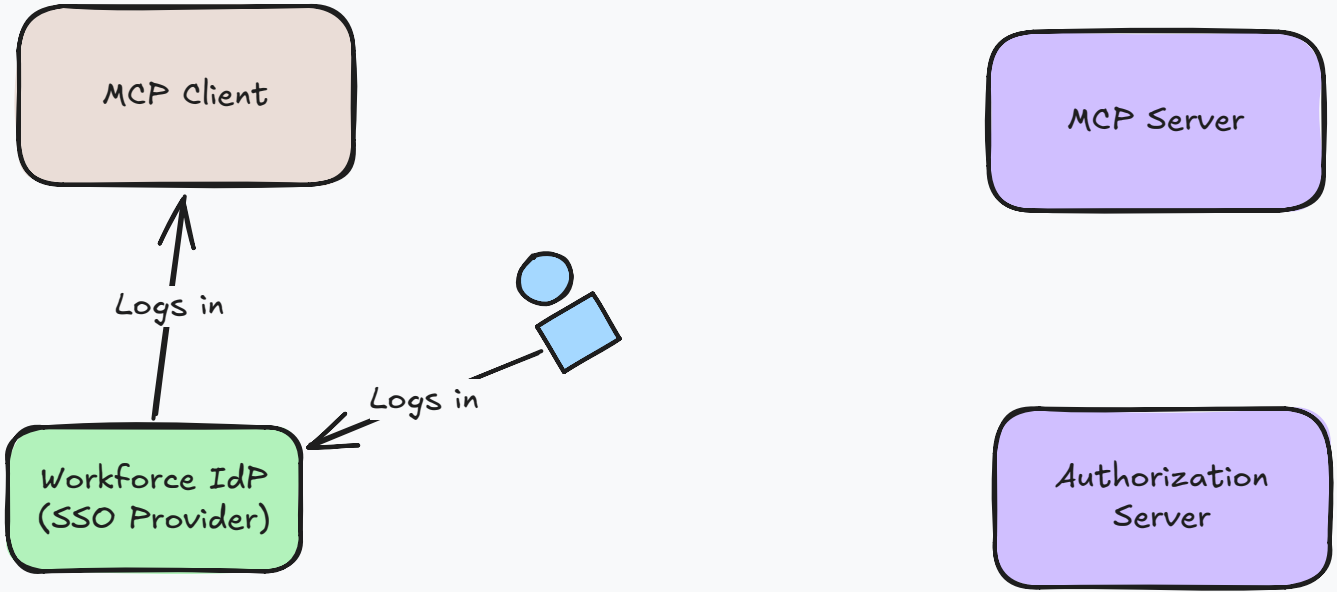

Figma MCP in Claude would like
to access your account and be
able to:
Connect to Figma's remote MCP server
If you click "Agree & Allow Access" below, this MCP connection will provide Figma MCP in Claude read and write access to your Figma account.
Access Token
ID-JAG Token


Figma MCP in Claude would like to access your account and be able to:
Connect to Figma's remote MCP server
If you click "Agree & Allow Access" below, this MCP connection will provide Figma MCP in Claude read and write access to your Figma account.
Access Token
Workforce IdP (SSO Provider)
ID-JAG Token

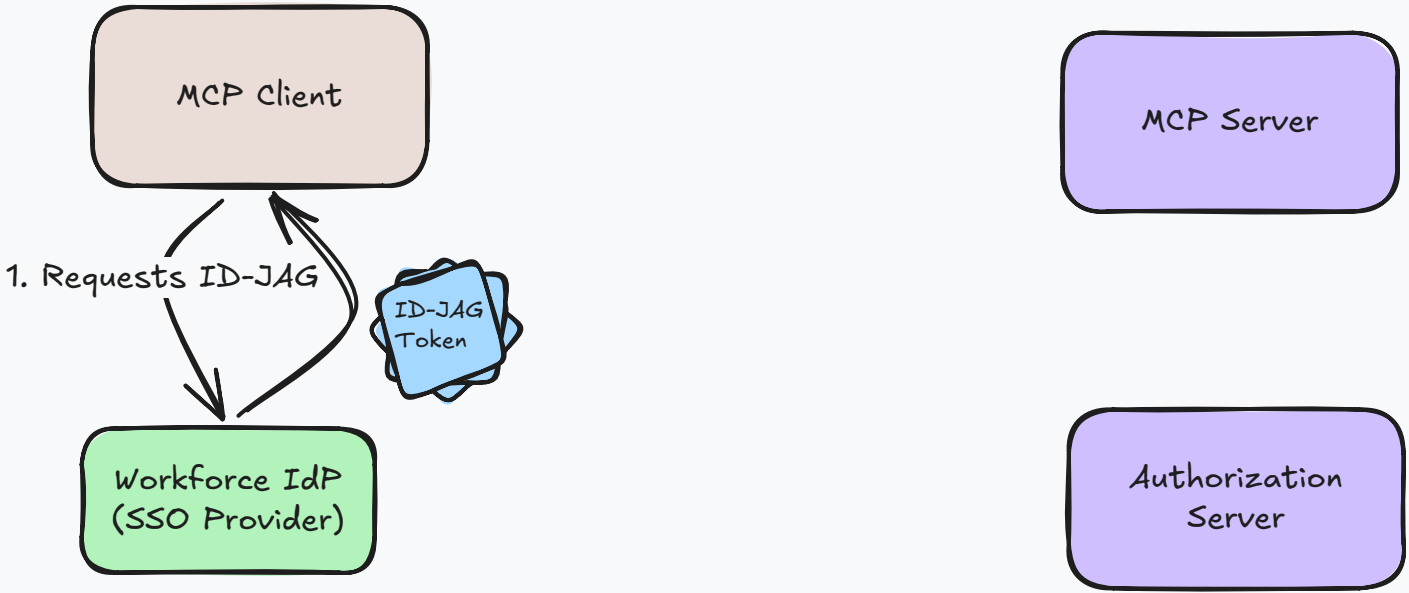

Workforce IdP
(SSO Provider)
admin@example

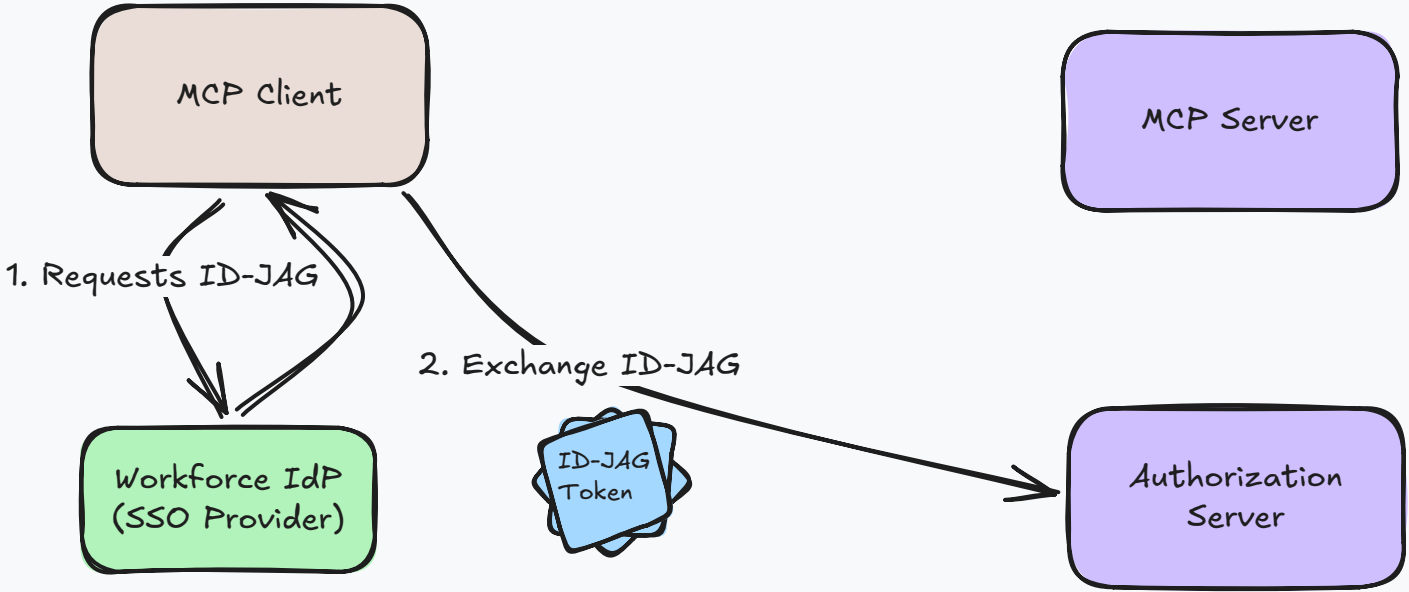

MCP Client
Configures
MCP Server
Trusts
Configures
Configures
Workforce IdP
(SSO Provider)
Authorization
Server

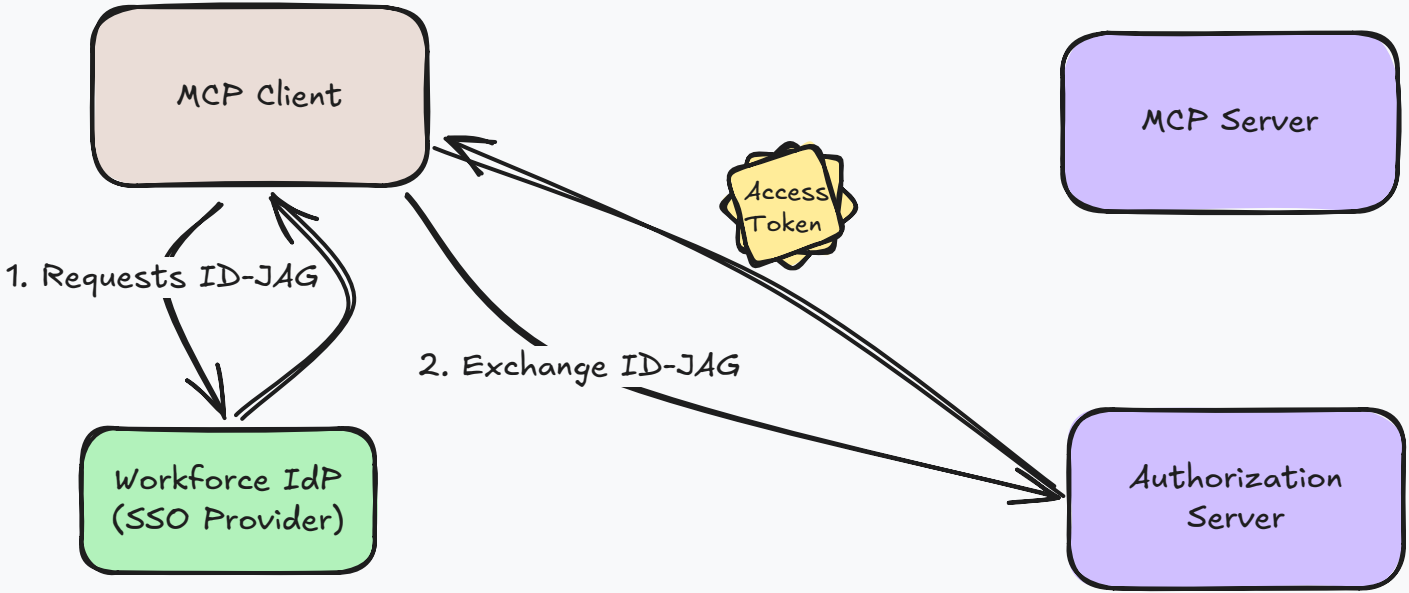

MCP Client
MCP Server
Trusts
Trusts
Workforce IdP
(SSO Provider)
Trusts
Authorization
Server

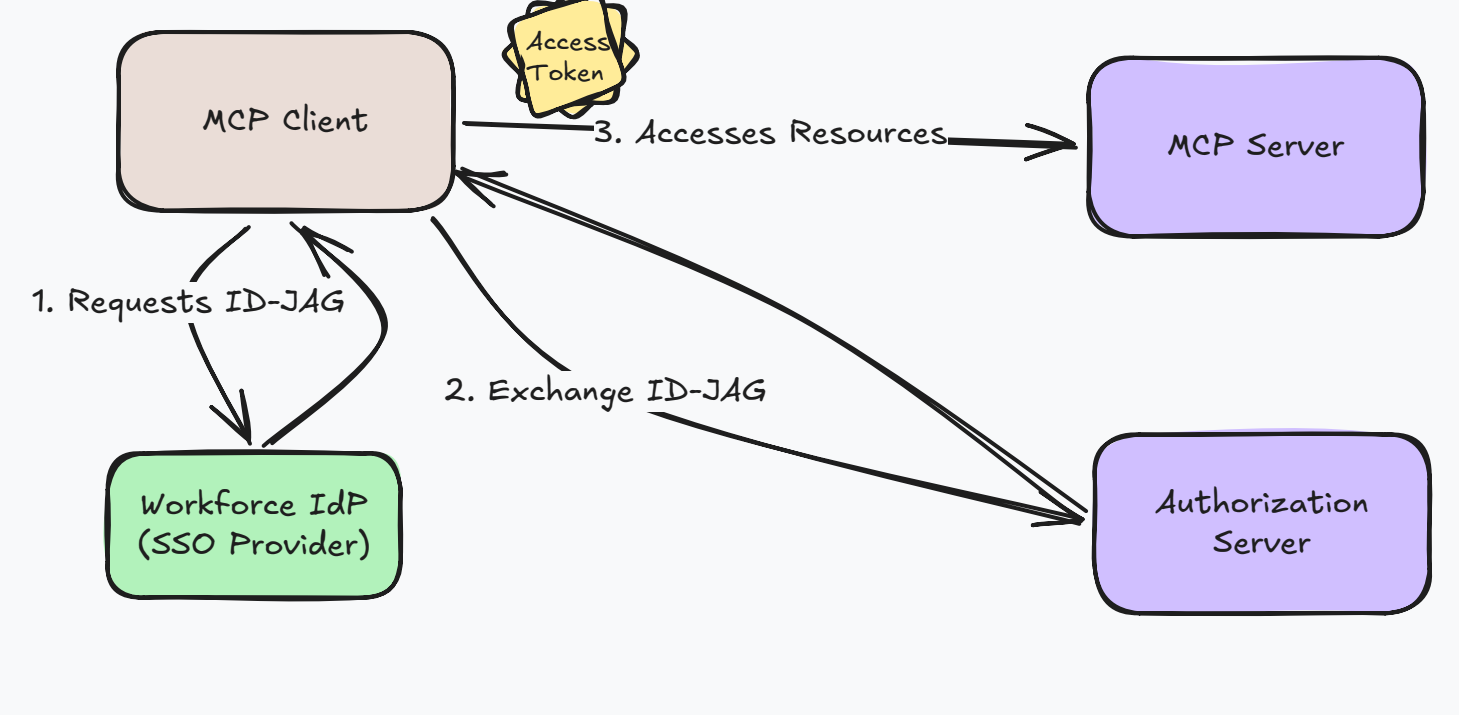

MCP Client
MCP Server
Logs in
Logs in
Workforce IdP
(SSO Provider)
Authorization
Server

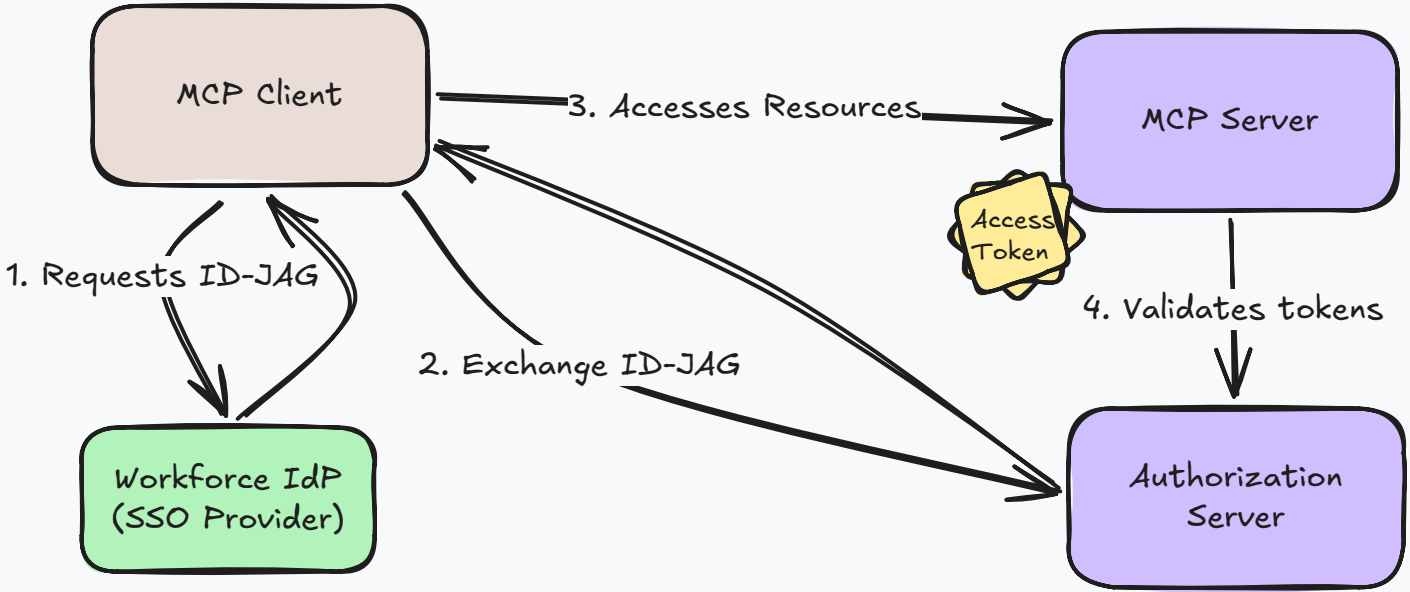

MCP Client
MCP Server
1. Requests ID-JAG
Workforce IdP
(SSO Provider)
Authorization
Server

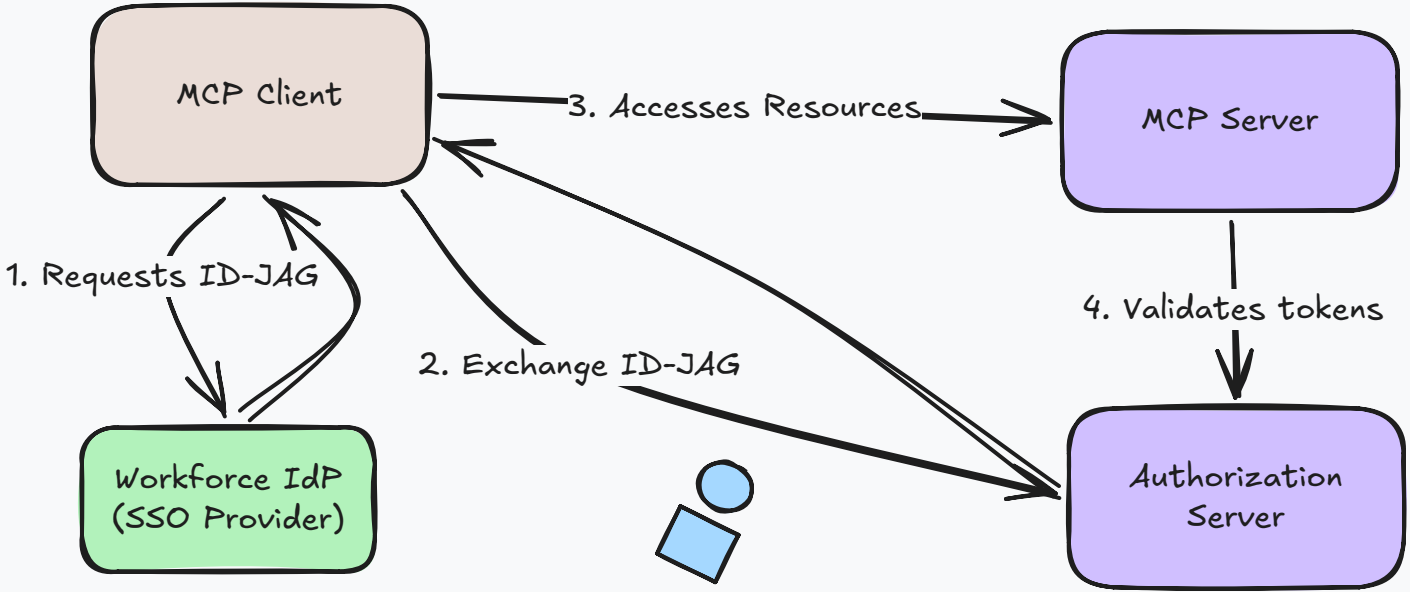

MCP Client
MCP Server
1. Requests ID-JAG
ID-JAG Token
Workforce IdP (SSO Provider)
Authorization Server


MCP Client
MCP Server
1. Requests ID-JAG
2. Exchange ID-JAG
Workforce IdP
(SSO Provider)
ID-JAG
Token
Authorization
Server


MCP Client
MCP Server
Access Token
1. Requests ID-JAG
2. Exchange ID-JAG
Workforce IdP (SSO Provider)
Authorization Server


MCP Client
Access Token
3. Accesses Resources
MCP Server
1. Requests ID-JAG
2. Exchange ID-JAG
Workforce IdP (SSO Provider)
Authorization Server


MCP Client
3. Accesses Resources
MCP Server
Access Token
1. Requests ID-JAG
4. Validates tokens
2. Exchange ID-JAG
Workforce IdP (SSO Provider)
Authorization Server


MCP Client
3. Accesses Resources
MCP Server
1. Requests ID-JAG
4. Validates tokens
2. Exchange ID-JAG
Workforce IdP
(SSO Provider)
Authorization
Server
Look ma, no hands!

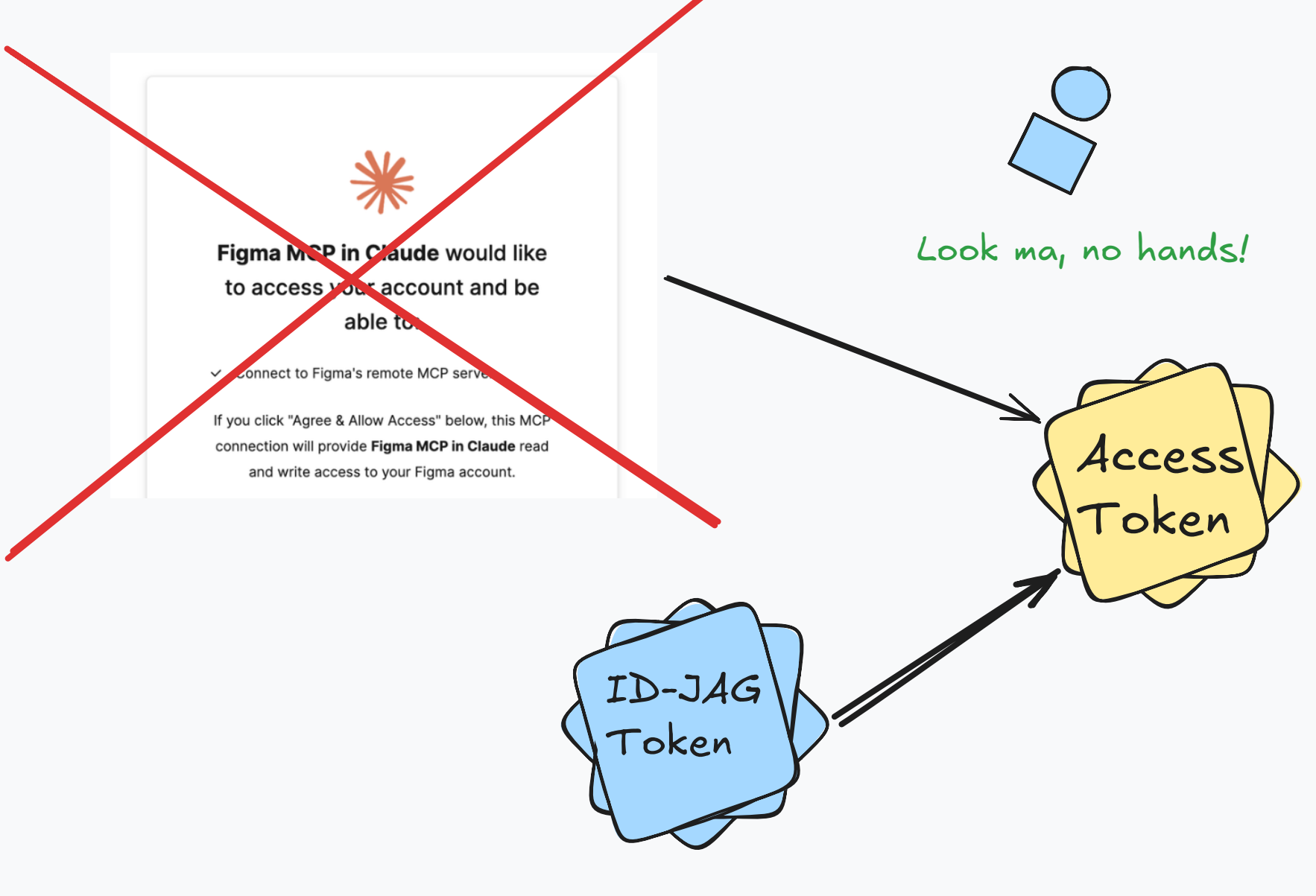
Demos!

Problems with identity today:

- Friction

Problems with identity today:

~~- Friction~~

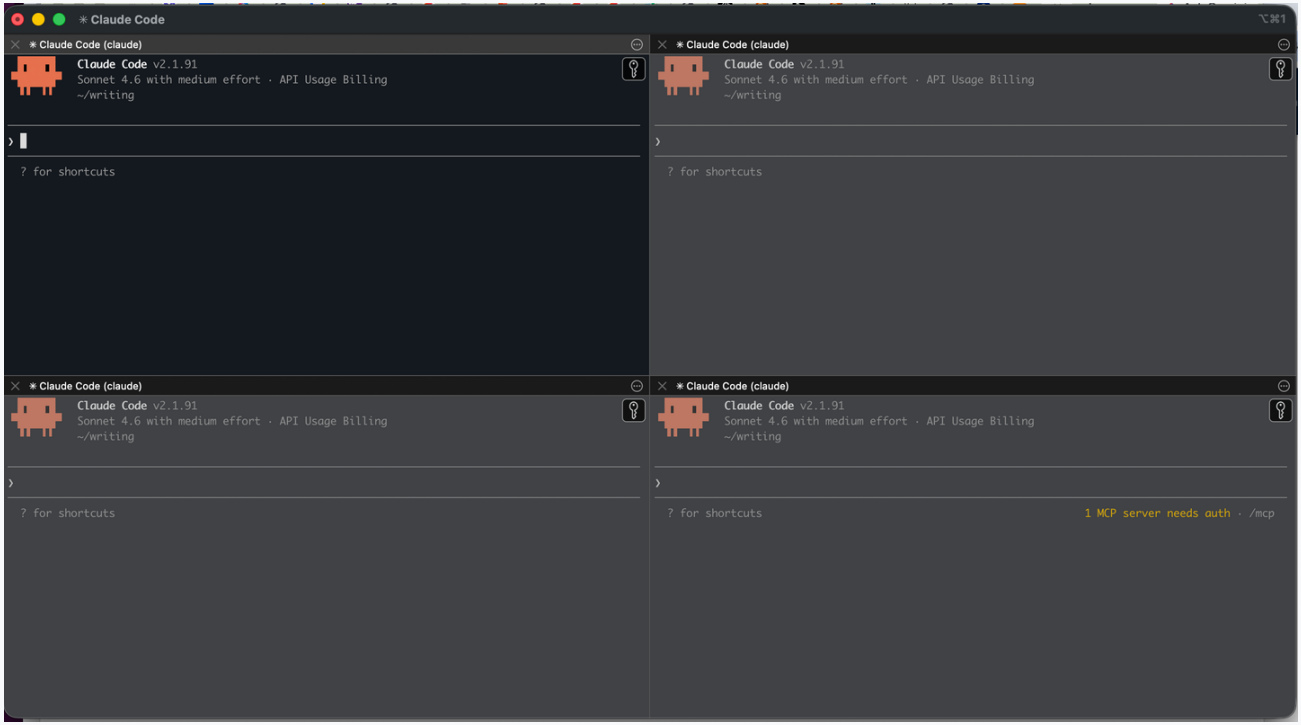

Figma MCP in Claude would like
to access your account and be
able to:
Connect to Figma's remote MCP server
If you click "Agree & Allow Access" below, this MCP connection will provide Figma MCP in Claude read and write access to your Figma account.
Look ma, no hands!
Access Token
ID-JAG Token

Problems with identity today:

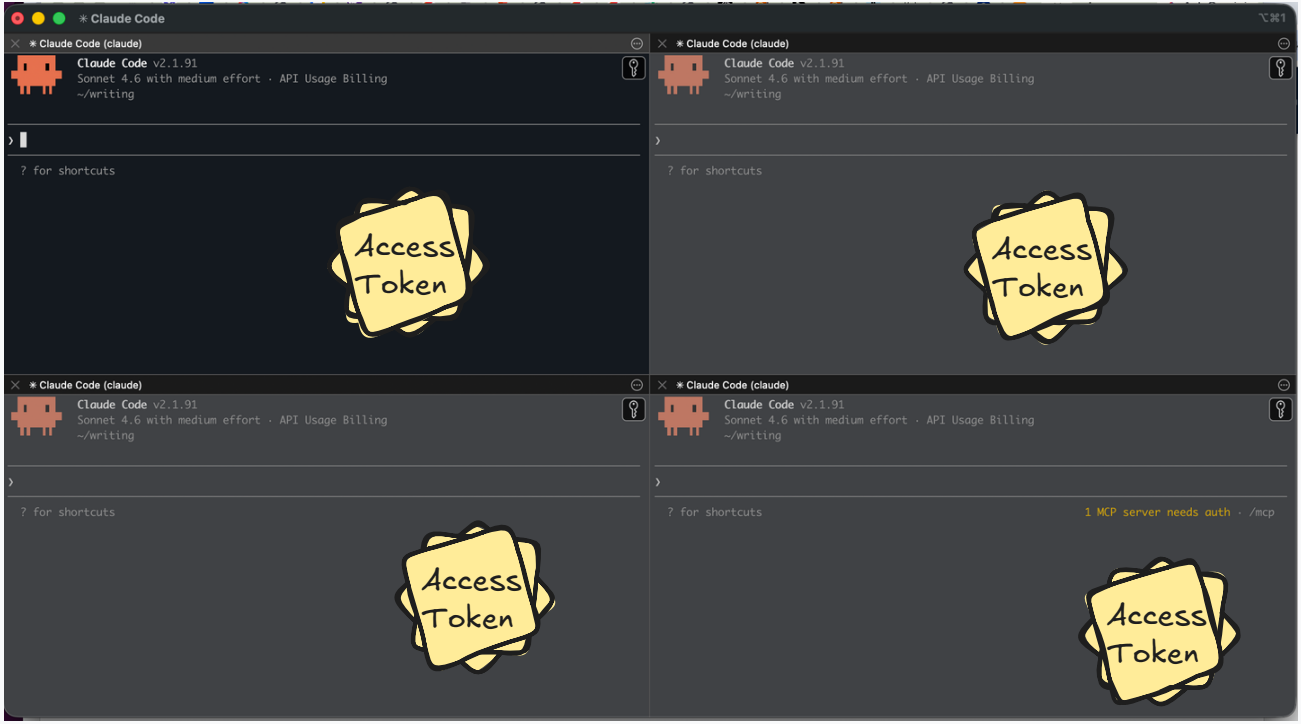
- ~~Friction~~

- Attribution

Per-conversation access tokens



Per-conversation access tokens



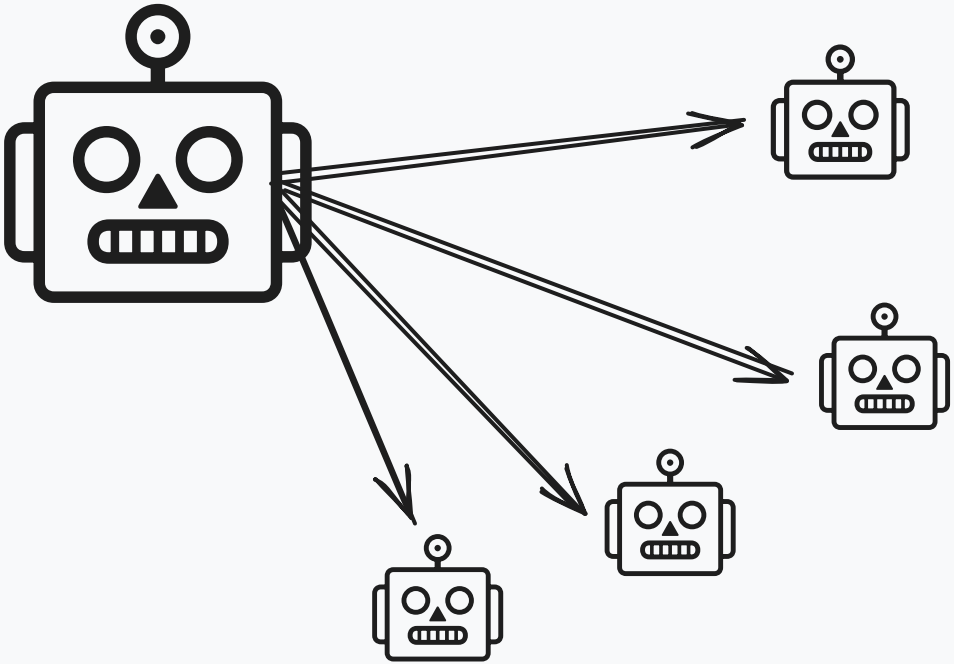
Problems with identity today:

- ~~Friction~~

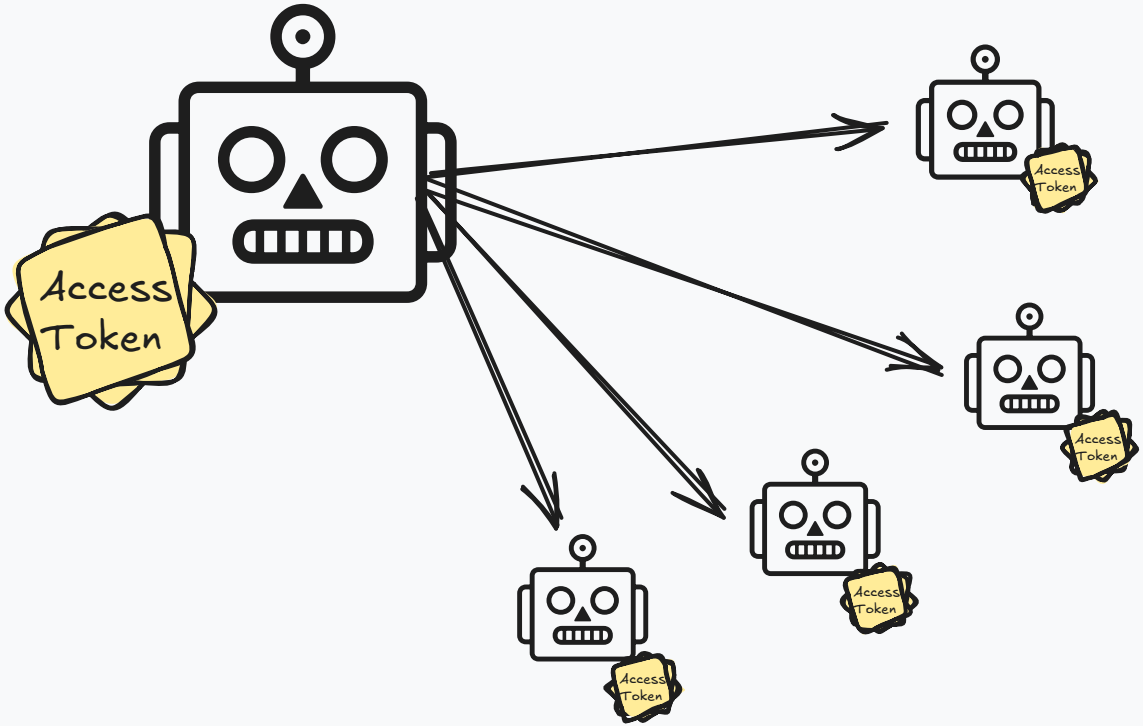
- Attribution

- Specificity

Downscoped access tokens for subagents



Downscoped access tokens for subagents



Takeaways

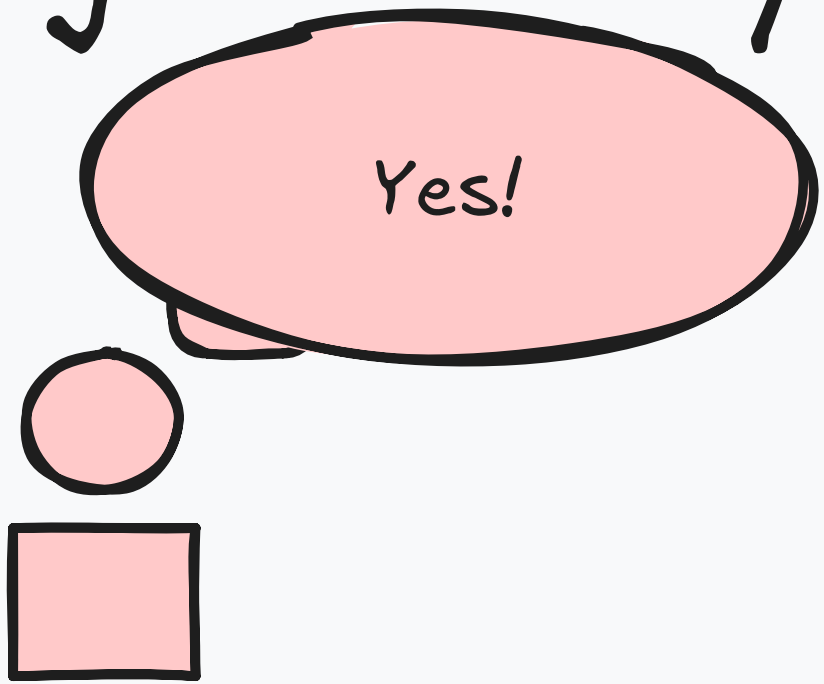
- One login, access to everything IT approved
- No more per-server OAuth flows for end users
- IT Admin gets central visibility, policy control, and revocation
- XAA unlocks more identity improvements in the future

Ask your IT Admin

Is xAA right for you?

Ask your IT Admin

Is xAA right for you?



admin@example

Resources + Questions

MCP Enterprise Auth docs

XAA.dev