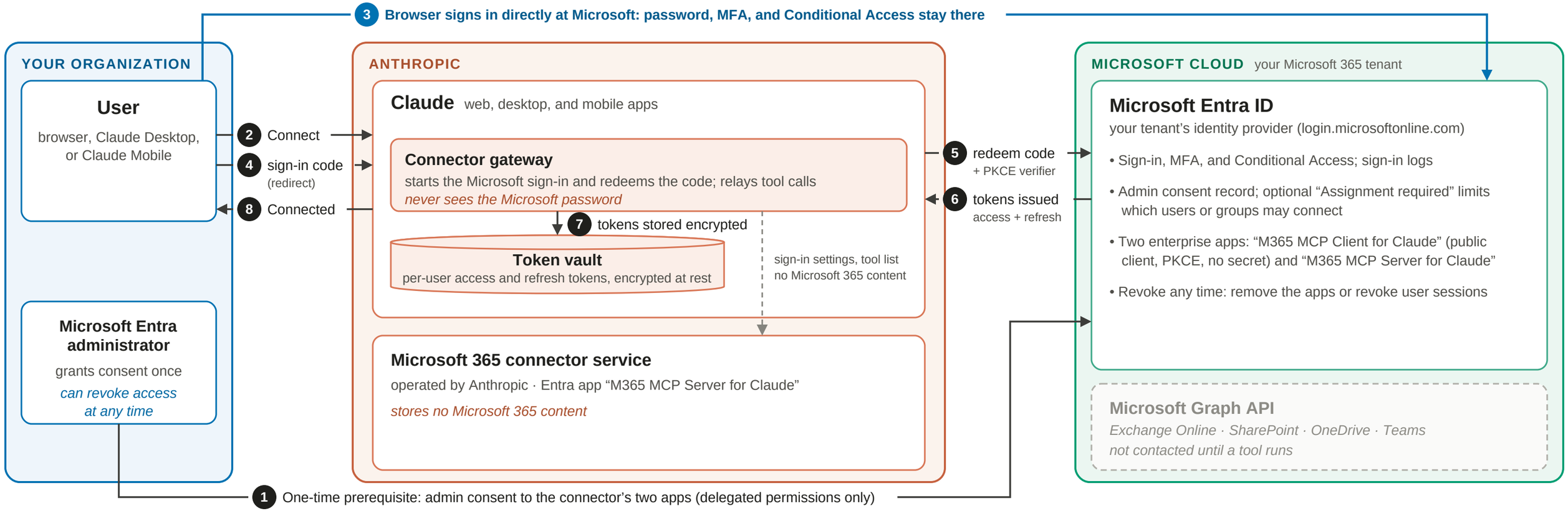
Microsoft 365 connector for Claude: how a user connects

One-time admin consent, then each user signs in at Microsoft. Anthropic receives tokens, never the password; no Microsoft 365 content is read yet.



What happens at each step

request / response · your user's browser, direct to Microsoft (not through Anthropic) · supporting exchange · not contacted in this view

1. Admin grants tenant-wide consent once: delegated permissions only, no application (app-only) permissions.
2. User clicks Connect in Claude.
3. Browser signs in at Microsoft (authorization code with PKCE); MFA and Conditional Access enforced and logged there.
4. Microsoft redirects the browser to claude.ai with a single-use sign-in code (the OAuth authorization code), not a token.
5. Gateway redeems the code server-to-server with its PKCE (Proof Key for Code Exchange) verifier; no client secret.
6. Entra ID issues an access token (connector-only audience, 60–90 minutes, set by Microsoft) and a refresh token.
7. Tokens stored encrypted, scoped to this user and organization; used only on this user's behalf.
8. Claude shows "Connected"; no Microsoft 365 content is read until a tool runs.

Claude asks the connector where users sign in and, once connected, loads its tool list; no content is read.

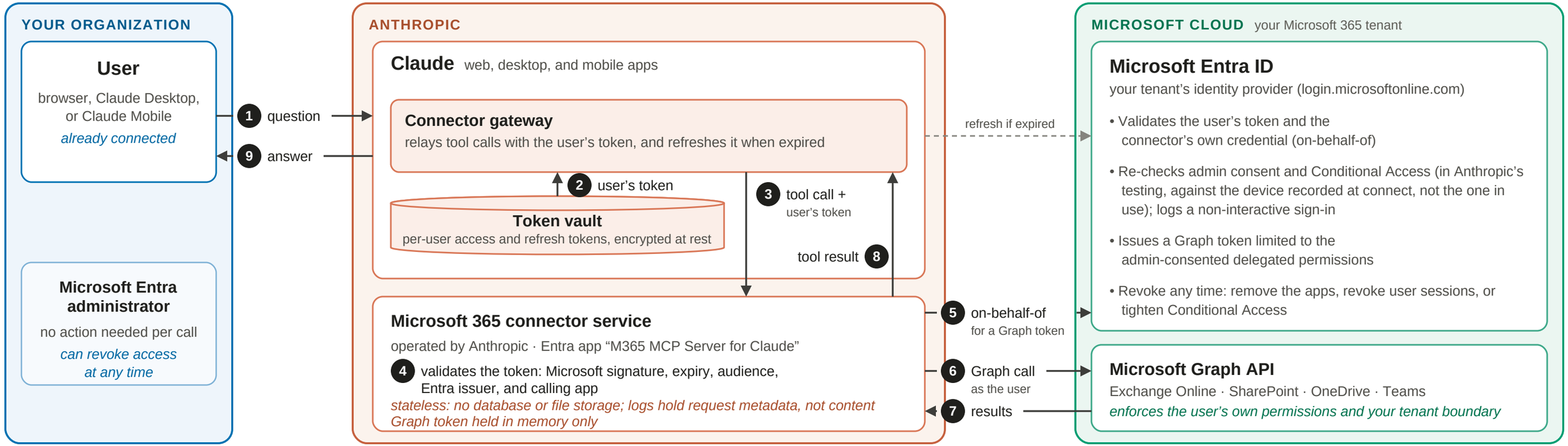
Key facts for security review

- **Delegated only:** Claude reaches only what the signed-in user can already open in Microsoft 365.
- **Conditional Access:** In Anthropic's testing, Entra ID evaluates the connector's server-side token requests as coming from Anthropic's published IP range and carrying the device recorded when the user connected, not the device or network in use at each tool call.

For the latest, see the Microsoft 365 connector security guide

Microsoft 365 connector for Claude: what happens on each tool call

Each call runs as the signed-in user with a short-lived Graph token; the connector keeps no Microsoft 365 content.



What happens at each step

request / response — supporting exchange (token refresh)

1. User asks for something that needs Microsoft 365 data; Claude calls a connector tool.
2. Gateway loads the user's token from the vault and refreshes it at Entra ID if expired.
3. Gateway sends the tool call and the user's token over HTTPS.
4. Connector validates the token: Microsoft signature, expiry, audience, Entra issuer, and calling app.
5. On-behalf-of: Entra ID re-checks consent and Conditional Access; issues a user-scoped Graph token (memory only).
6. Connector calls Microsoft Graph as the user.
7. Graph enforces the user's permissions and tenant boundary and returns content.
8. Connector returns the extracted text to Claude; the connector's logs hold metadata, not content.
9. Claude uses the tool result to answer the user.

Key facts for security review

- **Tokens:** Access and Graph tokens are short-lived (lifetimes set by Microsoft Entra ID); the refresh token lasts until it expires under your policy or is revoked.
- **Tool results** become part of the user's Claude conversation and are retained under your organization's Claude retention settings.