

Nov 26, 2025

- Attendees
 - tadas@tadasant.com
 - adamj@anthropic.com
 - Radoslav Dimitrov
 - toby@github.com
 - BobDickinson
 - [public]
- Agenda
 - [BobDickinson] Validation work

Nov 19, 2025

- Attendees
 - tadas@tadasant.com
 - adamj@anthropic.com
 - Radoslav Dimitrov
 - ~~toby@github.com~~
 - ~~[public]~~
- Agenda
 - BobDickinson's validation work
 - [Discussion](#)
 - [Tadas] I think this all makes sense, except I'm inclined to push for TypeScript as a source of truth instead of building out a more complex JSON schema object
 - This does mean refactoring our generation flows to start with TypeScript, generate JSON, and *then* generate OpenAPI. We currently define OpenAPI and then generate JSON from there. Would also be an opportunity to get rid of the manually-maintained server.json-related Go structs (`pkg/api/v0/types.go`)
 - [PR 1](#)
 - [PR 2](#)
 - Opinions:
 - Aligned that TS as a source of truth sounds like a good idea
 - Unclear what the gaps might be in translating TS <> JSON schema
 - Otherwise, Bob's ideas make sense in concept
 - Would be good to hear the vision directly from Bob before fully greenlighting all the work

- TODOs: schedule meeting with Bob, perhaps do TS investigation beforehand?
- Searching by type: <https://github.com/modelcontextprotocol/registry/pull/787>
 - All agreed that this is a useful feature
 - Tadas has concerns about introducing this one-off for **type** vs. something more generic ([extreme counter-example](#))
 - TODO: Tadas to review and write up thoughts async
- ~~Next public meeting in 2 weeks (TODO: add it)~~
 - Let's do public meeting next week since we messed up the Gmeet this week
 - TODO: Set up a new Gmeet with public access

Nov 12, 2025

- Attendees
 - tadas@tadasant.com
 - adamj@anthropic.com
 - Radoslav Dimitrov
 - toby@github.com
- Agenda
 - Inspector V2 and server.json validation
 - AI: Radoslav Dimitrov to ping Konstantin (or others from the Inspector community)
 - Next meeting public
 - meet.modelcontextprotocol.io
 - Server cards
 - BobDickinson's Schema validation
 - <https://github.com/modelcontextprotocol/registry/pull/636>
 - <https://github.com/modelcontextprotocol/registry/pull/630>
 - AI: all have an opinion on this by next week
 - Delete (and Update) endpoint on standardized sub-registry spec. Not implemented in public registry.
 - Agreed we should add this to spec.
 - Should we have publication origin / provenance in server metadata so that federated sub-registries can surface/filter that piece of data when querying
 - Adam: not usually a problem in practice due to **name**; but currently putting it in `_meta`
 - Rado: use case - same name, different source registry (e.g. GitHub server in two different registries; we trust one more than the other)
 - Long form async Issue

Nov 5, 2025

- Attendees
 - tadas@tadasant.com
 - adamj@anthropic.com
 - Radoslav Dimitrov
 - toby@github.com
- Agenda
 - Auth spec in the Registry?
 - Could we re-use OAuth from the MCP spec?
 - Tadas to write issue for someone to pick up
 - Harald, VS Code etc can provide feedback?
 - Easier testing of server.json (e.g. for semantic issues like misspelled env vars).
Ideas:
 - Add server.json support in MCP inspector?
 - Local registry with 1 server?
 - Pitch into V2 inspector effort
 - [SEP-1649 Server Cards](#)
 - Include packages
 - Dynamic resources
 - Doc link:
https://docs.google.com/document/d/13fVsxAeRWgHzG6XXcH_Ouh-0sMsk0t93AgUkOctap7g/edit?tab=t.0
 - [Reverse DNS discussion](#)
 - API version goals
 - v1 would have the result of SEP-1649
 - Would we preserve v0.1? Migrate existing data?
 - Integration updates
 - [adam] other things for registry
 - Registry web UI
 - Registry MCP server
 - → A way to get comfortable with avoiding scope creep: make it clear the target audience here is *publishers*, not agentic consumers trying to find MCP servers to *use*.

Oct 29, 2025

- Attendees
 - ~~tadas@tadasant.com~~
 - adamj@anthropic.com
 - Radoslav Dimitrov
 - ~~toby@github.com~~
- Agenda

- Claude was broken
- Release + promo

Oct 22, 2025

- Attendees
 - tadas@tadasant.com
 - adamj@anthropic.com
 - Radoslav Dimitrov
 - toby@github.com
- Agenda
 - Meeting logistics:
 - ~~Move 30 mins earlier?~~
 - Allow public joiners? Get it on the WG meeting calendar?
 - Biweekly?
 - **Tadas to set this up**
 - **Freeze announcement**
 - **Rado to announce on Discord/LinkedIn/X, Adam to help propagate**
 - MCPB Version
 - Windows OS. Envisions downloading them.
 - GA
 - Server Cards
 - New stuff? tools, authentication?
 - Tools would be good to include
 - MCP Foundation / resourcing for SLA?
 - WIP
 - Security
 - Rado to ping Jim (Docker)
 - Adam can sign up for Docker pro if needed

Oct 13, 2025

- Attendees
 - tadas@tadasant.com
 - ~~adamj@anthropic.com~~
 - Radoslav Dimitrov
 - Thomas Sickert
 - ~~toby@github.com~~
- Agenda
 - What's left for API freeze?
 - Aligned that this is just no breaking changes vs. no changes at all?
 - V0.1 means no breaking changes, but additive changes (with a patch bump) are fine

- V0.1 change
 - Let's just point to both. Let's just have them both do 200's.
 - Plan: keep running v0 and v0.1 as the same shape. Don't make any breaking changes to either.
 - When we decide we need to make a breaking change (or go GA), we decide at that point whether or not we want to continue supporting serving the v0.1 shape.
 - We consider the v0 endpoint a sort of "draft" that is liable to change whenever. V0.1 is
- Anything else?
- What will it take for GA? Vs. what is post-GA?
 - V1.0 (v1.3?)
 - SLA? Foundation-funded on-call?
 - SEP for server.json?
 - Backwards compatibility story so we can make changes iteratively
 - A few verified sub-registry integrations and at least one major client using it in production?
 - How do we encourage convergence on e.g. `oci` and not `docker` in ecosystem?
 - Encoded in schema?
 - Best practices docs?
 - Something else?
- Managed vs non-managed PSQL
 - Database replication from prod to staging
- Reference Server.json schema discussion
 - How opinionated do we want to be there?
 - Decide good middleground for the freeze and address the rest as follow ups

Oct 6, 2025

- **Attendees**

- ☐ ~~tadas@tadasant.com~~
- ☐ adamj@anthropic.com
- ☐ Radoslav Dimitrov
- ☐ toby@github.com

- **Agenda**

- ☒ Should we create #registry-wg-security private channel?
- ☐ Tasks to complete for the freeze at Oct, 10th
 - Format-related
 - Add
 - Title

- Icon: copy whatever is in the main MCP spec into the top level - think this is a list
 - List of tools: experiment with this in publisher provided `_meta` for now (can also put in prompts, resources, elicitation etc.) until we agree/standardise on this
- Update the oci-specific package type (to be single-line reference vs split across multiple properties)
- Remote URL templating (talked to leave it for later or perhaps do it now?)
- Other community-raised questions
- API-related
 - All good?
 - Delete GET `/v0/servers/{serverName}` - Get latest version of server by server name (URL-encoded), as can be done with GET `/v0/servers/{serverName}/versions/latest`
- Implementation details
 - Split jsonb into separate columns
- ☐ CI validation for:
 - Schema changes should result in new version
 - Do not mess up old migrations
- **Action Items**
 - ☐ Copy db state from Prod to Staging
 - ☐ Adam: Add icon
 - ☐ Adam: Drop unnecessary API endpoint
 - ☐ Rado: oci-specific package type
 - ☐ Tadas(?): finish the remote URL templating PR
 - ☐ Toby: Review Bob's PR related to format changes and see if there's other similar ones raised too
 - ☐ Update the publisher init command to allow for easy vendor initialization (i.e. include github's publisher extensions, etc)

Oct 2, 2025

- title
 - Put it in the server.json
- Icon
 - Take the shape from the current MCP spec (the sizes changed in the last week, but hopefully it's close to stable)
 - Put it in `_meta["io.modelcontextprotocol.registry/publisher-provided"]`, likely eventually we lift it into the server.json
 - Probably ok to just put it in server.json out the gate to minimize churn
- Static tool definitions
 - Enumerate all the possible ones?

- Could the registry pull back data from e.g. Anthropic, OpenAI
 - Skepticism that this is a proper comprehensive security solution
 - More compelling to do this from the “discovery” angle benefit
 - In this case, maybe not necessary to enumerate *everything*
- How do we notify sub-registries of changes?
 - RSS? ActivityPub? Webhooks?
 - Simpler/short-term: updatedSince property
 - Md5 the name?
 - Problem: What do we do about illegal content in *name*? How would we signal deletion?
 - Full table scan? Hard on our infra.
 - Second endpoint? Quite complex.
 - Long term: some ActivityPub-like thing?
 - **Hacky solution: email everyone the one time (if ever) it happens to our list of people interested in API updates**
 - Could we do an RSS feed?

Sep 29, 2025

- ~~● Rado permissions for registry wg~~
- CVE?
- Maybe missing something but I think we should decline this:
 - <https://github.com/modelcontextprotocol/registry/pull/511>
 - Let's clarify docs to make it clear we support closed source, but not private
 - Rado is on this. Filed - [#573](#)
- Remaining list of breaking changes
 - Rado's PR <https://github.com/modelcontextprotocol/registry/pull/562>
 - UUIDs
 - To remove or keep as secondary option?
 - We need “where to go” in the deprecated case
 - `_meta` lift / `server.json` immutability
 - We have a number of snake_case properties on <https://registry.modelcontextprotocol.io/openapi.json>
 - We should not have snake case anywhere in the openapi.json
 - Follow on PR
 - Radoslav Dimitrov - Fixed
 - Potentially:
 - <https://github.com/modelcontextprotocol/registry/issues/394#issuecomment-3346845895>
 - Need to review this - figure out if it'd be a non-breaking change
 - Go through backlog and decide if anything is a blocker for a freeze
 - ~~○ Provider metadata beyond namespace?~~
 - ~~○ MCP client modeling?~~
- Preview mode integration status

- PulseMCP
 - ToolHive
- Prioritization of docs refactor
- What are the blockers to GA
- Maintainer meeting timing – 30 min earlier?