

## Oct 9, 2026 | 📅 MCP: Files Upload/DL Working Group

Attendees: Kurtis Van Gent paris@openai.com tsarlandie@openai.com kvg@google.com  
den@anthropic.com ariagno@google.com claude@modelcontextprotocol.io  
patrick.rodgers@microsoft.com ~~stcharles@google.com~~

### Notes

- 

### Action items



---

## Oct 2, 2026 | 📅 MCP: Files Upload/DL Working Group

Attendees: ariagno@google.com den@anthropic.com kvg@google.com Kurtis Van Gent  
paris@openai.com patrick.rodgers@microsoft.com stcharles@google.com  
tsarlandie@openai.com

### Agenda:

- **Goal for the meeting:**
  - Crisply define the problem that we want to solve in this working group.
  - [Stretch goal] Identify blocking problems with the current proposal so we can start to iterate on a solution.
- Logistics
  - Meeting is recurring in this time slot now
  - Notes will live in this doc for now
  - Merging with filesystem WG?
    - Working from the same umbrella, but can work a little separately
- Cover CUJs from WG members
- Feedback on hard blockers on existing SEP-2631 proposal
- Specific Client Requirements
- What is in-scope for the Working Group?
- High-level Steer
  - Smallest solution that solves the in-scope problem
  - Should cleanly coexist with existing and pending MCP spec changes
- Design Discussion if time allows
- Next steps and wrap up
  - Wil St. Charles is OOO next Friday, so do we want to cancel the next instance or does someone else want to run it?

## Feedback:

- Cover CUJs from WG members
  - Google
    - A user asks Claude or ChatGPT to save a 40 MB PDF they attached in chat to a Drive folder.
    - An agent pulls a 200 MB CSV from Drive into its code sandbox to analyze it.
    - An agent uploads a 50 MB deck it generated as a new revision of an existing Drive file, keeping the same link.
  - Microsoft
    - I am an agent acting on behalf of a user and want to upload/download a file efficiently & securely, with my user present (can confirm).
    - I am an agent acting on behalf of a user and want to upload/download a file efficiently & securely, without my user present (auto run).
    - I am an agent acting on behalf of a user and want to upload a file to one of many potential locations efficiently & securely, with my user present (can confirm).
    - I am an agent acting on behalf of a user and want to upload a file to one of many potential locations efficiently & securely, without my user present (auto run).
- Feedback on hard blockers on existing SEP-2631 proposal
  - Google
    - Must support authorized upload and download (i.e. no bearer URLs)
    - Need a resilient and efficient protocol for moving large binary payloads. Resumable uploads and ranged downloads should be supportable.
    - Metadata should be supplied before bytes move (supports regionalization, fail early so doomed-to-fail uploads don't move a bunch of bytes, etc...)
  - Microsoft
    - any pre-auth url scheme is a non-starter, all requests must come with ideally the same MCP bearer token auth as other MCP calls to that server
    - the method that returns the download url needs to take parameters as there may be 1-N potential upload locations for an agent (multiple sites, drives, its own drive, other storage)
- Specific Client Requirements
  - Microsoft
    - bearer token on all requests
    - http binary streaming file transport (great if we can include chunks, resumable upload, byte range download)
    - nice if we can create a generic solution for "streams" vs "files" using sink/source approach or similar concept.
  - OpenAI

- Model should not require more than one turn to do a file upload (one tool call from the perspective of the model - the harness takes care of the upload logic)
- Small files download and upload should use in-band transfer to reduce latency
- Large files download need out-of-band support to avoid base64 encoding
- All files content should stay out of model context during transfers.
- All tokens and credentials need to stay out of context window.
- Protocol should support MCP gateway deployments where the user-harness does not have the OAuth credentials
- Be explicit in the on-wire format about what is a pointer to a file so that the gateway/harness can apply specific security constraint scanning to files (ie: a deterministic proxy should be able to see which URLs are files - that is not the case today)
- Other (to be discussed)
  - (thomas) Can we use out-of-band URLs even when the main transport is STDIO?

#### Notes

- STDIO Discussion
  - Focus on HTTPS first but consider how to support STDIO
  - Consider a structured file type which would be useful even for STDIO
- Various feedback docs from folks:
  - [\[Externally Shared\] Google Feedback on SEP-2631](#)
  - [mcp\\_resources\\_as\\_domain\\_state\\_working\\_document](#)
  - Microsoft Proposal:
    - <https://discord.com/channels/1358869848138059966/1551968557292593172/1552399008440520865>
      - Just use resumable protocol, consider open spec
        - <https://datatracker.ietf.org/doc/draft-ietf-httpbis-resumable-upload/>

#### Action items

- ☐ [den@anthropic.com](mailto:den@anthropic.com) : will close out SEP-2631
- ☐ [den@anthropic.com](mailto:den@anthropic.com) : sync with Ola about collapsing charters of WGs
- ☐ [tsarlandie@openai.com](mailto:tsarlandie@openai.com) : Will take a pass on a V0 version of a new SEP

## Sep 23, 2026 | 📁 MCP: Files Working Group

Attendees: [Kurtis Van Gent](#) [Paris Mitton](#) [Wil St. Charles](#)

#### Notes

- Intros

- Meeting Cadence and time slot
  - weekly, coordinate over discord
- Upload and download
  - should clarify what things don't work for download
    - auth
- Pain points with file transfers/byte movement from folks today
- What is the minimal viable problem here (4-5 CUJs)
  - User wants agent to upload file to Drive (10MB+)
  - Agent wants to download file from Drive (file sizes 10MB - 100MB)
- SEP-2631 high-level thoughts and feedback?
  - Auth headers on upload/download
  - [Google Feedback on SEP-2631](#)
    - This is missing a clarification about upload/download auth
  - MSFT - doesn't have one upload location, has 100s of upload locations
    - authorizeUpload would need to take params
  - MSFT + Google - would like chunked upload
  - Transport streaming
    - performance gains from using a streaming transport
    - could be used outside of files (streaming transcripts, etc...)
    - Patrick - feels almost mandatory
    - HTTP streaming
  - How does SEP 2631 work with STUDIO
  - User creds may get added by a gateway in between harness and data sink
  - Try to reduce number of turns required for upload/download
    - also consider how to reduce number of network calls
- Characteristics of a solution?
  - Pass by reference semantics to the model
    - corollary: Harness/MCP client code handles actual byte movement
  - Byte movement *can* happen with auth
    - we don't want to expose auth tokens to the model
  - Transfers should avoid the base64 tax if possible
    - latency is important to OAI
  - Small files could still support base64/data uris

#### Action items

- ☐ Contribute 3-5 critical CUJs we want to solve
- ☐ Technical blockers with SEP 2631 (or similar)
- ☐ Specific requirements for your client

## **Design Discussion Topics**

- Byte Transfer Mechanics
  - Out-of-band HTTP Transfer?
  - Shoe-horn something into the existing JSON RPC which supports raw content frames?
- Authorization
  - Should we support both auth'd byte movement and bearer URLs?
- STDIO Support