JMAP
Internet-Draft
Updates: RFC8621 (if approved)
Intended status: Standards Track
Expires: 2 June 2026

M. De Gennaro
Stalwart Labs
29 November 2025

# JMAP Mail Sharing
## draft-ietf-jmap-mail-sharing-00

## Abstract

This document specifies an extension to the JSON Meta Application Protocol (JMAP) for Mail to enable sharing of mailboxes between users. Building upon the JMAP Sharing framework defined in [RFC9670], this specification extends the Mailbox data type defined in [RFC8621] with properties necessary to configure and manage access permissions for shared mailboxes. The extension introduces a new capability that indicates server support for mailbox sharing and defines the additional properties required to share mailboxes with other principals, including the ability to control which users may access a mailbox and what permissions they possess.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 2 June 2026.

## Copyright Notice

Table of Contents



## 1. Introduction

JMAP ([RFC8620] — JSON Meta Application Protocol) is a generic protocol for synchronizing data, such as mail, calendars or contacts, between a client and a server. It is optimized for mobile and web environments, and aims to provide a consistent interface to different data types.

[RFC8621] defines JMAP for Mail, which provides a data model for accessing, organizing, and managing email messages and mailboxes. The specification enables clients to efficiently synchronize mail data with servers and includes support for mailbox hierarchies, message threading, and various mail operations.

[RFC9670] subsequently standardized JMAP Sharing, which defines a framework for sharing data between users in collaborative environments. The specification introduces the Principal data type to represent entities (individuals, teams, or resources) and establishes a consistent model for defining shared access to data through the use of access control properties.

However, [RFC8621] was published prior to the standardization of the JMAP Sharing framework in [RFC9670], and therefore does not incorporate the sharing model into the Mailbox data type. This creates a gap in the ability to share mailboxes using the standardized JMAP sharing mechanisms.

This document bridges that gap by defining how the Mailbox object defined in [RFC8621] is extended to support the sharing framework established in [RFC9670]. This extension enables users to share their mailboxes with other principals using a consistent sharing model that can be applied uniformly across different JMAP data types. The specification defines the necessary properties, permissions, and capability advertisements to enable interoperable mailbox sharing implementations.

## 1.1. Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

## 1.2. Addition to the Capabilities Object

The capabilities object is returned as part of the JMAP Session object; see Section 2 of [RFC8620]. This document defines one additional capability URI.

### 1.2.1. urn:ietf:params:jmap:mail:share

This capability indicates server support for sharing mailboxes as defined in this specification. When a server advertises this capability, it signifies that the Mailbox data type has been extended with the sharing properties defined in Section 4 of [RFC9670] and that clients may use these properties to configure mailbox sharing with other principals.

The value of this property in the JMAP Session "capabilities" property is an empty object.

The value of this property in an account’s "accountCapabilities" property is an empty object.

## 2. Mailbox Sharing

According to Section 4 of [RFC9670], shareable data types MUST define three specific properties to participate in the JMAP sharing framework: isSubscribed, myRights, and shareWith. These properties enable users to control whether they wish to see shared data, understand what permissions they have, and configure who the data is shared with, respectively.

In addition to these three properties, shareable data types SHOULD define a permission within the rights object that indicates whether a user has the authority to share the object with others. This permission controls access to modifying the shareWith property.

The Mailbox object defined in Section 2 of [RFC8621] already includes the isSubscribed and myRights properties, as mailbox subscription and access control were integral features of the original mail specification. However, the specification did not include the shareWith property or define a permission for sharing rights.

This specification extends the JMAP Mailbox object defined in [RFC8621] to include the shareWith property as defined below:

*shareWith*: Id[MailboxRights]|null (default: null) This is a map configuring who the mailbox is shared with, or null if it is not shared with anyone. Each key in the map is the id of a Principal with whom the mailbox is shared. The value for each key is the set of access rights that Principal has for the mailbox. The account id for the Principals may be found in the urn:ietf:params:jmap:principals:owner capability of the Account to which the mailbox belongs. The Principal to which this mailbox belongs MUST NOT be in the map. The property may only be modified if the user has the mayShare right.

This specification also extends the JMAP MailboxRights object defined in Section 2 of [RFC8621] to include the mayShare property as defined below. For servers that also support IMAP [RFC3501], this property corresponds to the IMAP ACL "a" right as defined in [RFC4314]:

*mayShare*: Boolean
The user may modify the shareWith property for this mailbox. For servers supporting IMAP access to the same data, this corresponds to the IMAP ACL "a" right defined in [RFC4314], which grants the ability to administer access control lists.

## 3. Security Considerations

All security considerations described in [RFC8621] and [RFC9670] apply to this specification. Additional considerations specific to mailbox sharing are detailed below.

### 3.1. Access Control Enforcement

Servers implementing this specification MUST strictly enforce access controls when sharing mailboxes. When a user has access to a shared mailbox, the server MUST ensure that the user can only perform operations permitted by their assigned rights. As specified in Section 9.5 of [RFC8621], servers MUST treat any data the user does not have permission to access as if it did not exist. This principle extends to shared mailboxes: a user with partial access to an account MUST NOT be able to infer the existence of mailboxes or messages they do not have permission to access.

### 3.2. Interaction with IMAP ACLs

Servers that provide both JMAP and IMAP [RFC3501] access to the same mail store should carefully consider the interaction between JMAP sharing permissions and IMAP ACLs [RFC4314]. The mapping between JMAP MailboxRights and IMAP ACL rights must be consistent and clearly documented. When a mailbox is shared through either interface, the permissions MUST be properly reflected in the other interface to prevent security vulnerabilities arising from inconsistent access control enforcement.

Particular attention must be paid to the mayShare right and IMAP ACL "a" right mapping. Servers MUST ensure that granting the mayShare permission through JMAP correctly corresponds to granting the "a" right in IMAP, and vice versa. Any discrepancies in permission semantics between the two protocols could lead to privilege escalation or unintended access.

### 3.3. Unauthorized Sharing

As noted in Section 6.2 of [RFC9670], sharing data with another user can allow an attacker who gains transitory access to an account to establish persistent access by configuring sharing with an attacker-controlled principal. Servers implementing mailbox sharing SHOULD consider requiring additional authentication or confirmation when sharing permissions are modified, particularly when adding new principals to the shareWith map or granting elevated permissions such as mayShare.

Servers MAY implement audit logging of sharing configuration changes to enable detection of unauthorized modifications. Administrators SHOULD be provided with tools to monitor and review sharing configurations across accounts.

### 3.4. Information Disclosure Through Error Messages

Servers must be cautious not to leak information about the existence of mailboxes or their sharing status through error messages. When a user attempts to access or modify a mailbox they do not have permission to access, the server SHOULD return the same error response as it would if the mailbox did not exist, rather than indicating that access was denied. This prevents users from enumerating shared mailboxes they do not have access to.

Similarly, when a user attempts to share a mailbox with a principal they do not have permission to share with, error messages should not reveal whether such restrictions exist or details about the target principal.

### 3.5. Resource Exhaustion

Servers SHOULD implement limits on the number of principals with whom a single mailbox may be shared to prevent resource exhaustion attacks. Servers MAY also implement rate limiting on sharing configuration changes to mitigate denial-of-service attacks through excessive modifications to sharing permissions.

As described in Section 6.3 of [RFC9670], servers should be prepared to handle scenarios where users create many sharing-related state changes, which could generate numerous ShareNotification objects. Servers SHOULD implement appropriate resource limits and notification coalescing strategies.

### 3.6. Privilege Escalation

Servers MUST ensure that users cannot escalate their own privileges through manipulation of sharing permissions. For example, a user who has been granted limited access to a mailbox MUST NOT be able to grant themselves additional permissions by modifying the shareWith property unless they have been explicitly granted the mayShare right.

The owner of a mailbox (the Principal associated with the account containing the mailbox) always has implicit full rights to the mailbox. This ownership MUST NOT be transferable through the sharing mechanism, and the owner MUST NOT appear in the shareWith map.

# 4. IANA considerations

## 4.1. JMAP Capability Registration for "mail:share"

IANA will register the "mail:share" JMAP Capability as follows:

*Capability Name:* urn:ietf:params:jmap:mail:share
*Specification document:* this document
*Intended use:* common
*Change Controller:* IETF
*Security and privacy considerations:* this document, Section 3

# 5. References

## 5.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC4314] Melnikov, A., "IMAP4 Access Control List (ACL) Extension", RFC 4314, DOI 10.17487/RFC4314, December 2005, <https://www.rfc-editor.org/rfc/rfc4314>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8620] Jenkins, N. and C. Newman, "The JSON Meta Application Protocol (JMAP)", RFC 8620, DOI 10.17487/RFC8620, July 2019, <https://www.rfc-editor.org/rfc/rfc8620>.

[RFC8621] Jenkins, N. and C. Newman, "The JSON Meta Application Protocol (JMAP) for Mail", RFC 8621, DOI 10.17487/RFC8621, August 2019, <https://www.rfc-editor.org/rfc/rfc8621>.

[RFC9670] Jenkins, N., Ed., "JSON Meta Application Protocol (JMAP) Sharing", RFC 9670, DOI 10.17487/RFC9670, November 2024, <https://www.rfc-editor.org/rfc/rfc9670>.

## 5.2. Informative References

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, DOI 10.17487/RFC3501, March 2003, <https://www.rfc-editor.org/rfc/rfc3501>.

## Appendix A. Changes

[[This section to be removed by RFC Editor]]

*draft-ietf-jmap-mail-sharing-00*

* Initial version

## Author's Address

Mauro De Gennaro
Stalwart Labs LLC
1309 Coffeen Avenue, Suite 1200
Sheridan, WY 82801
United States of America
Email: mauro@stalw.art
URI: https://stalw.art