

# **MIMI Room Policy**

**Rohan Mahy: [rohan.ietf@gmail.com](mailto:rohan.ietf@gmail.com)**

**MIMI Interim, 02-Oct-2024**

# What is room policy?

## Access controls for a room, and properties of a room

- Membership style
  - open
  - members-only
  - fixed-membership (1:1 or Chat DM)
  - parent-dependent
- **Types of Roles** in the room and their Attributes or **Capabilities**: Role Based Access Control
  - Functions required, optional, or forbidden:
    - read receipts/deliver reports
    - history sharing
    - link previews
    - pseudonyms
    - Logging
  - Join links
  - Bot policies
  - MLS Settings
    - Ex: PCS Updates
    - Type of Handshakes allowed (Public/SemiPrivate/Private)
    - GroupInfo and ratchet\_tree handling

# What kinds of capabilities can be assigned to a role?

- Membership Capabilities
  - canAddParticipant
  - canRemoveParticipant
  - canAddOwnClient
  - canRemoveSelf
  - canAddSelf
  - canCreateJoinLink
  - canUseJoinLink
- Moderation Capabilities
  - canBan
  - canUnBan
  - canKick
  - canRevokeVoice
  - canGrantVoice
  - canKnock
  - canAcceptKnock
  - canChangeUserRole
  - canCreateSubgroup
- Message Capabilities
  - canSendMessage
  - canReceiveMessage
  - canReportAbuse
  - canReactToMessage
  - canEditReaction
  - canDeleteReaction
  - canEditOwnMessage
  - canDeleteOwnMessage
  - canDeleteAnyMessage
  - canStartTopic
  - canReplyInTopic
  - canSendDirectMessage
  - canTargetMessage
- Asset Capabilities
  - canUploadImage
  - canUploadVideo
  - canUploadAttachment
  - canDownloadImage
  - canDownloadVideo
  - canDownloadAttachment
  - canSendLink
  - canSendLinkPreview
  - canFollowLink
- Breakout
  - canSendDirectMessage
  - canTargetMessage
- Real-Time Media
  - canStartCall
  - canJoinCall
  - canSendAudio
  - canReceiveAudio
  - canSendVideo
  - canReceiveVideo
  - canShareScreen
  - canViewSharedScreen
- Disruptive Policy Changes
  - canChangeRoomMembershipStyle
  - canChangeOtherPolicyAttribute
  - canDestroyRoom
  - MLS specific
  - update
  - reinit
  - PSK
  - external proposal
  - external commit

# Strict administrator RBAC policy (example)

## Capabilities per role

- banned
  - (no capabilities)
- guest
  - canSendMessage
  - canReceiveMessage
  - canRemoveSelf
- ordinary\_user
  - (everything guest can do, plus:)
  - canAddOwnClient
  - canChangeOwnName,Presence,Mood,Avatar
  - canReport
  - canSendLinks
  - canSendImages
  - canSendVideos

- group\_admin
  - (everything ordinary\_user can do, plus:)
  - canSendAttachments
  - canAddParticipant
  - canRemoveParticipant
  - canBanish
  - canUnBanish
  - canKick
  - canChangeRoomName,Subject,Avatar
  - canPromoteRole(from=[ordinary]; to=[group\_admin])
  - canDemoteRole([from=[group\_admin], to=[ordinary])
  - canDestroyRoom
  - canCreateJoinLink

## • Role levels (low to high capabilities):

- banned
- guest
- ordinary\_user
- group\_admin
- super\_admin
  - (everything group\_admin can do, plus:)
  - canPromoteRole(from=[ordinary,group\_admin], to=[superadmin])
  - canDemoteRole(from=[superadmin], to=[ordinary,group\_admin])
  - canChangeRoomMembershipStyle
- Role constraints: must have at least 1 "group\_admin"

# Cooperative room RBAC policy (example)

## Capabilities per role

- banned
  - (no capabilities)
- ordinary\_user
  - canSendMessage
  - canReceiveMessage
  - canRemoveSelf
  - canAddOwnClient
  - canChangeOwnName,Presence,Mod,Avatar
  - canReport
  - canSendLinks
  - canSendImages
  - canSendVideos
  - canSendAttachments
- ordinary\_user (continued)
  - canAddParticipant
  - canRemoveParticipant
  - canKick
  - canChangeRoomName,Subject,Avatar
  - canCreateJoinLink
- group\_admin
  - (everything ordinary\_user can do, plus:)
  - canBanish
  - canUnBanish
  - canPromoteRole(from=[ordinary]; to=[admin])
  - canDemoteRole([from=[admin], to=[ordinary])
  - canDestroyRoom
- Role levels (low to high capabilities):
  - banned
  - ordinary\_user
  - group\_admin
  - super\_admin
- super\_admin
  - (everything group\_admin can do, plus:)
  - canPromoteRole(from=[ordinary,admin], to=[superadmin])
  - canDemoteRole(from=[superadmin], to=[ordinary,admin])
  - canChangeRoomMembershipStyle
- Role constraints: must have at least 1 "group\_admin"

# Moderated room RBAC policy (example)

## Capabilities per role

- banned
  - (no capabilities)
- non-participant
  - canKnock
  - canJoinViaLink
- guest
  - canReceiveMessage
  - canRemoveSelf
- attendee
  - (everything guest can do, plus:)
  - canAddOwnClient
  - canChangeOwnName,Presence,Mood,Avatar
  - canReport

- speaker
  - canSendMessage
  - canChangeRoomName,Subject,Avatar
  - canSendLinks
  - canSendImages
  - canSendVideos
  - canSendAttachments
- moderator
  - (everything speaker can do, plus:)
  - canAddParticipant
  - canRemoveParticipant
  - canAcceptKnock
  - canBan
  - canUnBan
  - canKick
  - canPromoteRole(from=[ordinary]; to=[admin])
  - canDemoteRole([from=[admin], to=[ordinary])
  - canCreateJoinLink

## Role levels (low to high capabilities):

- banned
  - non-participant
  - guest
  - attendee
  - speaker
  - moderator
  - super\_admin
- super\_admin
    - (everything group\_admin can do, plus:)
    - canDestroyRoom
    - canPromoteRole(from=[ordinary,admin], to=[superadmin])
    - canDemoteRole(from=[superadmin], to=[ordinary,admin])
    - canChangeRoomMembershipStyle
- Role constraints: must have at least 1 "moderator"