

MIMI Room Policy

draft-mahy-mimi-room-policy

Rohan Mahy: rohan.ietf@gmail.com

IETF 121, 7-Nov-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
 - canChangeUserRole(from=[ordinary]; to=[group_admin])
 - canChangeUserRole([from=[group_admin], to=[ordinary])
 - canDestroyRoom
 - canCreateJoinLink
- super_admin
 - (everything group_admin can do, plus:)
 - canChangeUserRole(from=[ordinary,group_admin], to=[superadmin])
 - canChangeUserRole(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
 - canChangeUserRole(from=[ordinary]; to=[admin])
 - canChangeUserRole([from=[admin], to=[ordinary])
 - canDestroyRoom
- super_admin
 - (everything group_admin can do, plus:)
 - canChangeUserRole(from=[ordinary,admin], to=[superadmin])
 - canChangeUserRole(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
- super_admin
 - (everything group_admin can do, plus:)
 - canDestroyRoom
 - canChangeUserRole(from=[ordinary,admin], to=[superadmin])
 - canChangeUserRole(from=[superadmin], to=[ordinary,admin])
 - canChangeRoomMembershipStyle
- Role constraints: must have at least 1 "moderator"