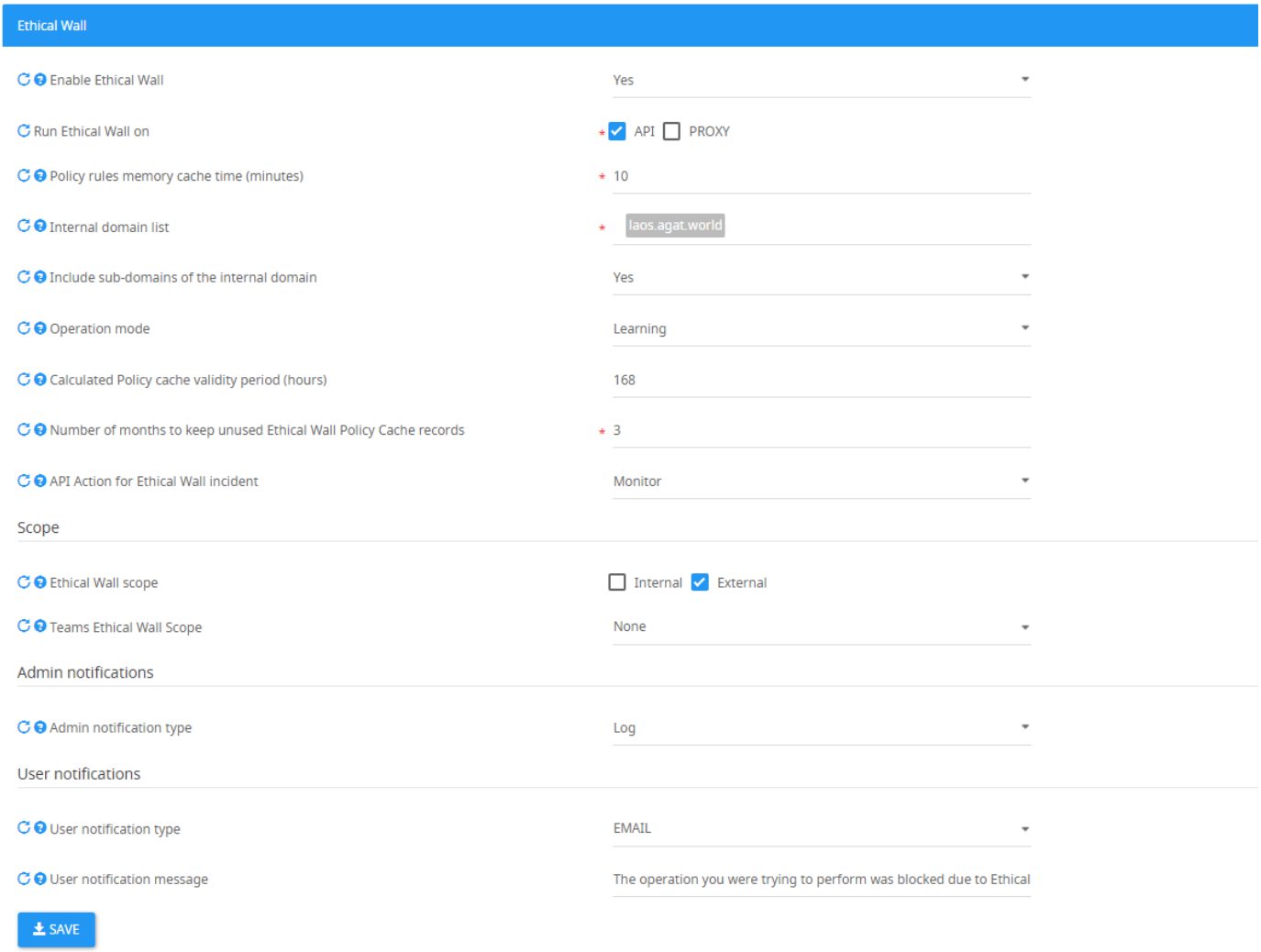
How to Configure the Ethical Wall?

The Ethical Wall provided by SphereShield serves as an information barrier to enforce data separation between groups & users within an organization or federated domains.

Ethical Wall Settings

In order to reach the Ethical wall settings, please go to your Access Portal Admin Area Settings Ethical

Please note all the following settings will not appear unless the "Enable Ethical Wall" Settings is set to "Yes".



Run Ethical Wall on – Choose according to your proxy for real-time inspection and API for near-real-time and detection.

Policy rules memory cache time (minutes) – Set the number of minutes for the engine to save policies and policy cache locally on the server before refreshing and fetching updated policies from the Database.

Internal domain list – Enter the MS 365 domains of your environment.

Include sub-domains of the internal domain - whether subdomains will be considered as internal or not.

Operation Mode – Set the operation mode on which the engine runs (Live, Learning, or Dummy). When onboarding a new user base, you should set the operation mode to learning.

Calculated Policy cache validity period (hours) – Set the number of hours for policy cache records to remain valid, after this expires the non-valid records will get deleted.

Number of months to keep unused Ethical Wall Policy Cache records - for how long to keep unused cached records in the table. Set to 0 if you don't want them to be deleted.

API Action for Ethical Wall incident - When in API mode. The action to take upon and incident.

Ethical Wall scope – The scope of the Ethical Wall, External controls federated users, while internal controls internal users' communications.

Teams Ethical Wall scope - which teams should be monitored by the Ethical Wall engine.

Admin notification type – Choose the type of notification for notifying admins about Ethical Wall incidents
(Required configuration of the notification settings)

User notification type – Choose the type of notification for notifying users about Ethical wall incidents they have caused (Required configuration of the notification settings).

User notification message – Enter the message to be sent to users after they have caused an Ethical Wall Incident.

Ethical Wall Policies

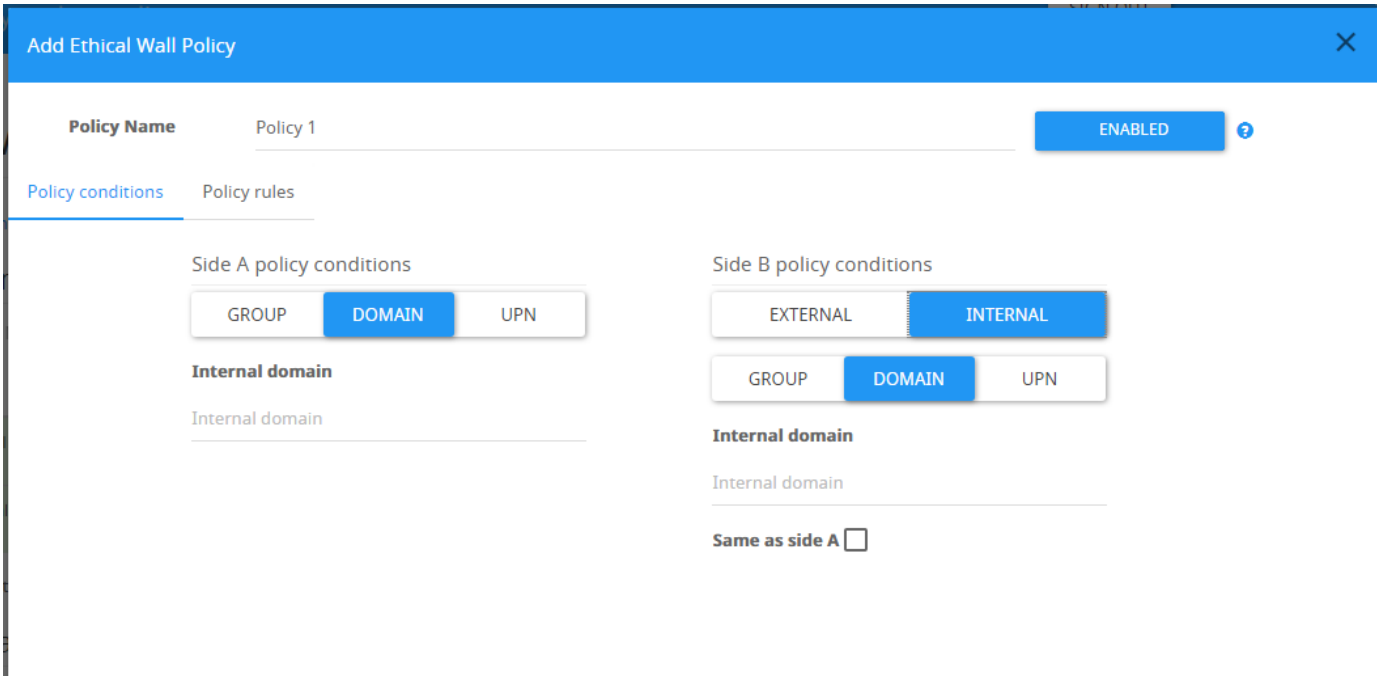
In order to configure Ethical Wall policies, please go to the Access Portal Admin Area Ethical Wall Policy, or by using the following URL: */admin /federationpolicy*

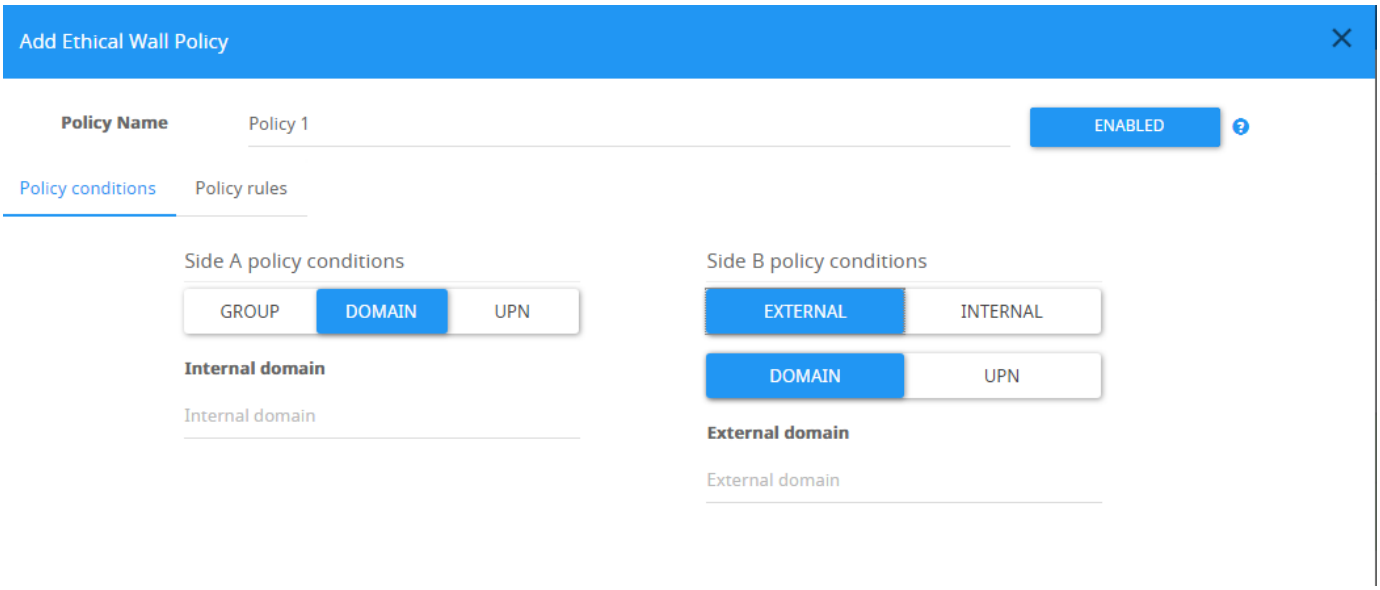
Ethical Wall policies can be set to apply internally (on users and groups within the organization that communicate with other users or groups within the organization). Alternatively, policies can also be set to apply externally (For federated domains).

Ethical Wall policies can be applied to specific groups within the domain that the Access Portal can pull from the Active Directory. When enabling the Ethical Wall, it will create a default policy for two-participants conversation and multi-participants conversation, these policies cannot be moved up/down and cannot be deleted. Use it as a baseline for when none of the policies apply. There are 2 default policies for internal Ethical wall, another 2 default policies for the external Ethical wall (for P2P and conference both internally and externally) and the third one is for communication within Teams

P2P (Peer to Peer) Policies

These policies are policies that are applied when a certain user chooses to communicate with another user, by searching the appropriate contact in the user's client and starting a conversation.





Below is a general explanation about this type of Ethical Wall policy.

When setting an Ethical Wall policy it is set between 2 sides (Side A, Side B).
Side A Should be an internal domain\User\AD Group, and side B can be Internal domain\UPN\AD Group or External Domain\UPN.
Side B of an Ethical Wall policy can have special configurations:
• "Same as side A" – The ability to set policies for each internal domain when using multiple ones.

When we have a policy created, we can use the Allow/Block/Control button in order to choose what capabilities of Microsoft Teams we'd like to have allowed/blocked.

Allow – Allow all controlled capabilities between side A and side B.

Block – Block all controlled capabilities between side A and side B.

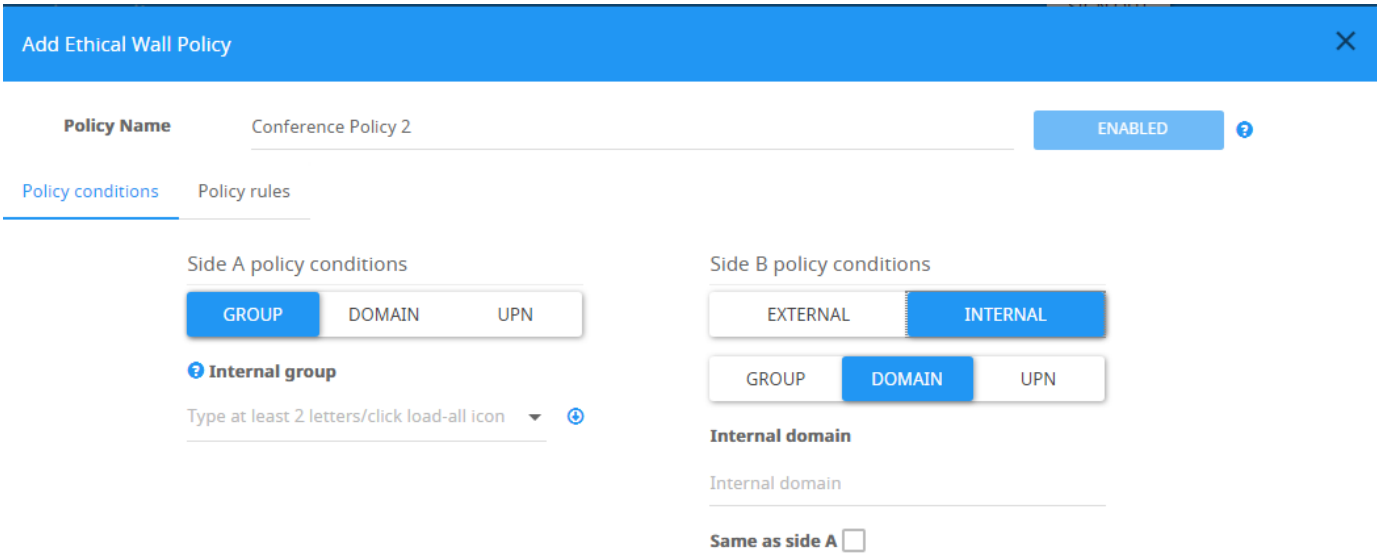
Control – Modify the policy to specific needs:

Within the Policies, the customer may set the restriction to each side differently, by having control on different Skype for Business capabilities:

- **Chat** – The ability to send a chat message.
- **Audio** – The Ability to initiate an audio call.
- **Video** – The ability to initiate a video call.
- **File Sharing** – The ability to share a file.
- **Desktop Sharing** – The ability to perform a screen presentation.

Conference Policies

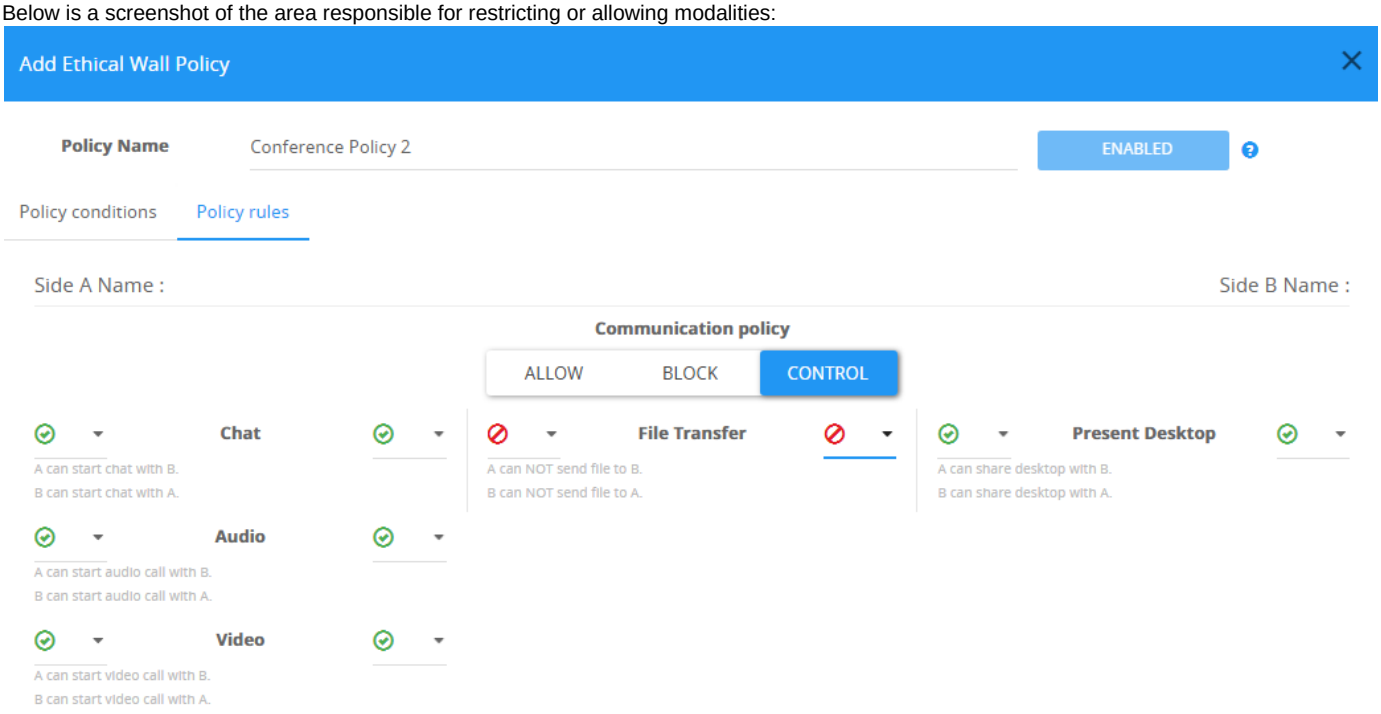
These types of policies are policies that are applied when a meeting takes place. Below is a general explanation about the rules and settings of this type of Ethical wall policy. Note that the policy conditions can't be changed in the default conference policy.
When setting an Ethical Wall policy it is set between 2 sides (Side A, Side B). Side A Should be an internal domain/Group/UPN, Side B can be an internal domain and also and External Domain.



Within the Policies, the following restrictions can be set over these 6 configurations:

- **Chat** – The ability to initiate a chat.
- **Audio** – The Ability to initiate an audio conversation.
- **Video** – The ability to initiate a video call.
- **File transfer** – The ability to send a file
- **Present Desktop** – The ability to present the screen.

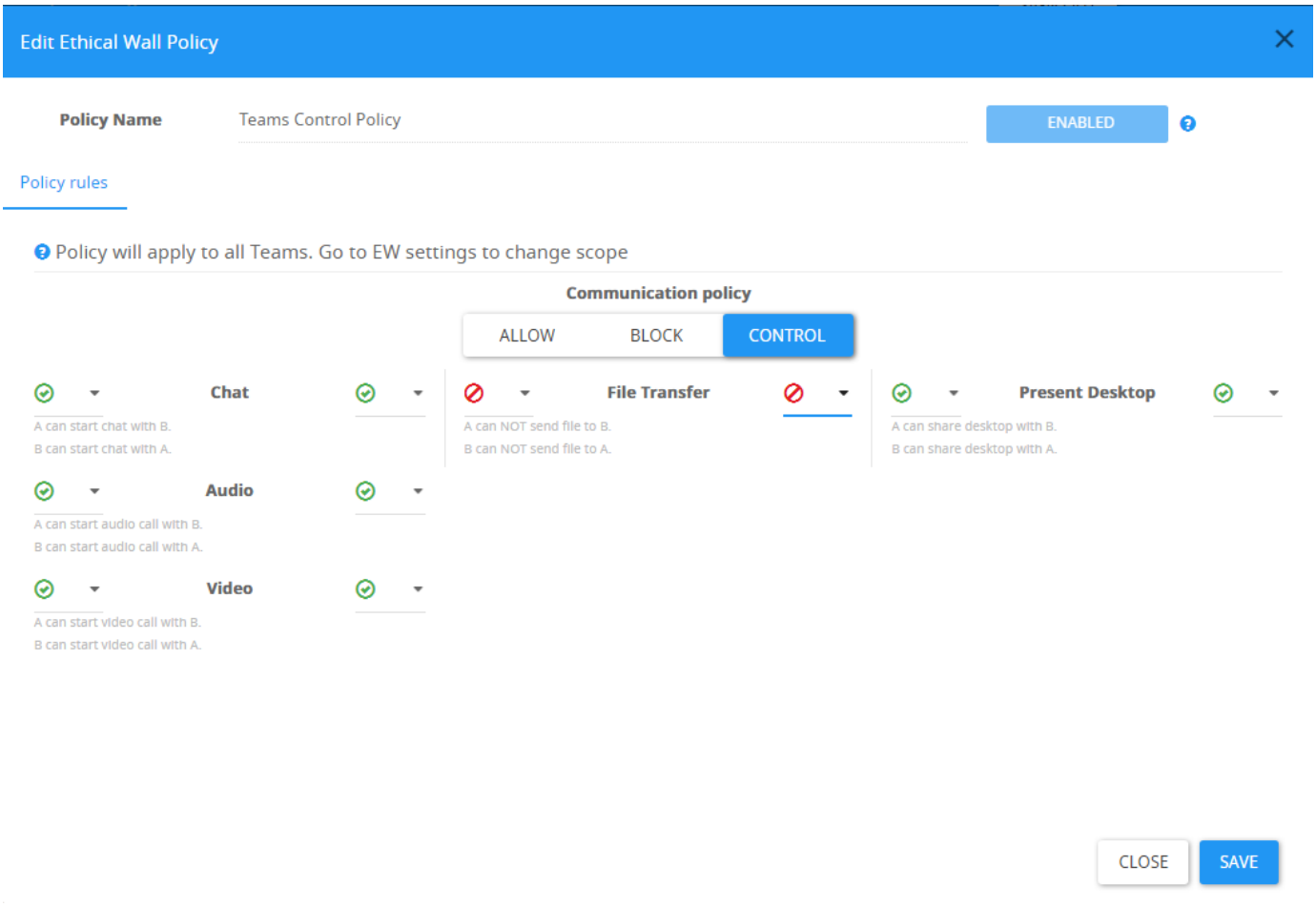
Below is a screenshot of the area responsible for restricting or allowing modalities:



TEAMS CONTROL POLICY

There is only 1 policy of this type. The rules of this type of policy will to any conversation inside a Teams channel, according to your configuration.

Below is a screenshot of the rules you can configure for this policy:


Edit Ethical Wall Policy
Policy Name
Teams Control Policy
ENABLED
Policy rules
Policy will apply to all Teams. Go to EW settings to change scope
Communication policy
ALLOW
BLOCK
CONTROL
Chat
A can start chat with B.
B can start chat with A.
File Transfer
A can NOT send file to B.
B can NOT send file to A.
Present Desktop
A can share desktop with B.
B can share desktop with A.
Audio
A can start audio call with B.
B can start audio call with A.
Video
A can start video call with B.
B can start video call with A.
CLOSE
SAVE