Estudo em Casa
Recomendações de segurança

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Plataforma ZOOM

ZOOM – Versão: 4.6.10 (20033.0407)*

Acesso à plataforma

A preparação de videoconferências pode ser feita através da plataforma ZOOM em linha (Figura 1) ou através da aplicação cliente instalada no dispositivo (Figura 2).

Em qualquer das situações, no momento da autenticação do utilizador, recomenda-se a inativação da opção "Continuar conectado" ("*Keep me signed in*").

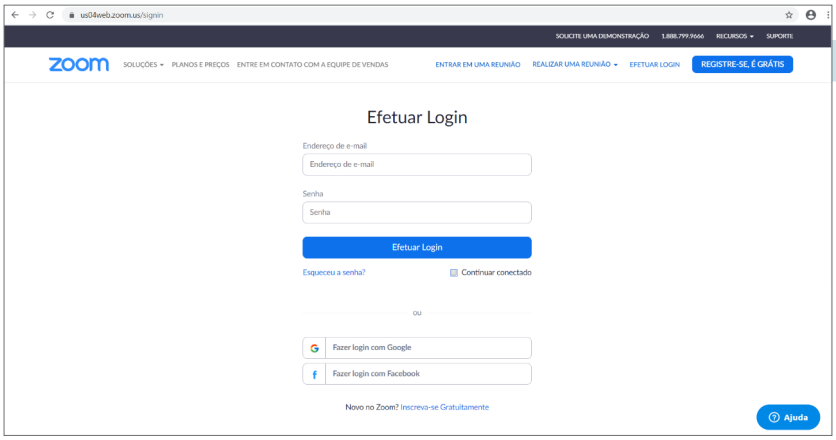

Fig.1

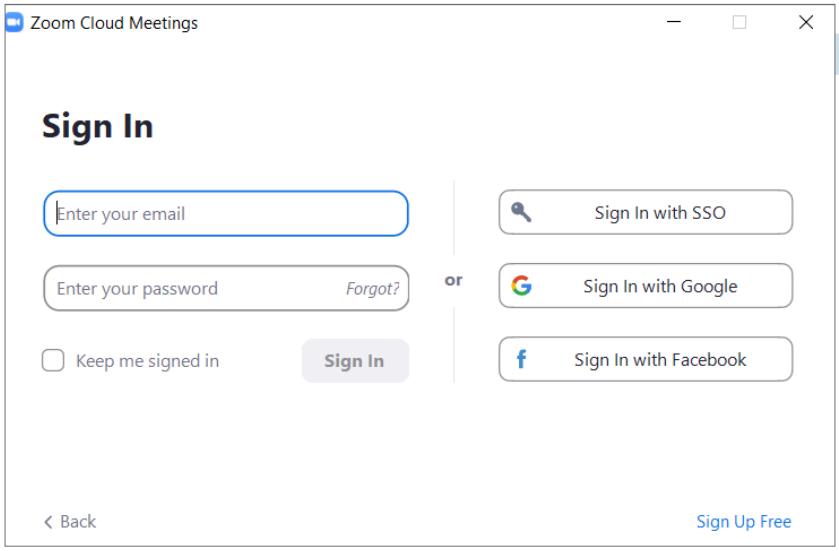

Fig.2

* As presentes recomendações têm por base a informação disponível e conhecimento do CNCS no momento da sua produção. Refletem por isso recomendações que visam apenas reduzir os riscos de segurança a confidencialidade conhecidos na utilização das aplicações, não excluindo por isso especiais cuidados adicionais, incluindo cuidados externos à utilização das plataformas no que respeita à segurança e proteção da privacidade dos utilizadores.

Configuração de base

Antes do agendamento de reuniões há alguns aspetos de configuração que o utilizador deve considerar. Estas configurações manter-se-ão por defeito em reuniões posteriores. Algumas destas configurações só estão disponíveis através da plataforma em linha. Na aplicação cliente, o utilizador poderá ser redirecionado através da opção "Ver mais configurações" ("*View More Settings*") no ecrã de configurações (Figuras 3 e 4).

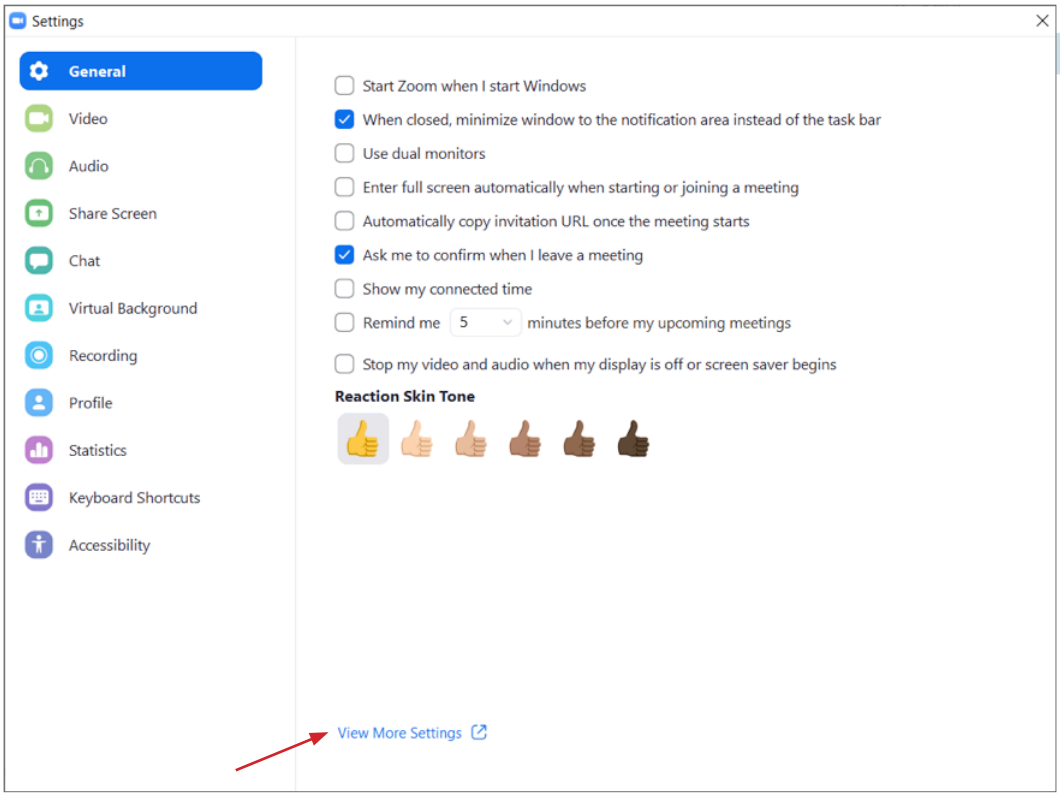

Fig.3

(aplicação cliente)

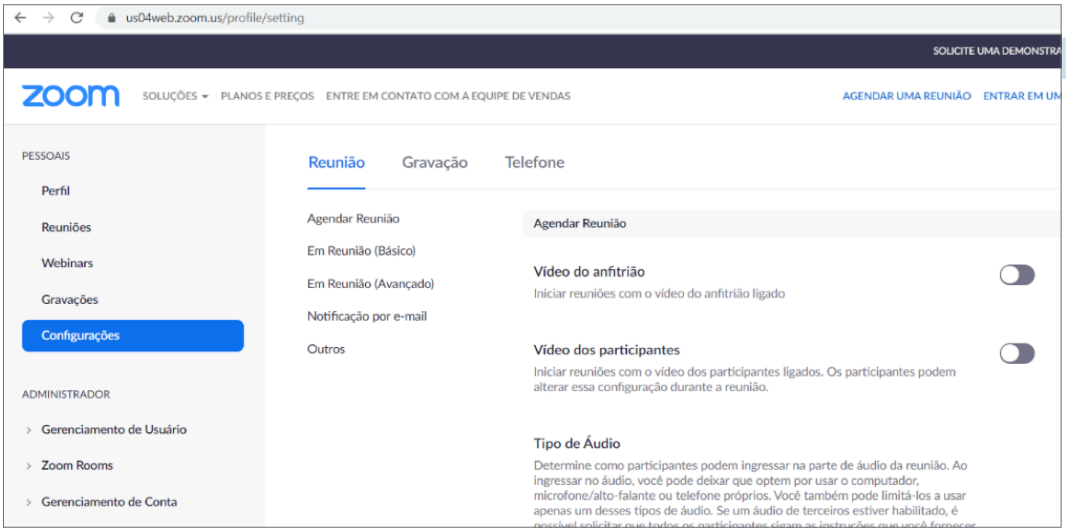

Fig.4

No menu de configurações, através da plataforma em linha, destacam-se as seguintes opções:

- **Requer uma senha para a ID pessoal de reunião (PMI)** – para maior segurança, **recomenda-se que a opção "Todas as reuniões que usam PMI" seja ativada** (Figura 5). O grau de segurança desta opção poderá ser aumentado com a criação manual de uma senha, até dez caracteres, **definindo um grau de maior complexidade recorrendo a caracteres alfabéticos, numéricos e especiais**[1];
- **Requer a senha para que os participantes ingressem pelo telefone** – para maior segurança, **recomenda-se que esta opção seja ativada** (Figura 5);
- **Requer criptografia para pontos de extremidade de terceiros (H323/SIP)** – segundo a ZOOM, as comunicações apresentam algum grau de criptografia (assinalada com um cadeado no canto superior o ecrã da reunião em curso – Figura 6) entre plataformas ZOOM. Segundo as opções de configuração, para que o mesmo possa acontecer na interação com outras plataformas, **recomenda-se que esta opção seja ativada** (Figura 7).

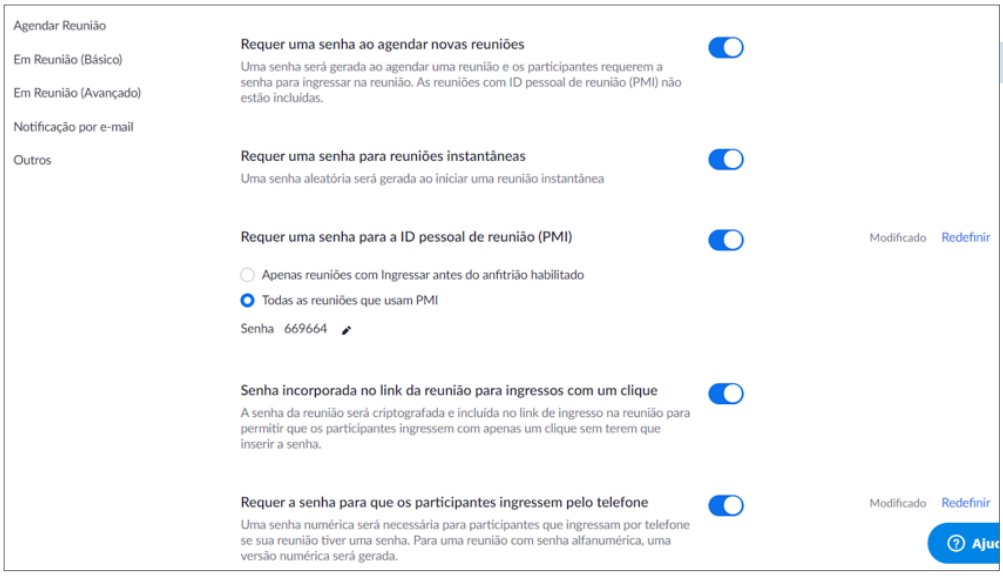

Fig.5

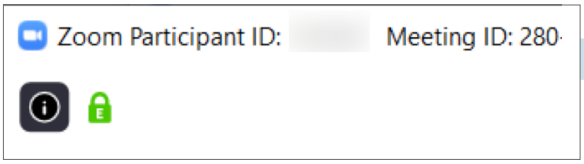

Fig.6

Fig.7

[1] Sobre como gerar passwords mais seguras consultar:
https://www.cncs.gov.pt/content/files/bp_pp_nov19.pdf
https://www.cncs.gov.pt/content/files/password.pdf

Paralelamente a estas configurações chama-se ainda a atenção para duas opções que poderão constituir boas práticas de acesso às reuniões:

- **Compartilhamento de tela** – por defeito, todos os participantes têm permissão para partilhar o ecrã. Esta opção deve ser avaliada pelo organizador em função do contexto da reunião (Figura 8);
- **Mostrar o link *"Join from your browser"*** – por defeito, esta opção está inativa. Ativando esta opção, permitirá que o participante, fazendo uma avaliação das condições de acesso e de risco, possa aceder à reunião através do explorador de Internet em vez da instalação da plataforma cliente (Figura 9). No entanto, esta funcionalidade encontra-se ligada a uma outra opção: *"Only authenticated users can join meetings from Web client"* (na versão analisada esta opção encontra-se apenas na língua inglesa).
- ***Only authenticated users can join meetings from Web client*** – esta opção, relacionada com a anterior, encontra-se no primeiro separador "Agendar Reunião" e está ativa por defeito (Figura 10). Esta opção implica que mesmo acedendo através de um explorador de Internet, o convidado terá que dispor de uma conta Zoom para aceder à reunião. Para excluir essa condição, o organizador terá que desativar essa opção – o convidado passa a aceder através do endereço fornecido sendo-lhe pedido apenas o ID da reunião (preenchido por defeito) e o seu nome.

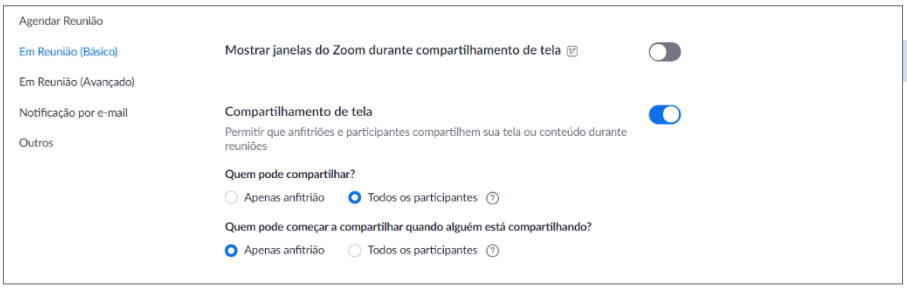

Fig.8

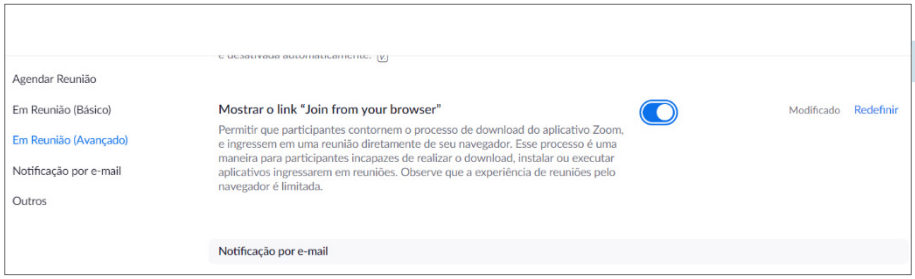

Fig.9

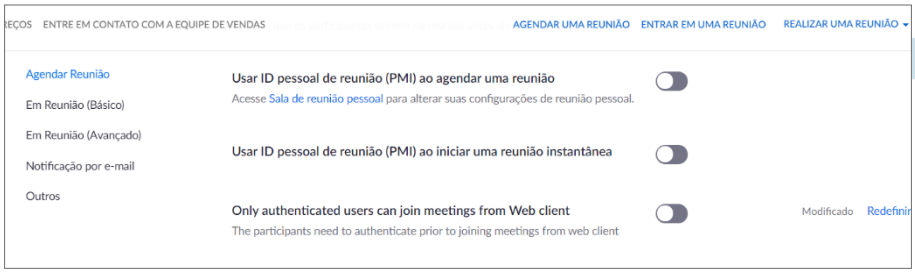

Fig.10

Agendar reuniões (videoconferência)

No agendamento das reuniões, tanto através da plataforma em linha como na aplicação cliente, as seguintes configurações merecem alguma atenção:

- **ID da reunião** – este identificador determinará o link de acesso à reunião: **recomenda-se que se opte pela sua criação automática para cada reunião** (Figura 11);
- **Senha da reunião** – **recomenda-se que esta opção seja sempre selecionada.** A criação da senha é automática por cada reunião criada, mas o grau de segurança desta opção poderá ser aumentado com a criação manual de uma senha, até dez caracteres, **definindo um grau de maior complexidade recorrendo a caracteres alfabéticos, numéricos e especiais[2];**

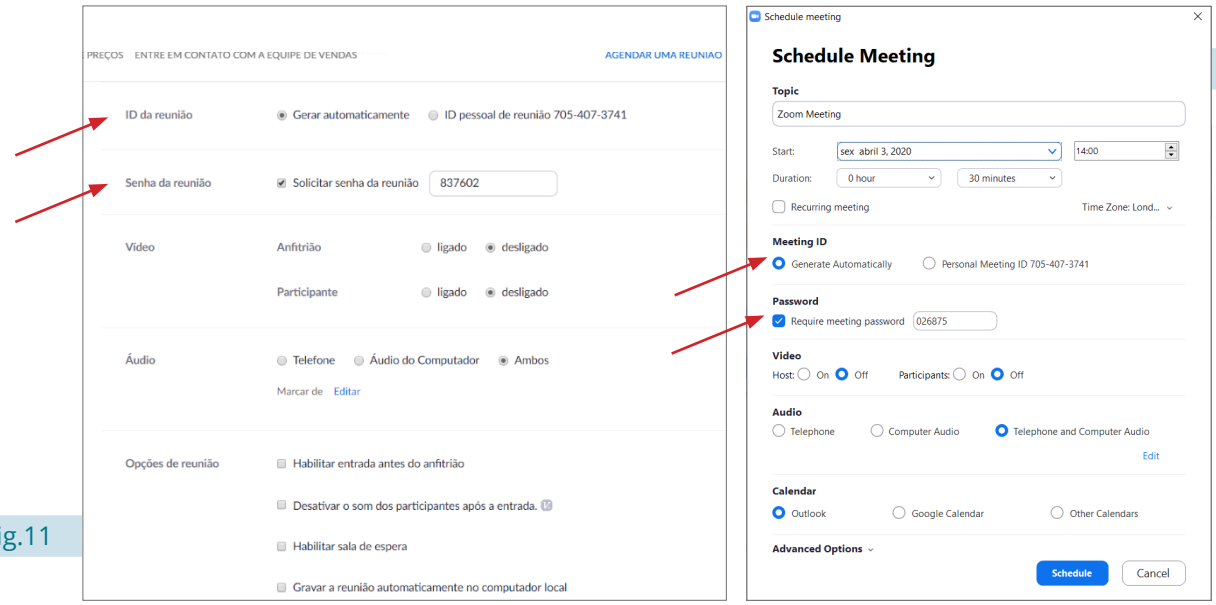

Fig.11

Fig.11
(aplicação cliente)

[2] Sobre como gerar passwords mais seguras consultar:
https://www.cncs.gov.pt/content/files/bp_pp_nov19.pdf
https://www.cncs.gov.pt/content/files/password.pdf

- **Opções de reunião** – por defeito, as quatro opções de reunião estão inativas. **Recomenda-se ativar a opção "Habilitar sala de espera"** (Figura 12) que permitirá que o acesso à reunião apenas seja feito após a autorização do organizador (Figura 13).

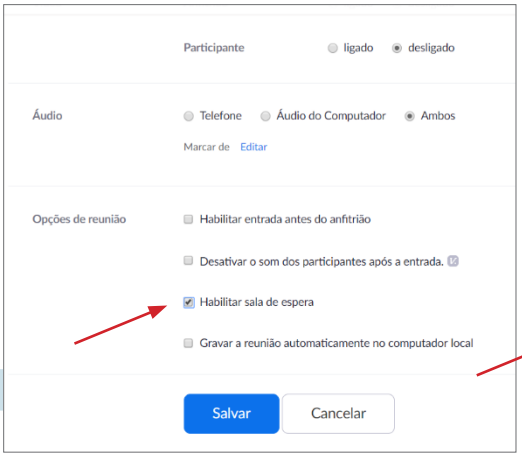

Fig.12

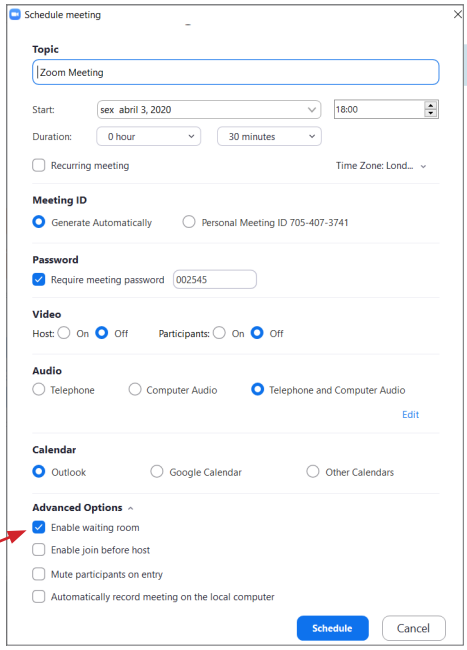

Fig.12
(aplicação cliente)

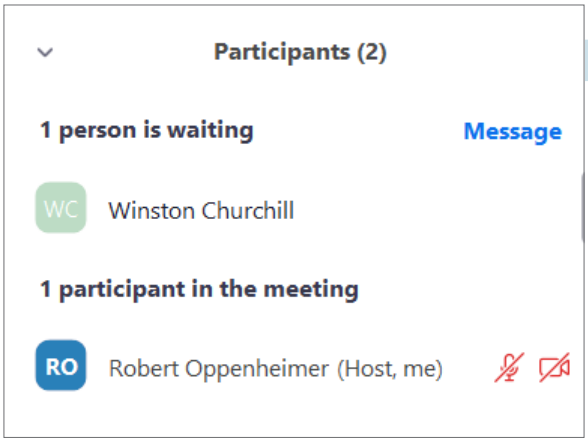

Fig.13

Segurança nas reuniões

A partir da versão 4.6.10 (20033.0407) a plataforma Zoom passou a dispor de um conjunto de ferramentas que pretende aumentar o nível de segurança na gestão das reuniões. Essas ferramentas encontram-se no painel de instrumentos da reunião e são acessíveis pelo botão "*Security*" (Figura 14).

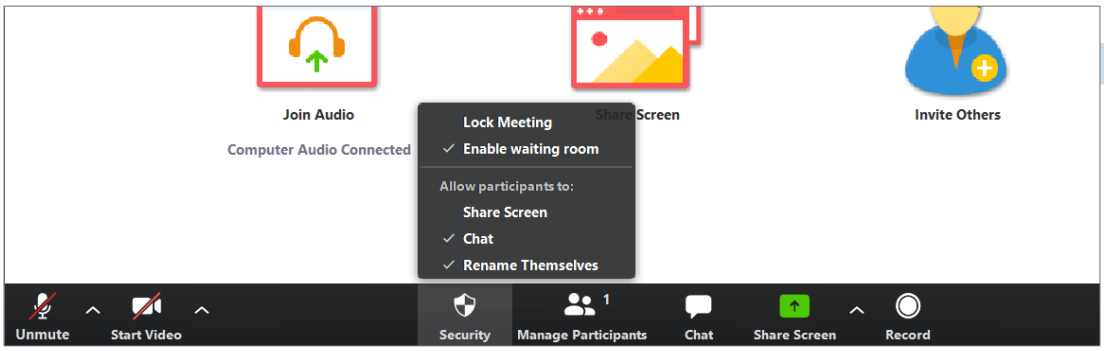

Fig.14

Através deste menu, o organizador pode gerir dois aspetos importantes:

- **Enable waiting room** – o organizador, caso não o tenha feito no painel de configurações (ver Figura 12), pode fazer essa gestão a partir daqui. **Recomenda-se ativar a opção "Habilitar sala de espera"** que permitirá que o acesso à reunião apenas seja feito após a autorização do organizador;
- **Lock Meeting** – esta opção permite ao organizador, depois de ativada, inibir o acesso de participantes à reunião mesmo que tenham sido convidados. **Recomenda-se ativar a opção "Lock Meeting"** para não permitir o acesso de novos participantes para além dos que se encontram nesse momento na reunião (Figura 15).

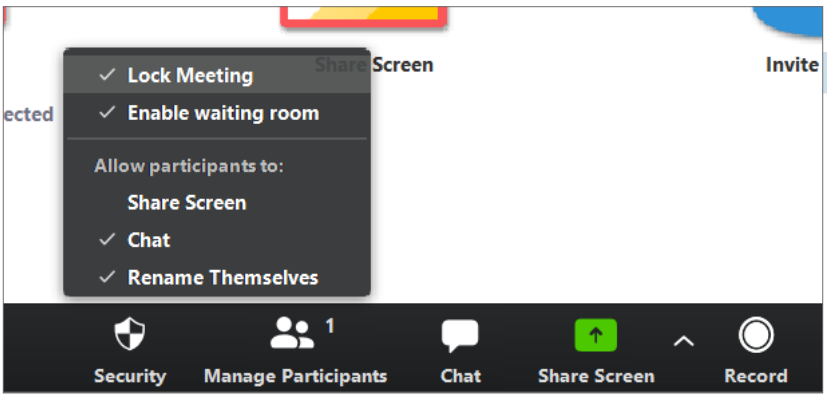

Fig.15