Zoom privacy tips

- ✓ Bespreek de privacyaspecten vooraf met de deelnemers. Denk daarbij aan zaken als: welke gegevens gebruik je, waarom, sla je ze op, wie kan er bij, hoe lang bewaar je ze en hoe beveilig je de gegevens.

- ✓ Ga je je scherm delen tijdens de Zoom meeting? Deel dan alleen de applicatie die je gaat gebruiken (bijvoorbeeld PowerPoint om een presentatie te laten zien) en niet je hele desktop. Ook al deel je je hele desktop niet, toch is het slim om alle meldingen (van je mailbox, WhatsApp, social media etc.) uit te zetten voordat je gaat Zoomen. Het (per ongeluk) delen van dat soort persoonlijke of interne meldingen kan in sommige gevallen gezien worden als datalek.

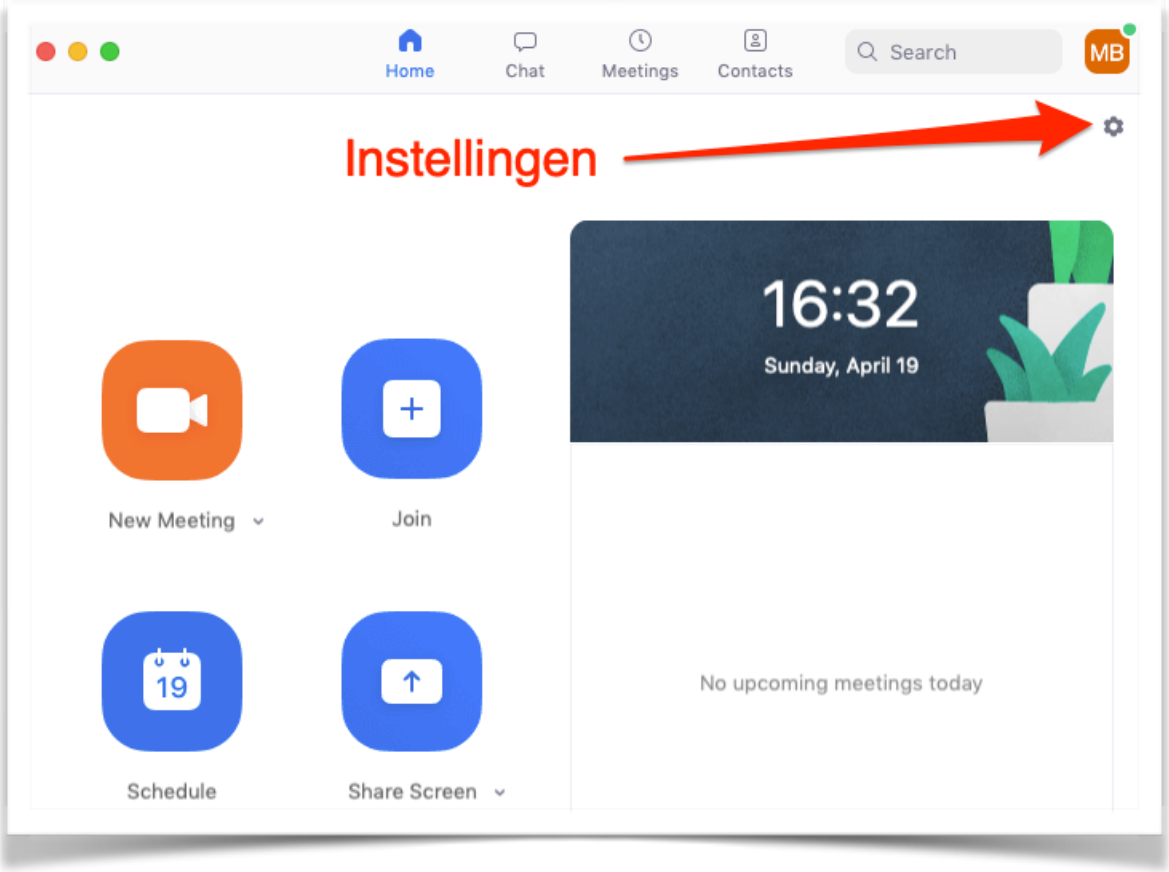
- ✓ Sluit de Zoom applicatie en log uit nadat je Zoom sessie is afgelopen.

- ✓ Plak na het Zoomen je camera af, of gebruik een webcam cover. Zo kunnen hackers niet stiekem bij je binnen kijken.

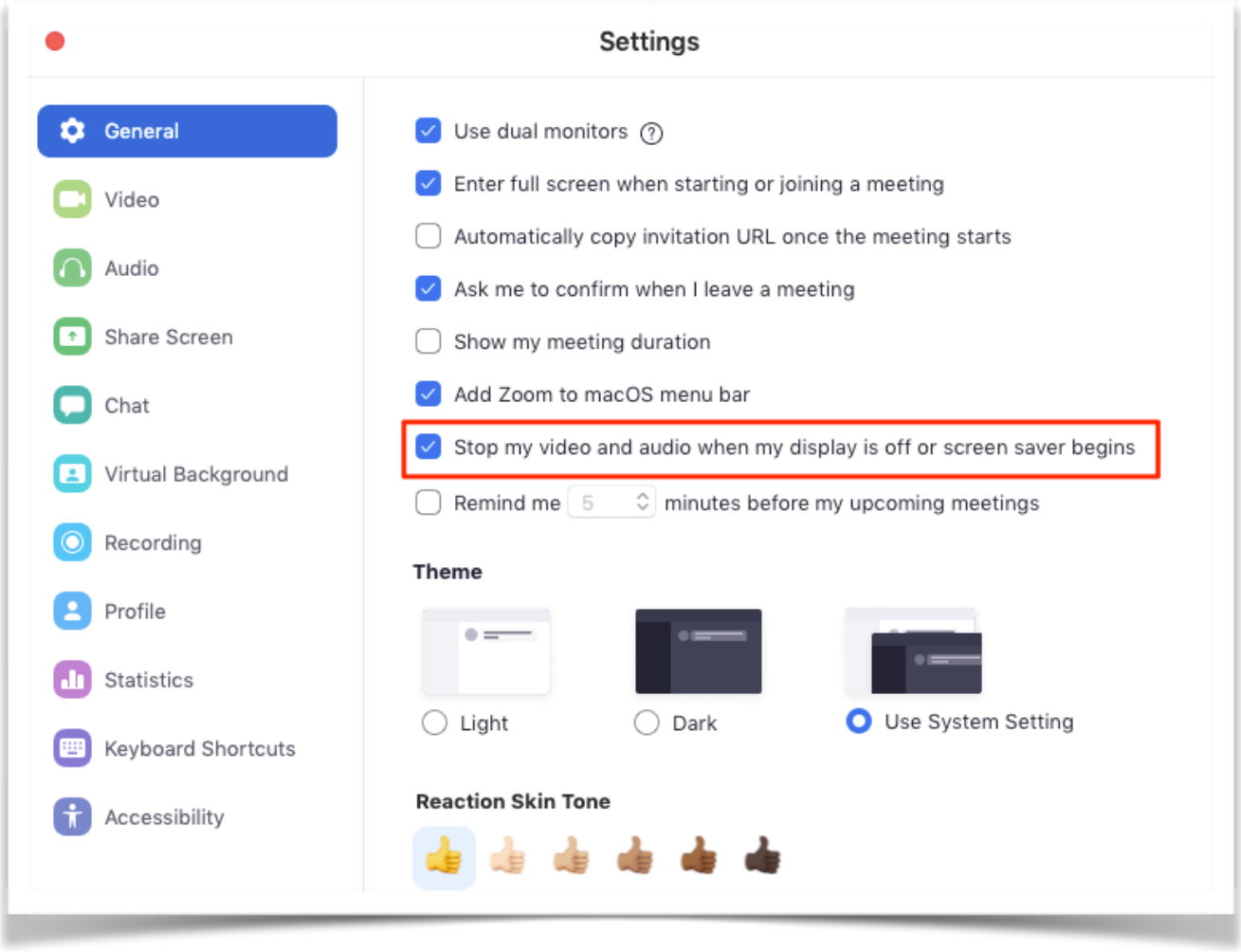
- ✓ Is er een nieuwe update voor je Zoom app? **Direct updaten!** Vaak worden hiermee beveiligingslekken gedicht en de beveiliging verbetert.

- ✓ Stel Zoom zo privacyvriendelijk mogelijk in.

Hier vind je een aantal privacy gerelateerde instellingen:

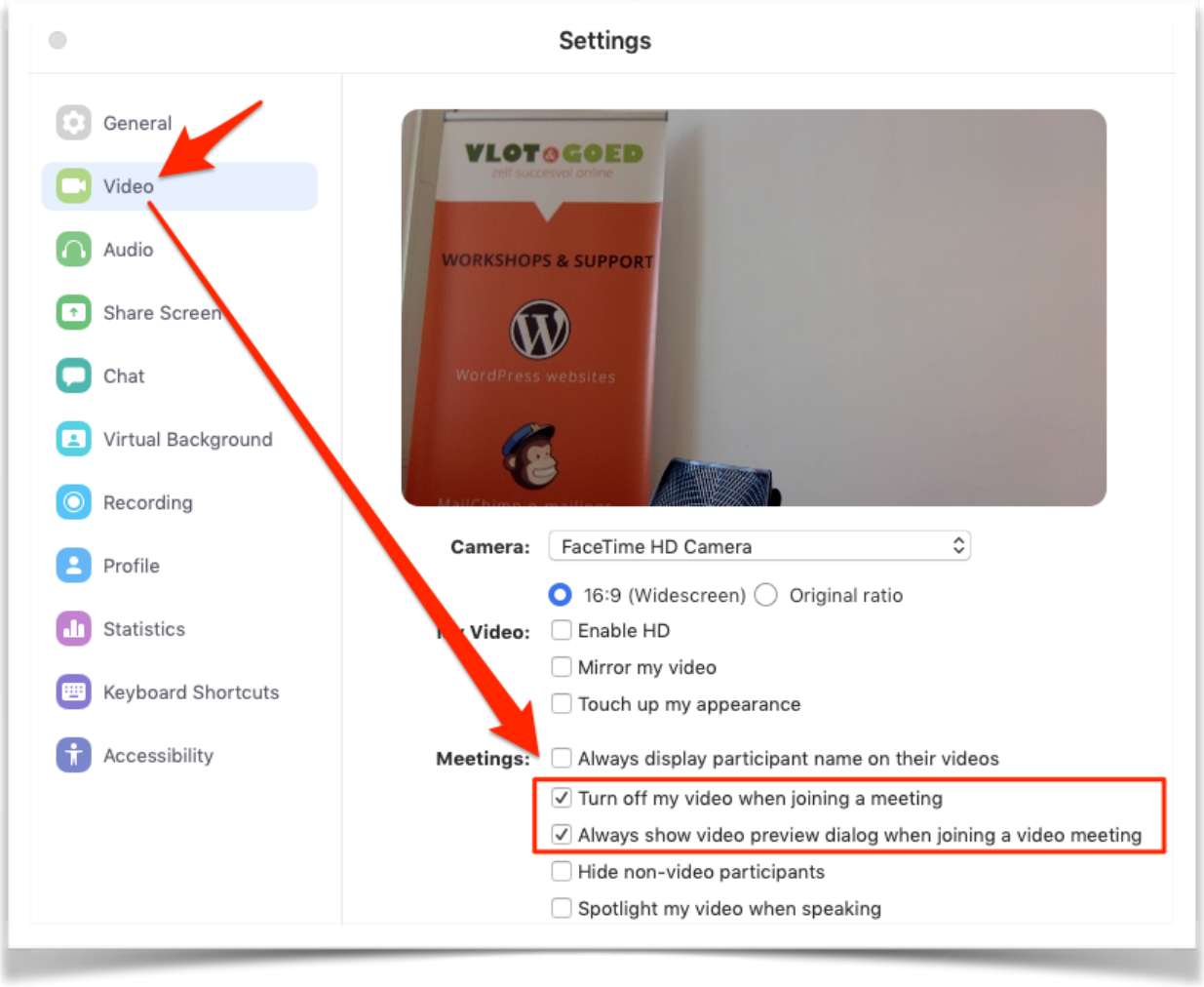


A. Voorkom dat je beeld en audio ingeschakeld blijven wanneer je monitor uit is:

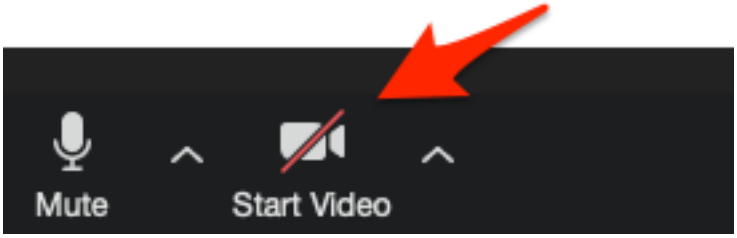


B. Bepaal zelf wanneer je voor het eerst in beeld komt

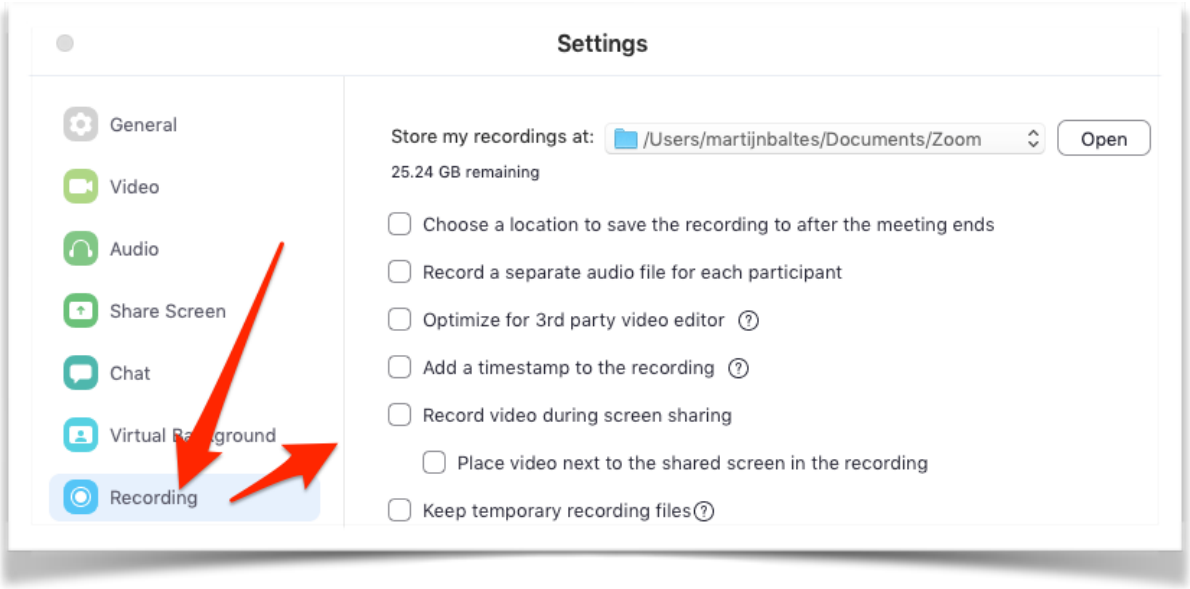
Dus niet automatisch als je de meeting start. En (als je geen host bent) ook niet direct op het moment dat je wordt toegelaten.



Wil je in beeld komen, dan doen je dat in de meeting op eigen initiatief (wanneer jij en je achtergrond er klaar voor zijn) door linksonder in de zwarte balk te klikken op"Start Video":

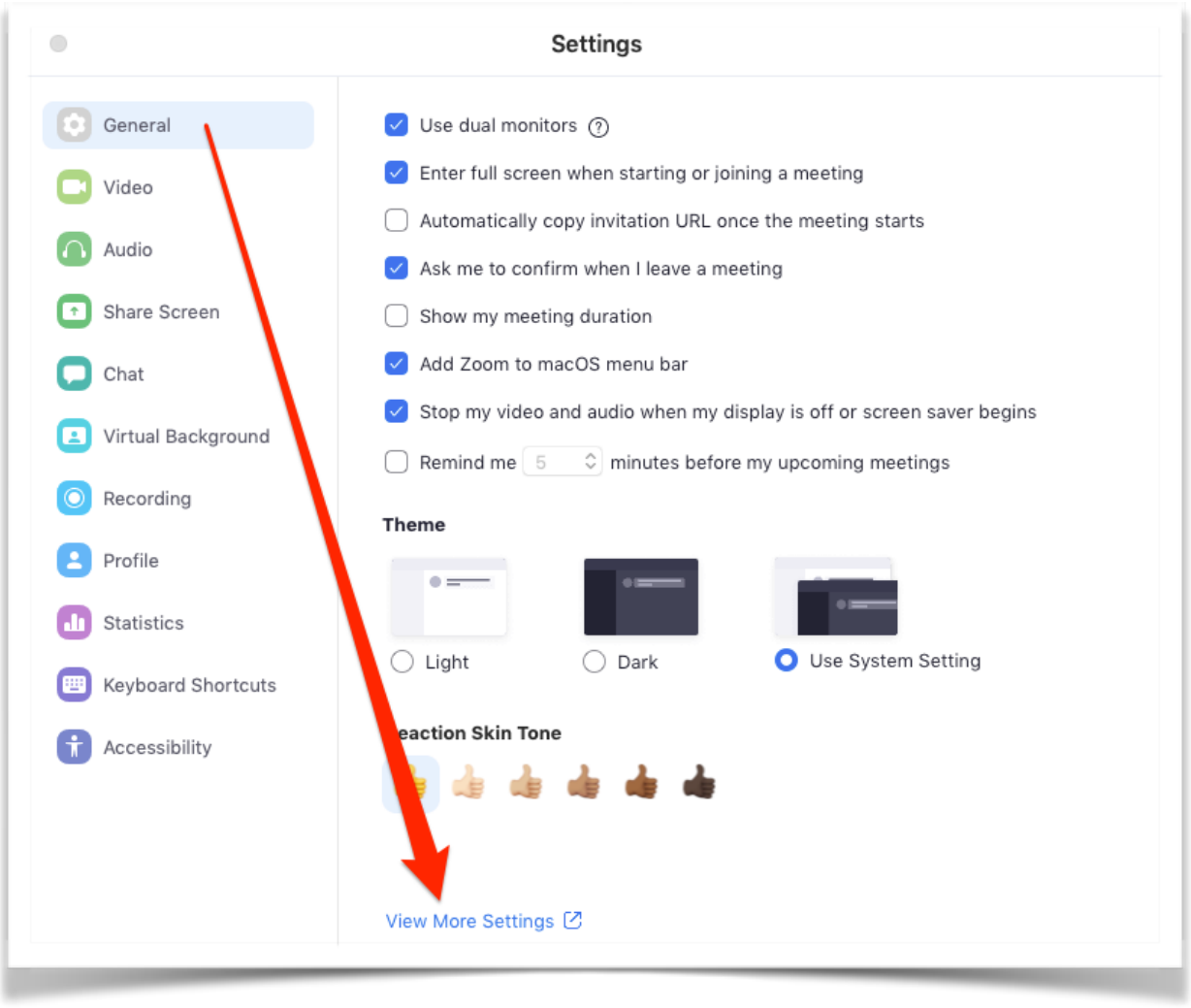


C. Zet op het tabblad 'Recording' alles uit

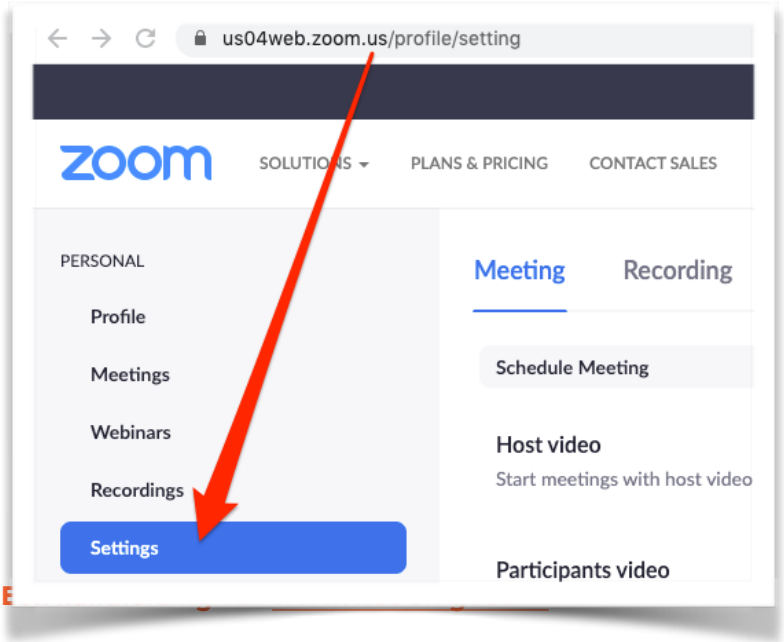


Tot zover de instellingen die je in de Zoom app vindt. De instellingen op de volgende bladzijden doe je buiten de Zoom app in je online Zoom account.

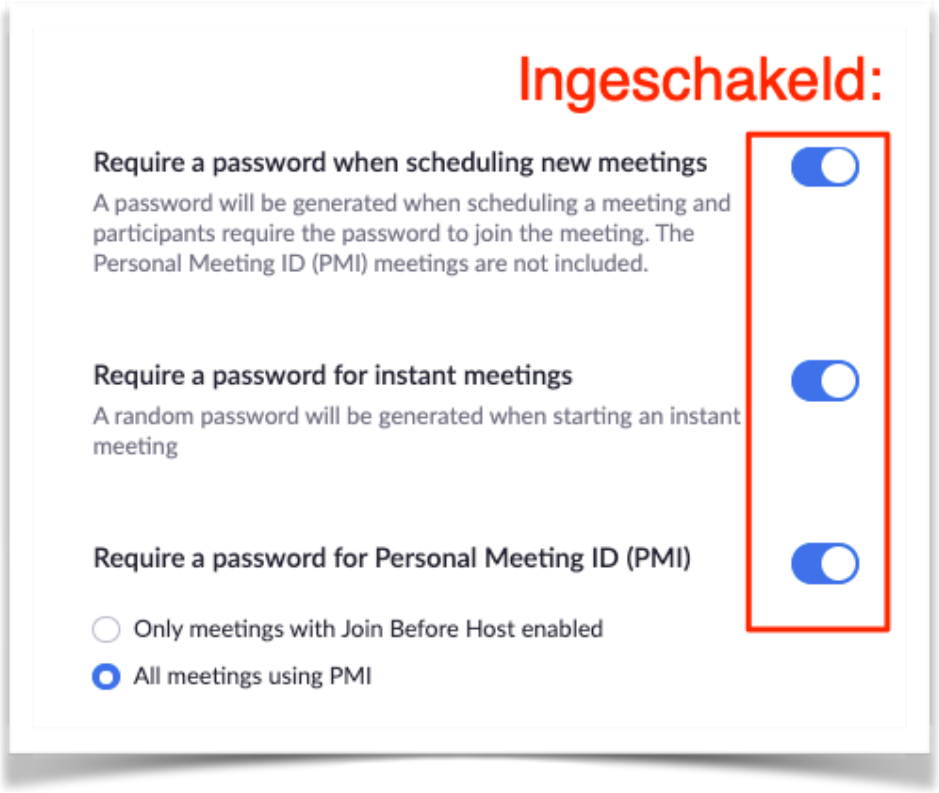
D. Belangrijke instellingen in je Zoom account:



Mogelijk word je na het klikken op "View More Settings" (zie hierboven) in de Zoom app gevraagd in te loggen in je online Zoom account. Daarna beland je in het tabblad Settings van je Zoom account (in je browser):

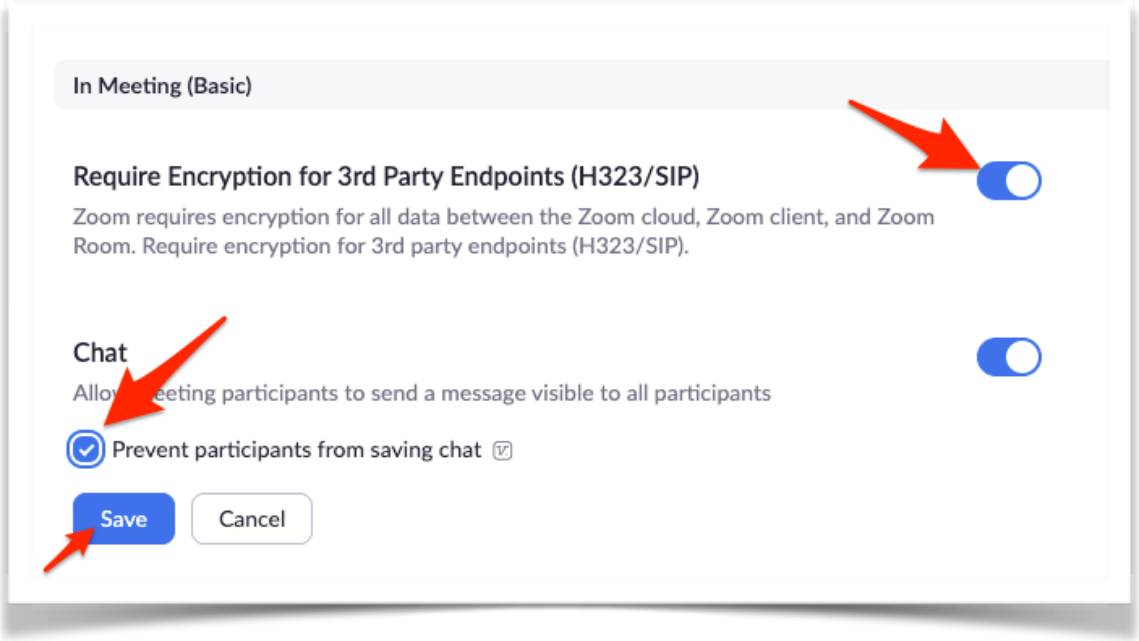


In je Zoom account zijn, als het goed is, de schuifjes in het onderstaande plaatje al blauw (= alle Zoom meetings voorzien van een wachtwoord). Wel even checken voor de zekerheid:



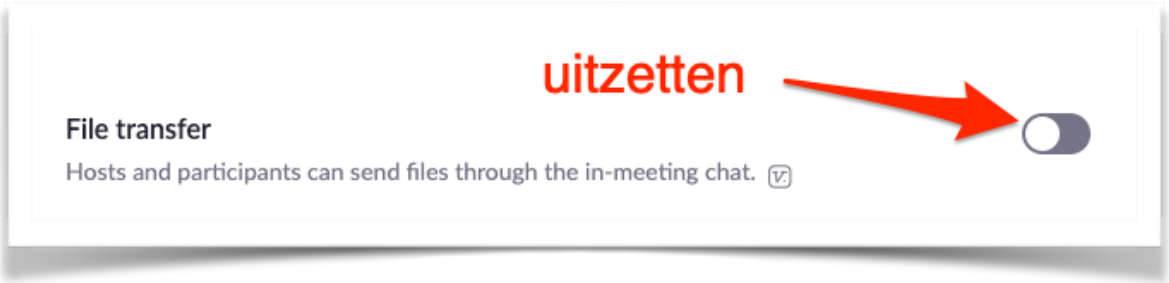
Scroll een heel stuk naar beneden naar het onderdeel "In Meeting (Basic) en schakel deze opties in:

✓ Aanzetten: Require Encryption for 3rd Party Endpoints (H323/SIP)
✓ Aanzetten: Chat - vinkje in "Prevent participants from saving chat"



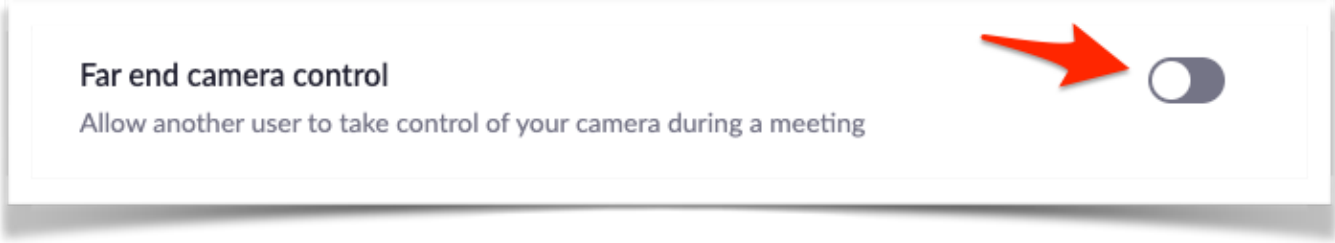
✓Schakel File transfer uit:

Bestanden uitwisselen kun je beter doen via je bedrijfsnetwerk, (versleutelde) e-mail of andere gebruikelijke platforms die je al in gebruik hebt hiervoor.



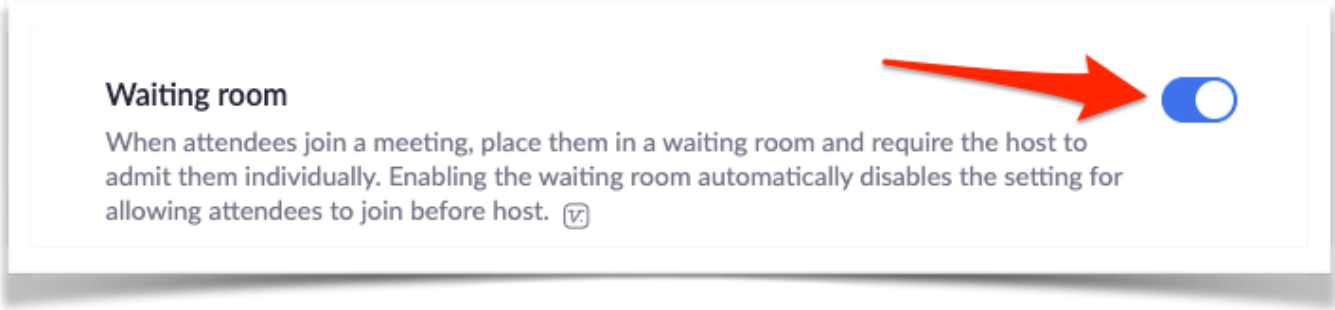
Scroll weer een eind naar beneden.

✓ Zorg dat "Far end camera control" uit staat:

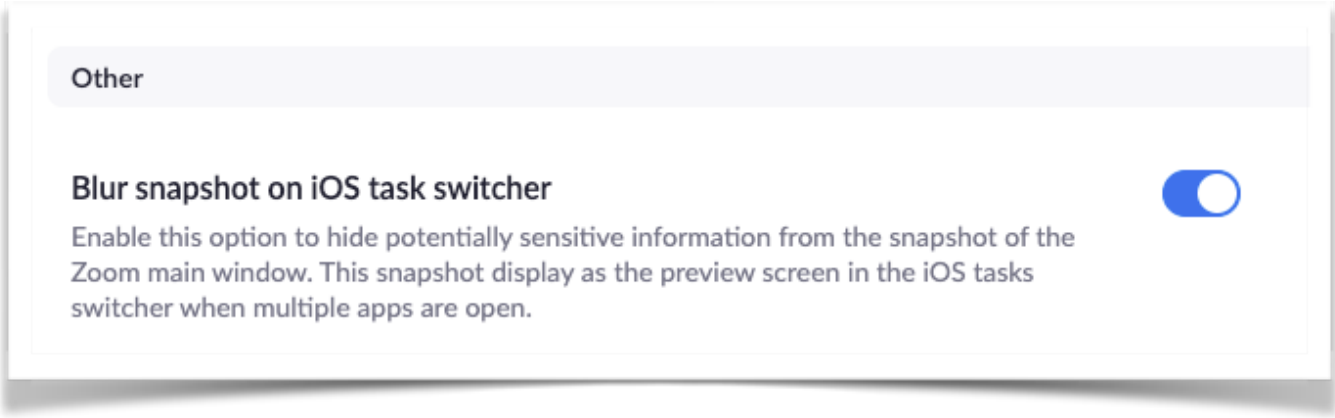


Scroll een stukje verder.

✓Zorg dat de "waiting room" is ingeschakeld. Dan bepaal je als host zelf wie er binnen mag komen in de Zoom meeting:



Voor iPhone en iPad gebruikers, deze optie inschakelen om mogelijk gevoelige informatie in de Zoom "schermwissel" snapshot te verbergen (te zien bij het wisselen van tussen apps):



Disclaimer: ik ben geen jurist of informatiebeveiligingssexpert. Deze tips zijn bedoeld om je een beeld te geven van wat je onder andere kunt doen binnen Zoom als het gaat om het verbeteren van enkele privacy gerelateerde aspecten. Raadpleeg een specialist om te bepalen welke acties in jouw situatie noodzakelijk zijn.