OnceHub Support

Webex Meetings security best practices

Last Modified on Dec 9, 2024

At OnceHub, we designed our native Webex Meetings integration with security at the forefront of our minds.

Important:

Webex has announced an end-of-life for its current meetings-related API. From March 31st, 2024, it will be permanently replaced by their newer REST API. To ensure Webex meeting links continue to be generated automatically, you must log into OnceHub and reauthenticate your Webex connection before March 31st.

Some existing features are not supported by the new API, so configuring your booking page will be a little different:

- The new API supports only dynamic passwords
- Audio settings will be taken from your Webex account, and can no longer be set in OnceHub
- Meetings shorter than 10 minutes will not be supported.
  - In booking pages: Customers will see an error message, and won't be able to schedule a meeting when trying to book a Webex-hosted meeting shorter than 10 minutes.
  - In booking calendars: The booking will be scheduled, but there will be no Webex link attached.

To reauthenticate your Webex connection, follow these steps:

1. Go to your profile settings by clicking the initials/profile picture at the top right of your screen
2. Click **Video conferencing**
3. Beneath the Webex heading, click **Reauthenticate** and follow the prompts to complete the process

You are welcome to reach out to support@oncehub.com if you have any questions.

Unique meeting IDs and links for every session

If you're used to offering a static link to your Webex Meetings Personal Room, like https://meetingsamer20.webex.com/meet/pr1234567890, break that habit fast and connect our native Webex Meetings integration instead. It may be simpler to use the same customized meeting link to everyone meeting with you, but that opens a huge vulnerability for uninvited guests. Each session needs its own meeting created, with its own meeting ID.

There's no need to waste time signing into Webex Meetings, creating the meeting, and sending a separate email with the conferencing information. When a customer books with you, OnceHub automatically creates a meeting in Webex Meetings and includes all conferencing information in the booking confirmation notification and on the calendar event.

Note:

Once you have a unique meeting ID, be sure only to share the conferencing information with those you want

to join. Many make the mistake of including a joining link on publicly available posters or websites. This increases the risk of an insecure meeting.

A password for every session

Some hackers can use technology to guess unique meeting IDs or may take advantage of publicly-posted information. Make sure anyone joining your session also receives a meeting password and don't advertise it anywhere except among authorized attendees. This gives an additional measure of security, creating another barrier for uninvited guests.

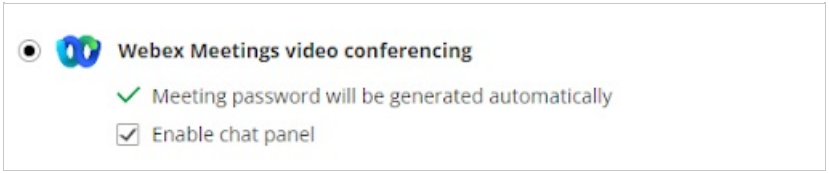

Figure 1: Meeting passwords

Educate your team members before they go live

Be sure not to skip a dry run for each team member giving meetings. That dry run is one of the most important steps helping them maintain professionalism in their video meetings. Especially if they've not used the video conferencing app much, there's a learning curve they'll need to adjust to in order to feel comfortable leading their session.

They should have a high awareness of all their available features. Notable settings that help them control the experience include:

- Waiting room features
- Chat features, including disabling private chat
- Muting participants
- Disabling video
- Turning off annotation
- Managing screen sharing of fellow attendees
- Removing participants

If they'll be occupied with meeting content and a number of people will be present, it may be worth having another person from your organization join. The team member leading the meeting can designate this additional team member as a co-host. The co-host can control the above listed features while the original host leads the meeting.

Team members should also ensure they've downloaded the correct software version before their session and join a few minutes early, just in case they encounter technical difficulties. These can be challenging to predict, so their best bet is always to join four or five minutes early, so they can address any unexpected issues.

With a strong handle on the features available to them, they'll be able to lead the session with authority and be prepared to shut down any unanticipated security issues that come their way. For most sessions, they won't need to use this knowledge, but everyone (except the uninvited guests) will be grateful they're ready if a security breach occurs.