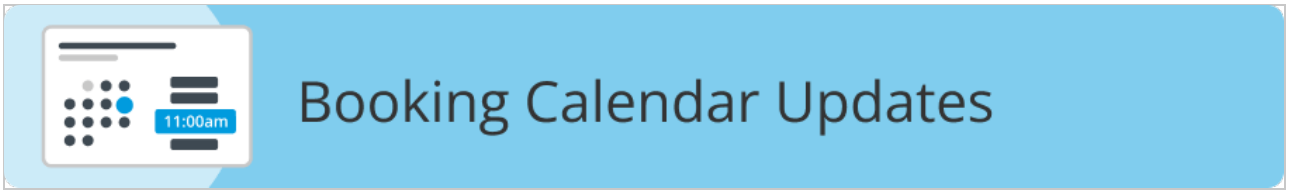
14 May 2026: Integrate OnceHub with Microsoft Entra ID, New Compliance Control: Restrict User Integrations and More...



Google Meet Link Update for Group Sessions

Google has updated how **Google Meet links** behave when used across multiple calendar events. To align with these Google Meet link behavior changes, **OnceHub Group Sessions** will now use a OnceHub redirect link instead of exposing the raw Google Meet link directly.

Participants can continue joining meetings as usual through the OnceHub join link, which will automatically redirect them to the correct Google Meet session.

Integrate OnceHub with Microsoft Entra ID (SCIM)

You can now integrate OnceHub with Microsoft Entra ID using SCIM to automate adding and deleting users to your OnceHub account.

- **Automated Provisioning and Deprovisioning:** Automatically add and delete OnceHub users (provisioning and deprovisioning) directly from Microsoft Entra ID. This allows IT admins to manage users and groups at scale without manual invitations.
- **Real-Time Synchronization:** Provides real-time synchronization to ensure user access is always current and up-to-date, reducing administrative overhead.

Who Can Access It

Plan: Available as part of the **Security & Compliance Add-On**.

Users:

- **Account Owners and Administrators:** Hold full authorization to configure the account-wide integration.

© Copyright OnceHub 2025. All rights reserved.

- **Team Managers and Members:** Restricted from accessing or modifying integration settings.

For detailed instructions on setting up this integration, please refer to our **How to Integrate OnceHub with Microsoft Entra ID** article.

New Compliance Control: Restrict User Integrations

As part of our ongoing commitment to enhancing security and compliance controls, OnceHub has introduced a **User Integrations** master switch on the Account Permissions page. This feature allows Account Owners to restrict specific platforms (e.g., Zoom, Google, iCloud), ensuring all team members adhere to the company's authorized tech stack.

When restricted, the integrations are disabled in the **User's Integrations** page preventing the use of unauthorized tools and ensuring all account data remains within your company's secured environment.

Key Benefits

This update centralizes governance, helping IT departments maintain compliance in regulated industries like healthcare or finance by ensuring sensitive data only flows through approved channels.

- **Administrative Control:** Account Owners can toggle integrations ON or OFF for the entire organization; Admins have view-only access.
- **Parent-Level Governance:** Disabling a parent integration (e.g., Google Calendar) automatically restricts associated sub-integrations (e.g., Google Meet, Gmail).
- **User Transparency:** Clear UI indicators inform users which tools are restricted, reducing support requests.

For more detailed instructions, please see our **Managing Account Permissions** article.

© Copyright OnceHub 2025. All rights reserved.