Booking for Outlook Setup Guide

Setting up Room Resource Account and SharePoint

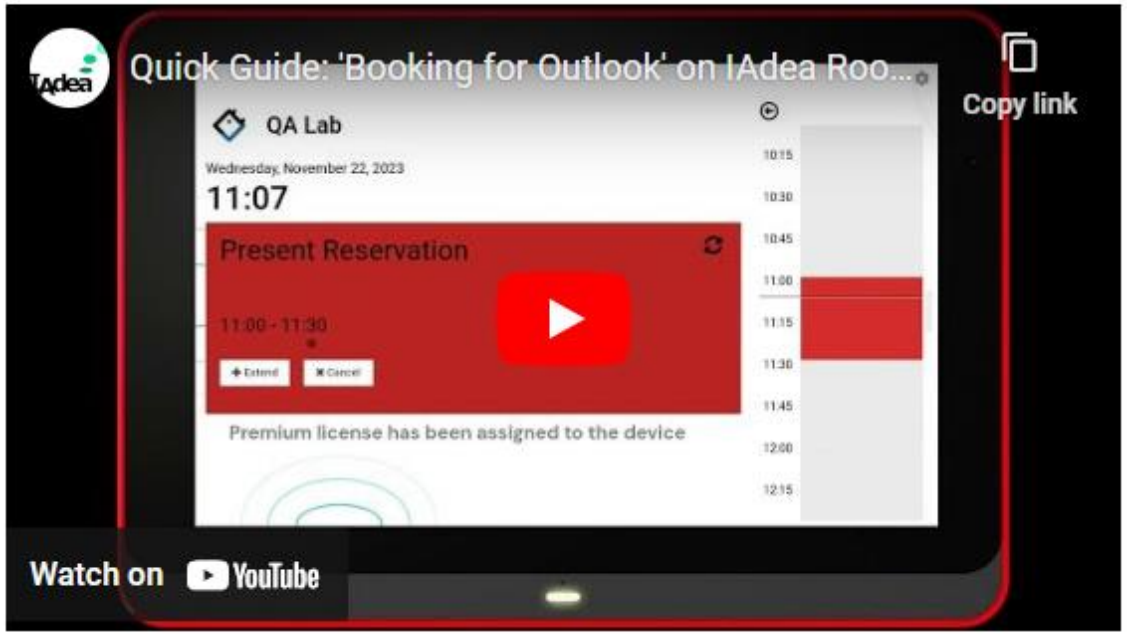
By: IAdea FAE

8/21/2024

Booking for Outlook Tutorial – The Introduction

- https://support.iadea.com/hc/en-us/articles/25874019540761-Booking-For-Outlook-Tutorial-The-Introduction

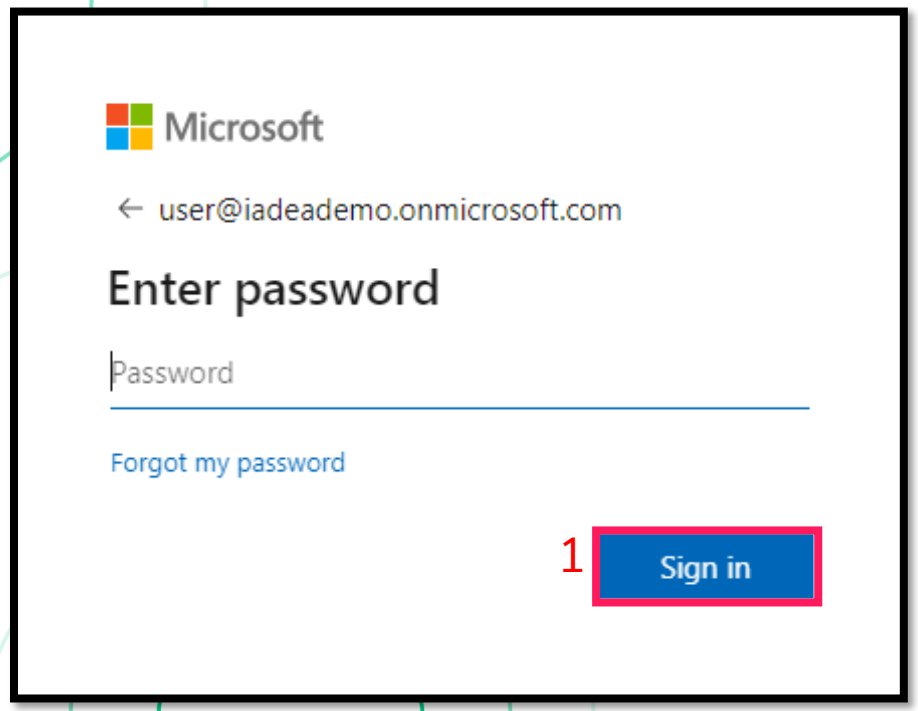
A comprehensive overview of the introductory video, guiding you through the initial setup and key features of Booking for Outlook:

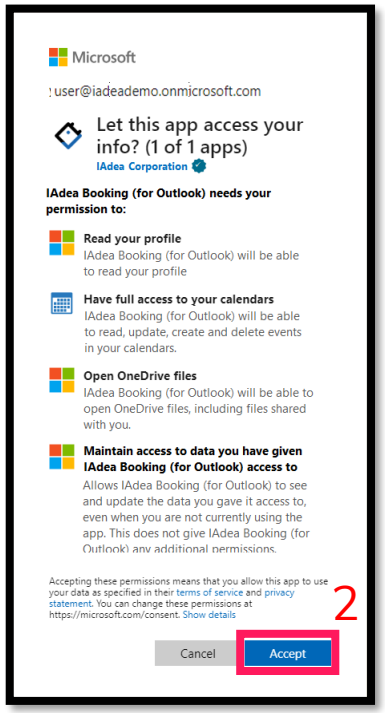


Please Note for First Room Login

1. When you first launch the Booking for Outlook app, it will redirect you to the Microsoft login page. Please enter your credentials and click **[Sign in]**
2. If this your first sign-in, Microsoft will prompt you to grant access to the app. Click **[Accept]**.
3. Next, you will be asked if you want to stay signed in. Click **[Yes]**.

Note: If you accidentally press [Cancel] at step 2, please refer to the TroubleshootingSection#1 to manually revoke app access.



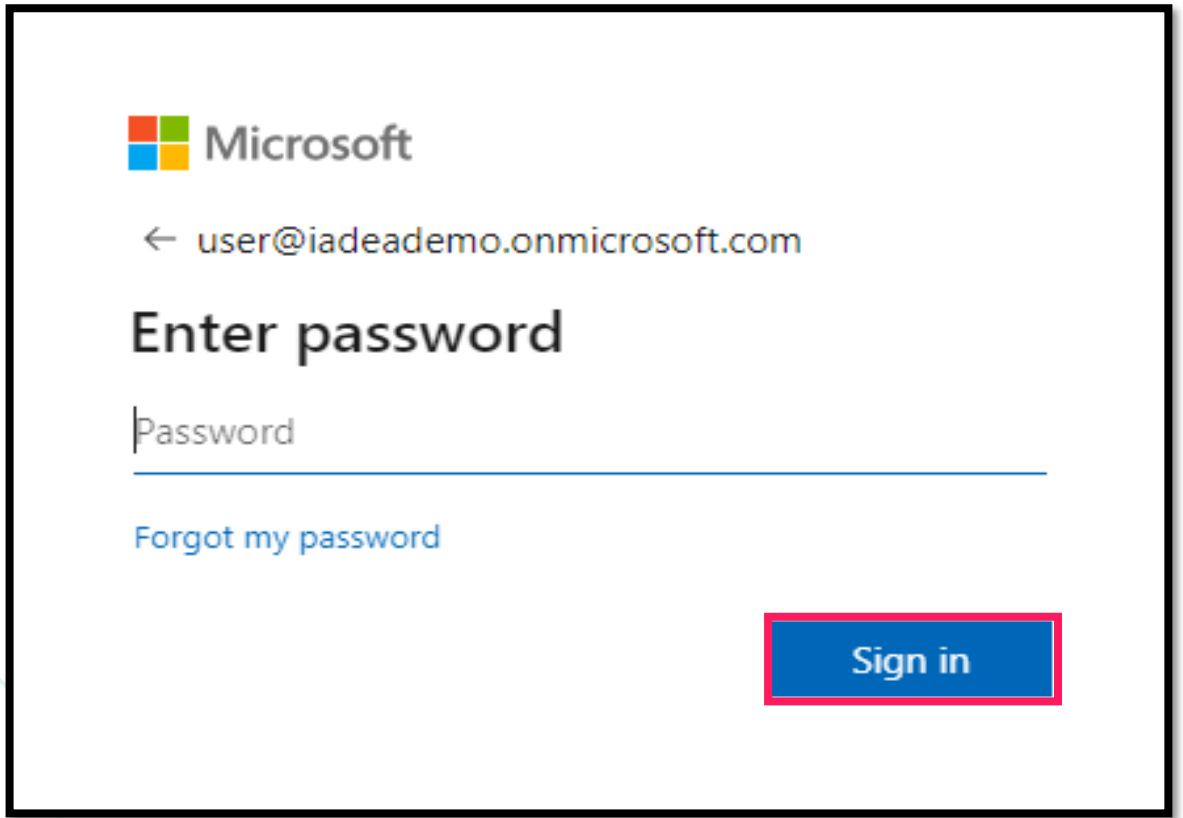


Step 1. Creating Room Resource Account

- Sign in to the Office 365 portal
- Create room resource account
- Reset the account password and set up new password

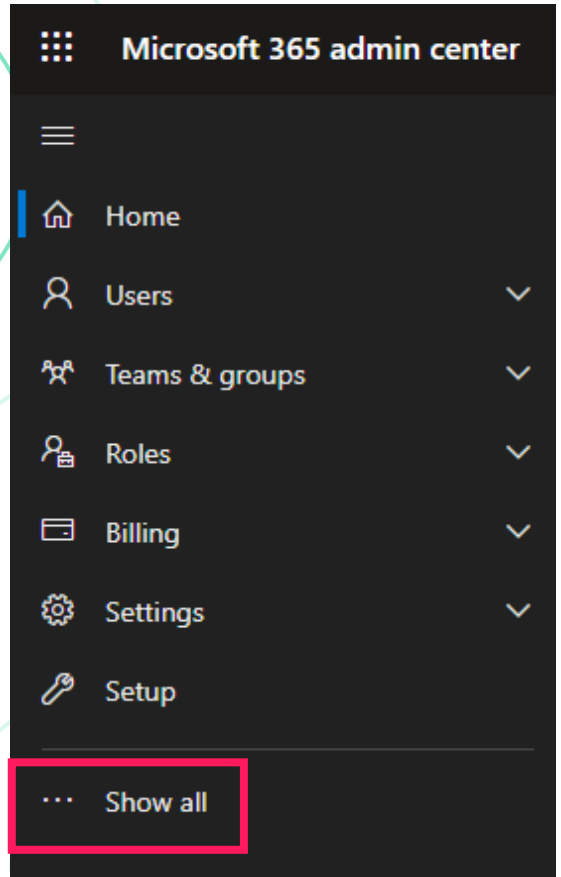
1. Accessing Your Office 365 Admin Portal with the Global Admin Account

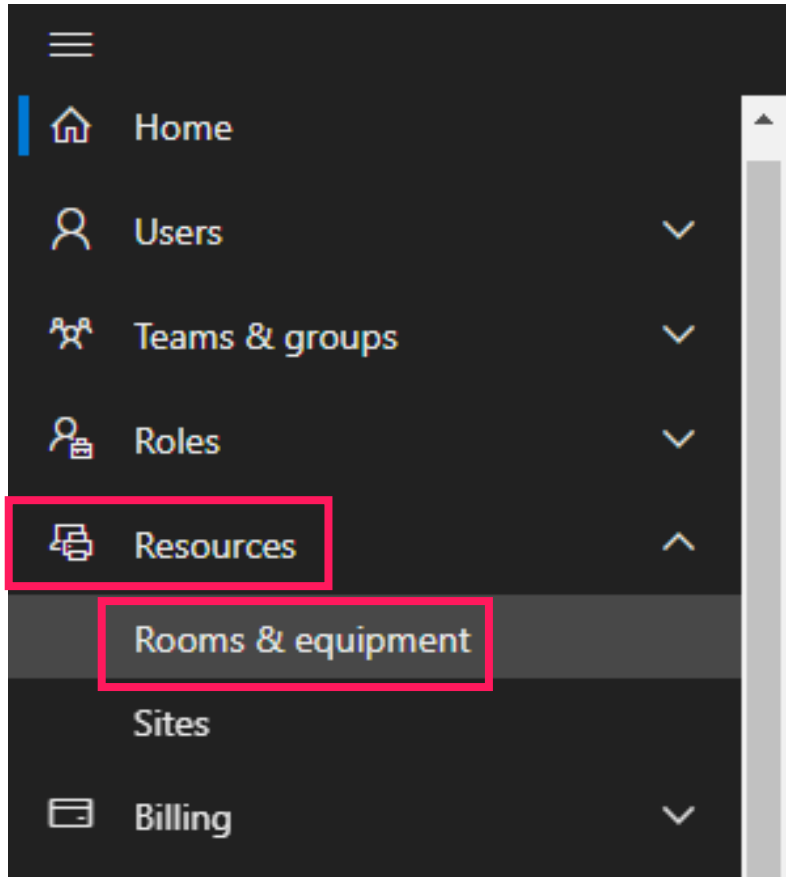
- Log in to the Office 365 admin portal using your admin credentials: https://admin.microsoft.com/.

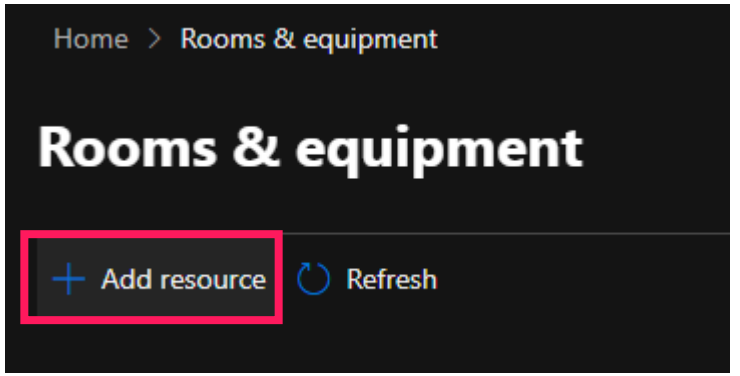


2. Establishing a Room Resource

- Navigate to the left side bar, select [Resources] from the menu, and choose [Rooms & equipment]. Proceed by clicking [Add resource].

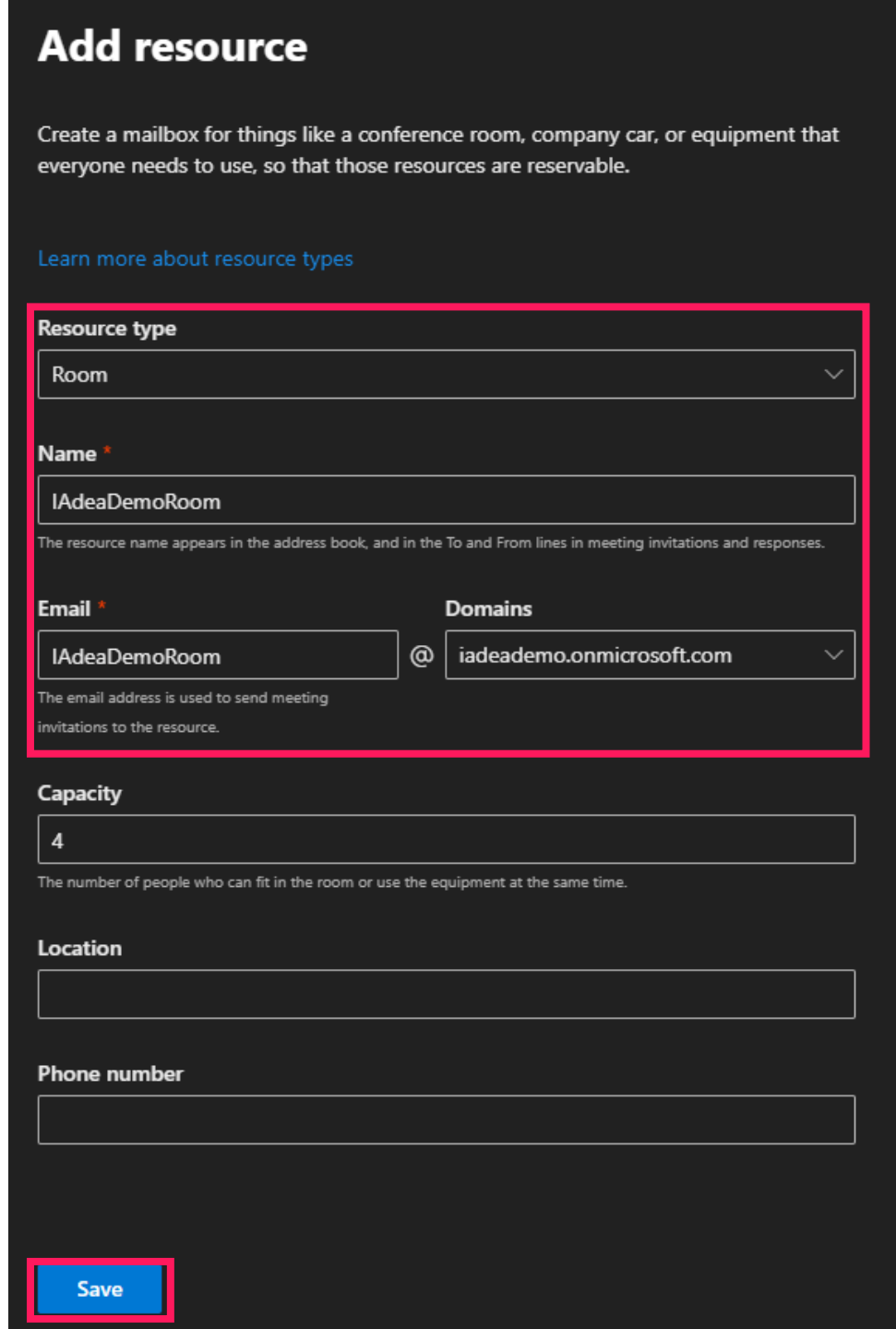






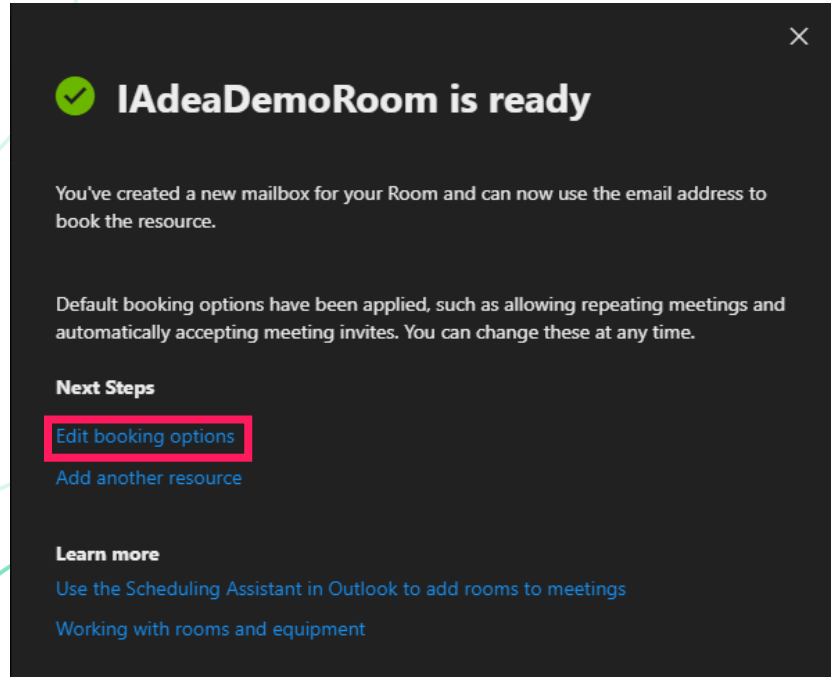
3. Filling the Room Details

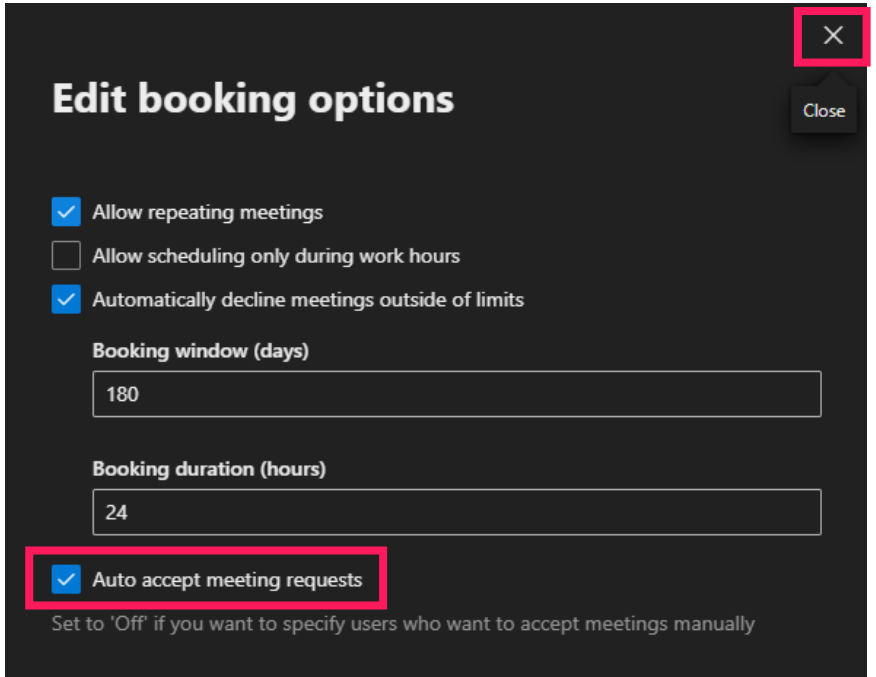
- Upon clicking the [Add resource] button, an input window will appear.
- Enter the room’s name and email address, then click [Save].



4. Adjusting Booking Preferences

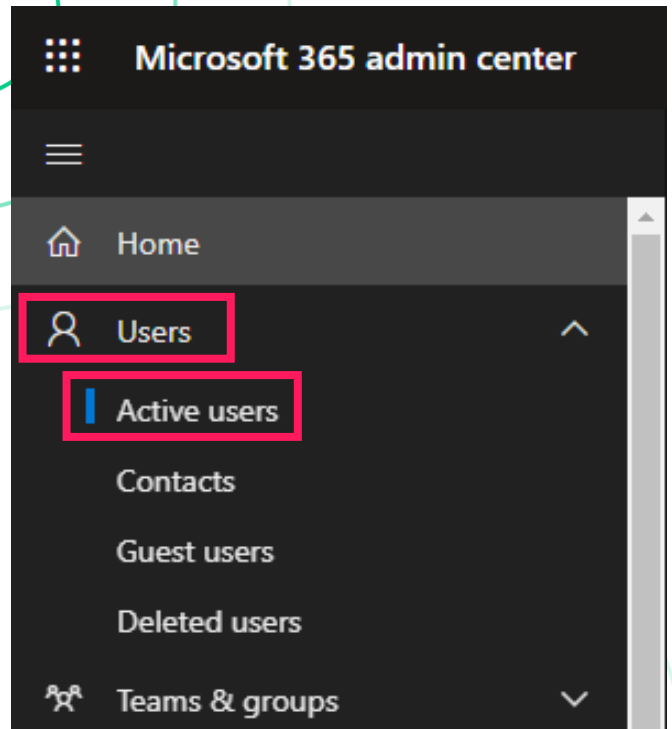
- To modify booking preferences, select [Edit Booking Options].
- Suggestion: Activate [Auto Accept Meeting Requests].
  - If disabled, you will need admin to approve every meeting reservation.
- Once done, close the dialog.

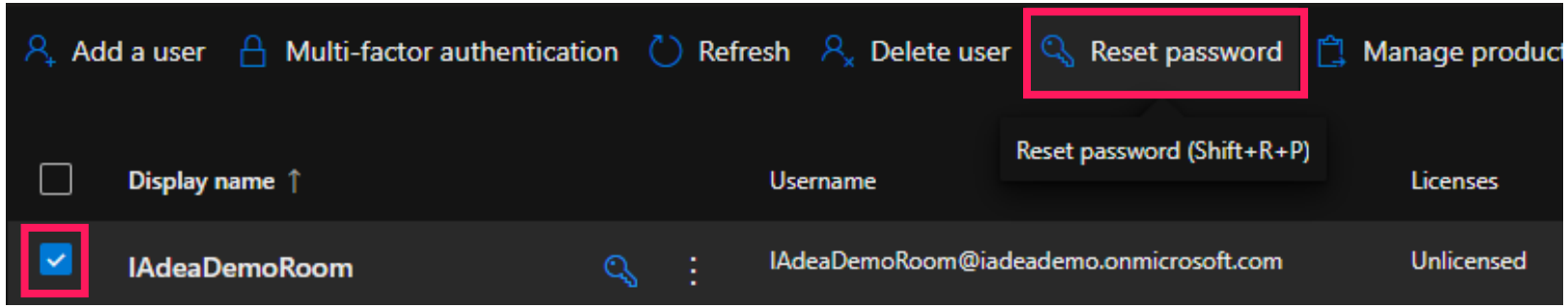




5. Resetting Room Account Password

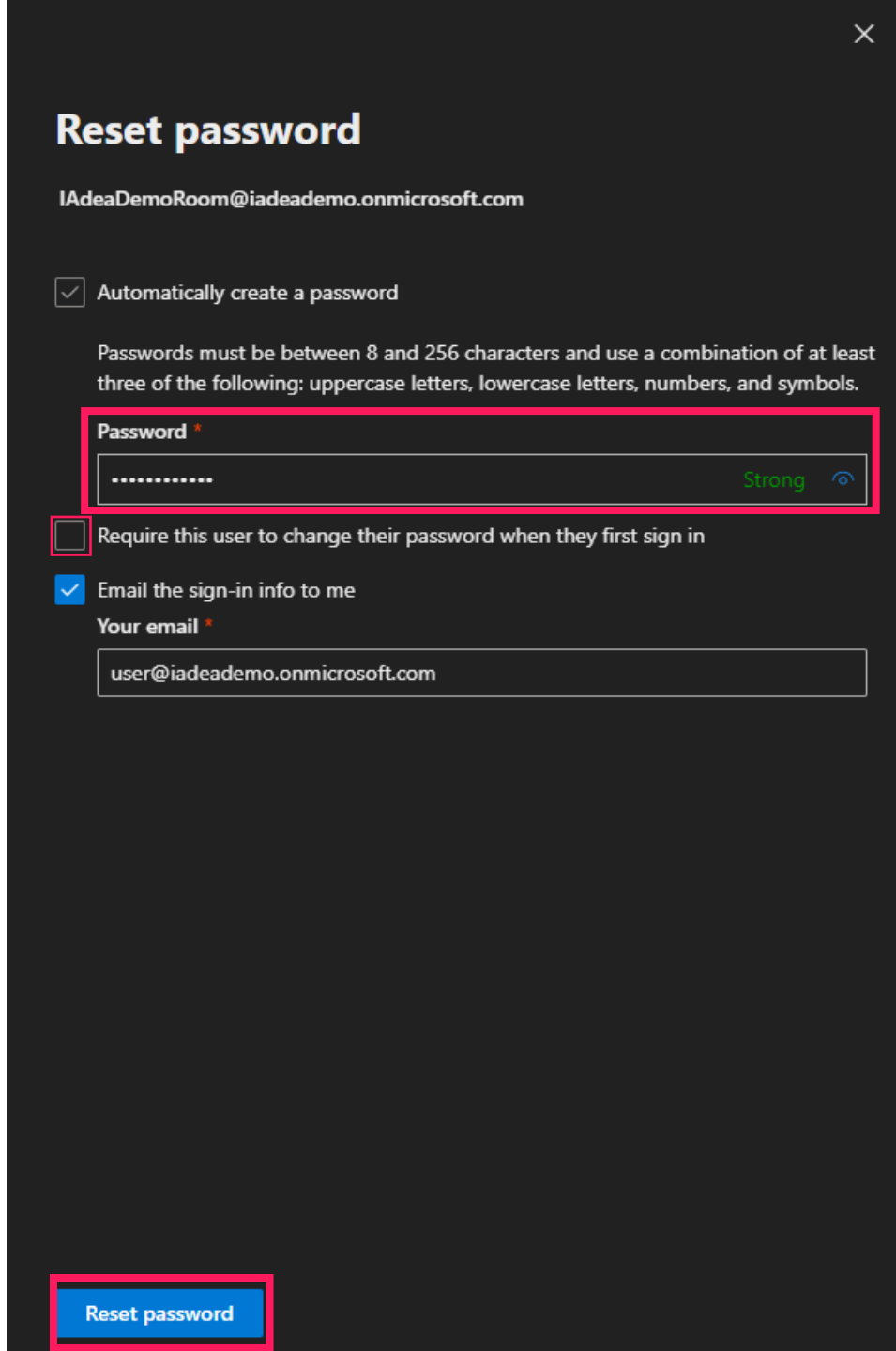
- Navigate to the left sidebar, select [Active Users] from the Users menu.
- Locate the newly created room resource, then choose [Reset Password].





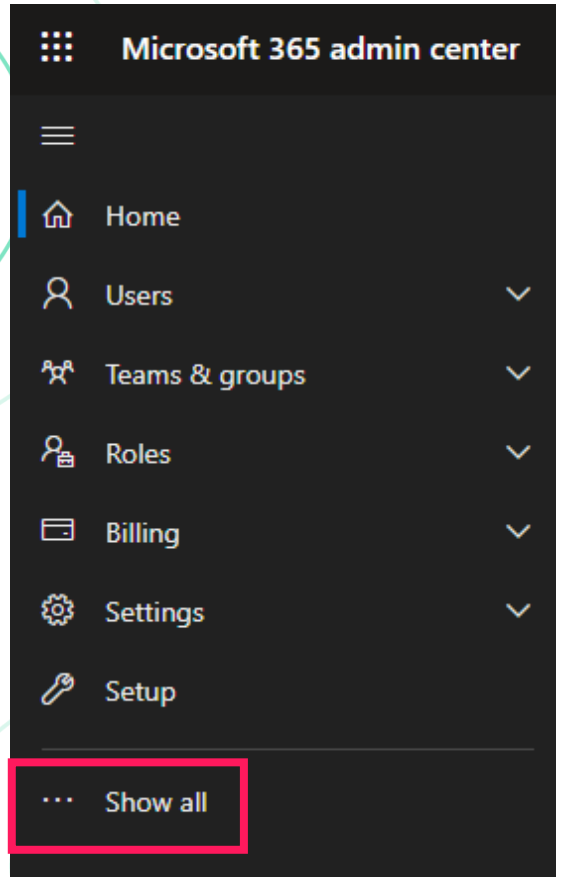
6. Entering The New Password

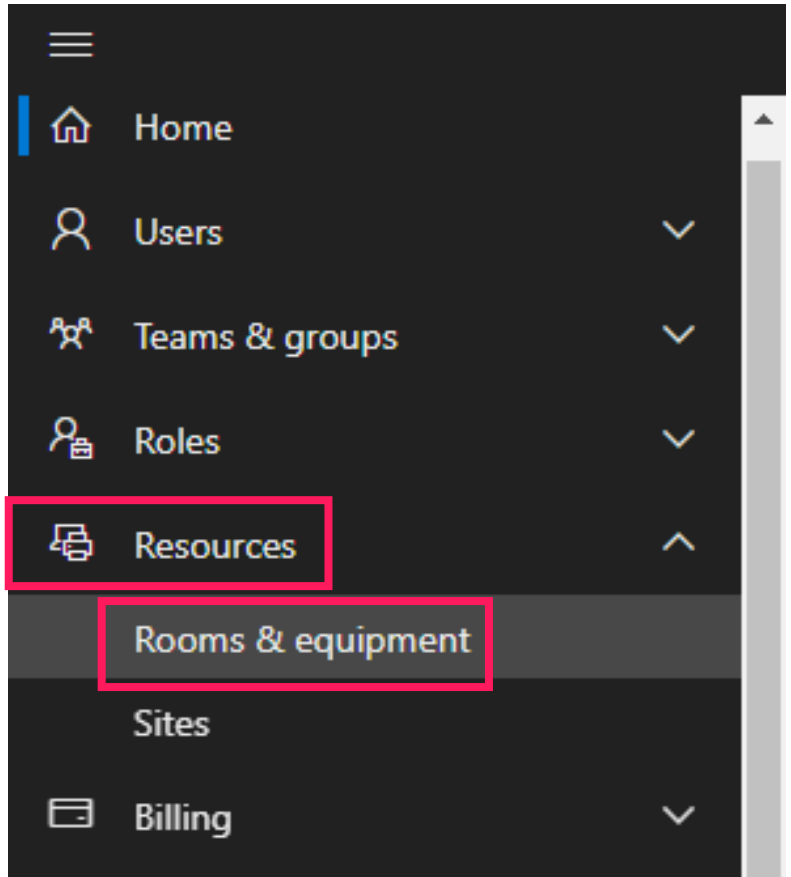
- Input a new password for the room.
- Ensure to uncheck the box **'Require this user to change their password when they first sign in'**.
- Optionally, choose to receive sign-in information via email by selecting the **'Email the sign-in info to me'** checkbox and entering an email address.
- Click [Reset password] and then [Close].

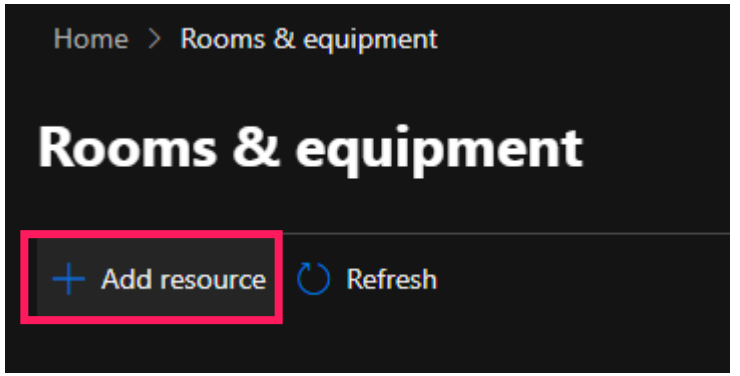


7. Establishing Multiple Rooms

- Apply the same procedure described earlier for each additional room. These rooms will use the same global configurations set up in step 3.





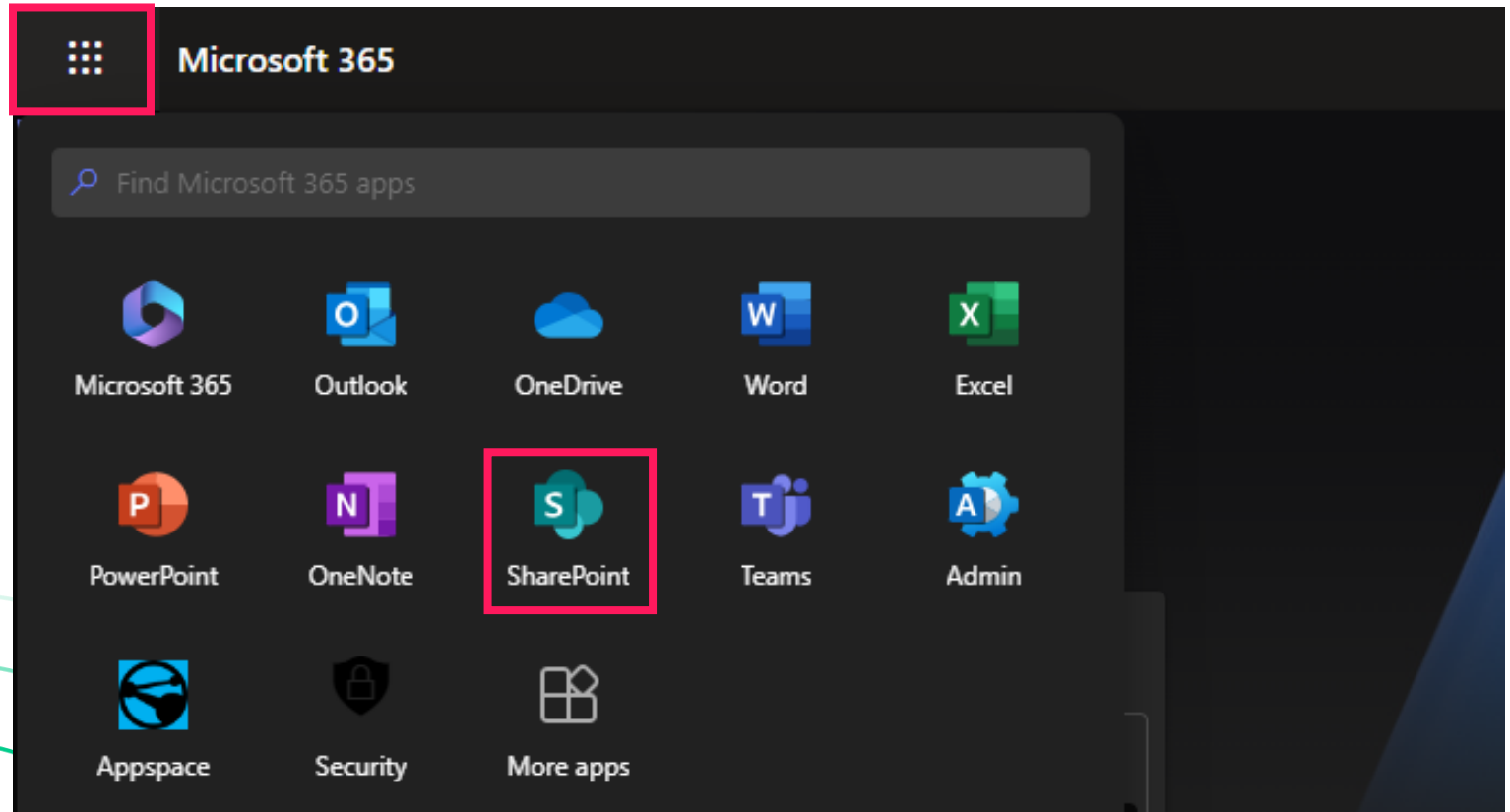


Step 2. Identifying the SharePoint Root Site

- Access SharePoint through Office365
- Identify the Root Site

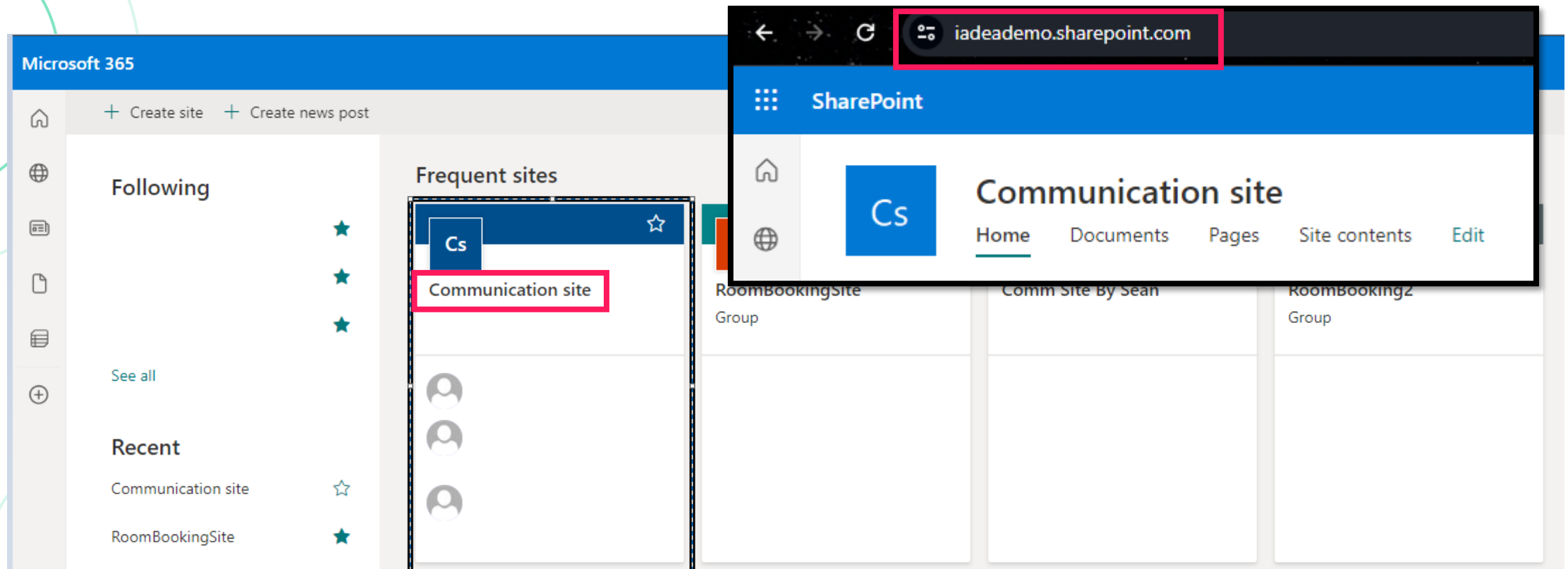
1. Accessing Office365 and Launching SharePoint

- Log in to your Office365 account: https://www.office.com/
- Navigate to the application thumbnail and choose SharePoint.



2. Identifying Your Root Site

- The default root site is typically labeled as the ‘Communication site’.
- Its URL commonly follows the pattern ‘[DomainName].sharepont.com’.

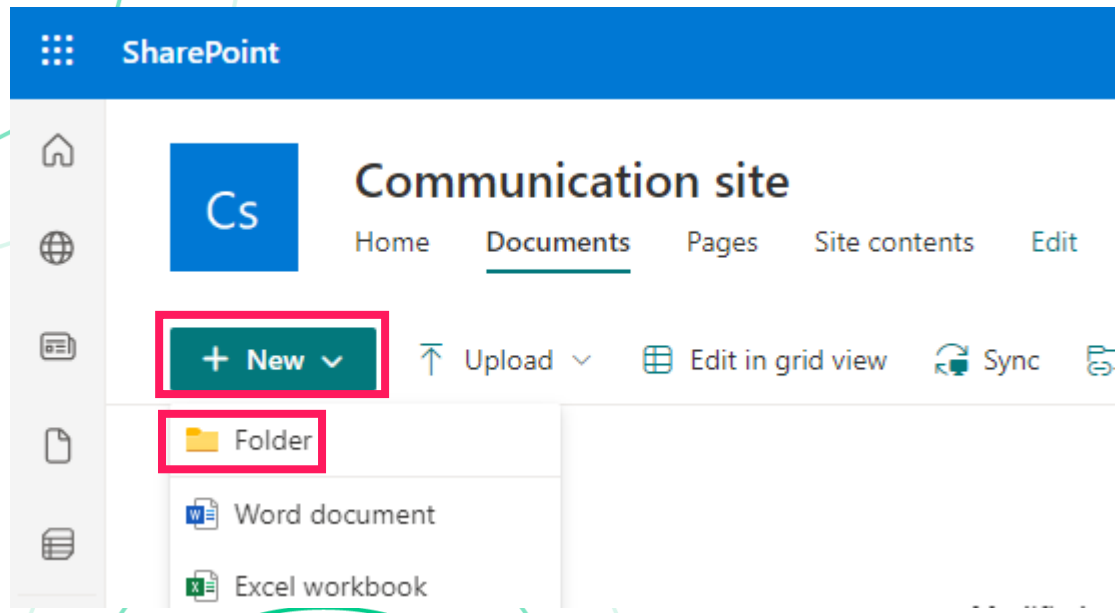


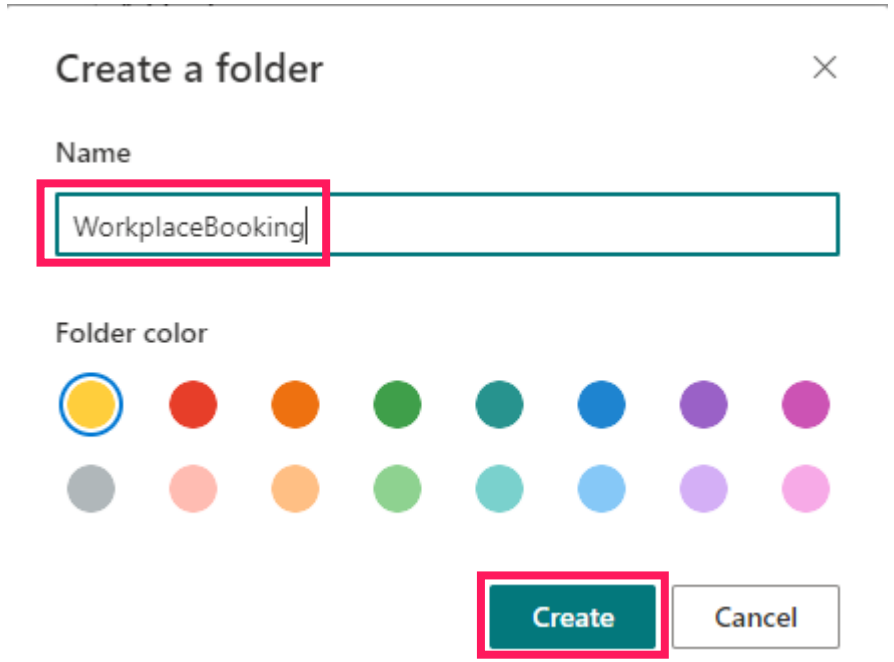
Step 3. Configuring Files on SharePoint

- Create a WorkplaceBooking folder under the root site document
- Create the config file: config.json
- Assign a customized background and logo

1. Creating a New Folder Named WorkplaceBooking

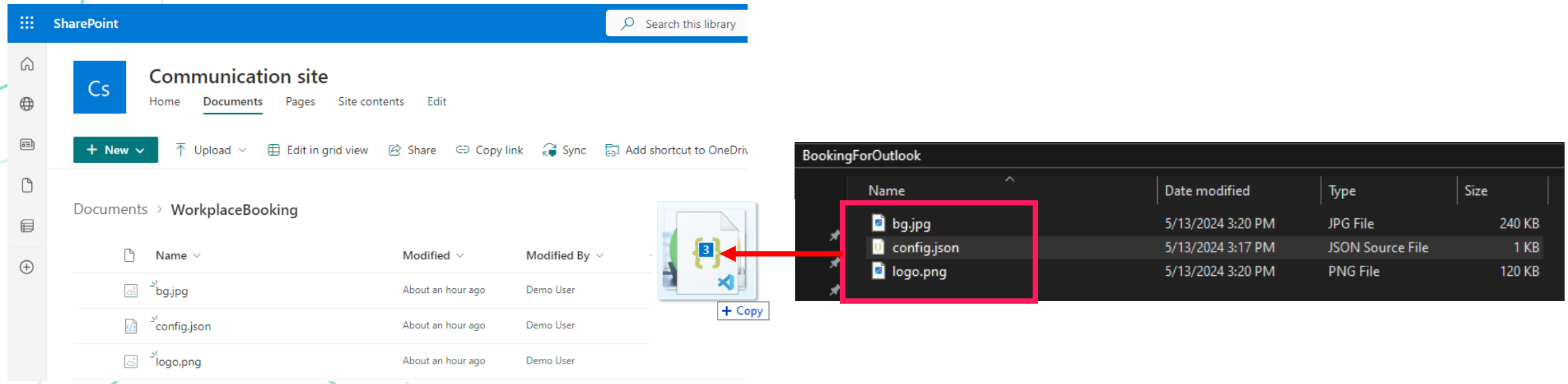
- Navigate to [Documents] under Root Sites, then click [New] > [Folder].
- Name the new folder as [WorkplaceBooking], then click [Create].





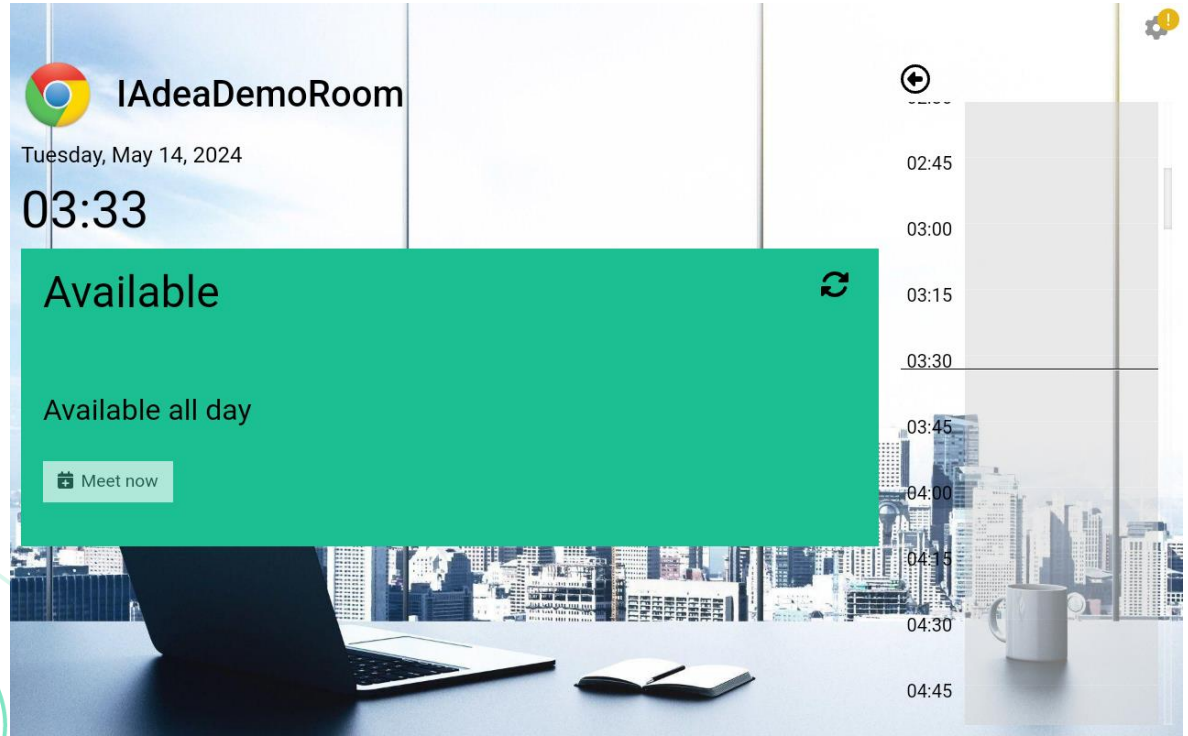
2. Pasting Config and Image Files

- Choose a background picture and your company's logo for Booking for Outlook (Name it bg.jpg and logo.png).
- Drag the selected files along with the config.json provided and paste them into the WorkplaceBooking folder.



Final Result

- If you can see the logo and background changes on the panel after refreshing or rebooting, then Booking for Outlook has successfully synced to your SharePoint.



Step 4. Changing Global Configurations

- Customize global configurations through config,json file.

Global Configurations

- Follow Section 5.1 of the **'doc_IAdeaBooking-manual_ENG_v1.0.0-01.pdf'** document.
- Utilize the provided **config.json** file for setting up IAdea Booking.
- Avoid direct copying of config.json from the document to prevent formatting issues.

5.1 Config.json file

The default config.json file looks similar to settings below:

```
{
   "locale": "en-US",
   "configLockPin": 1688,
   "dateTimeOption": {
        "hour12": false
   },
   "background": "bg.jpg",
   "logo": "logo.png",
   "theme": {
        "foreground": "#000000",
        "availableColor": "# 1cbf92",
        "busyColor": "#bb2323",
        "timeline": {
             "bgColor": "#d3d3d3",
             "futureEventTimeBlockColor": "#c96565",
             "currentEventTimeBlockColor": "#d72c2c",
             "expiredEventTimeBlockColor": "#6c757d"
        }
   },
   "calendar": {
        "enableOnsiteBook": true,
        "enableFutureEventBook": true,
        "enableFutureEventCancel": true
   },
   "lightbar": {
        "available": {
             "color": "#00ff00",
             "mode": "on"
```

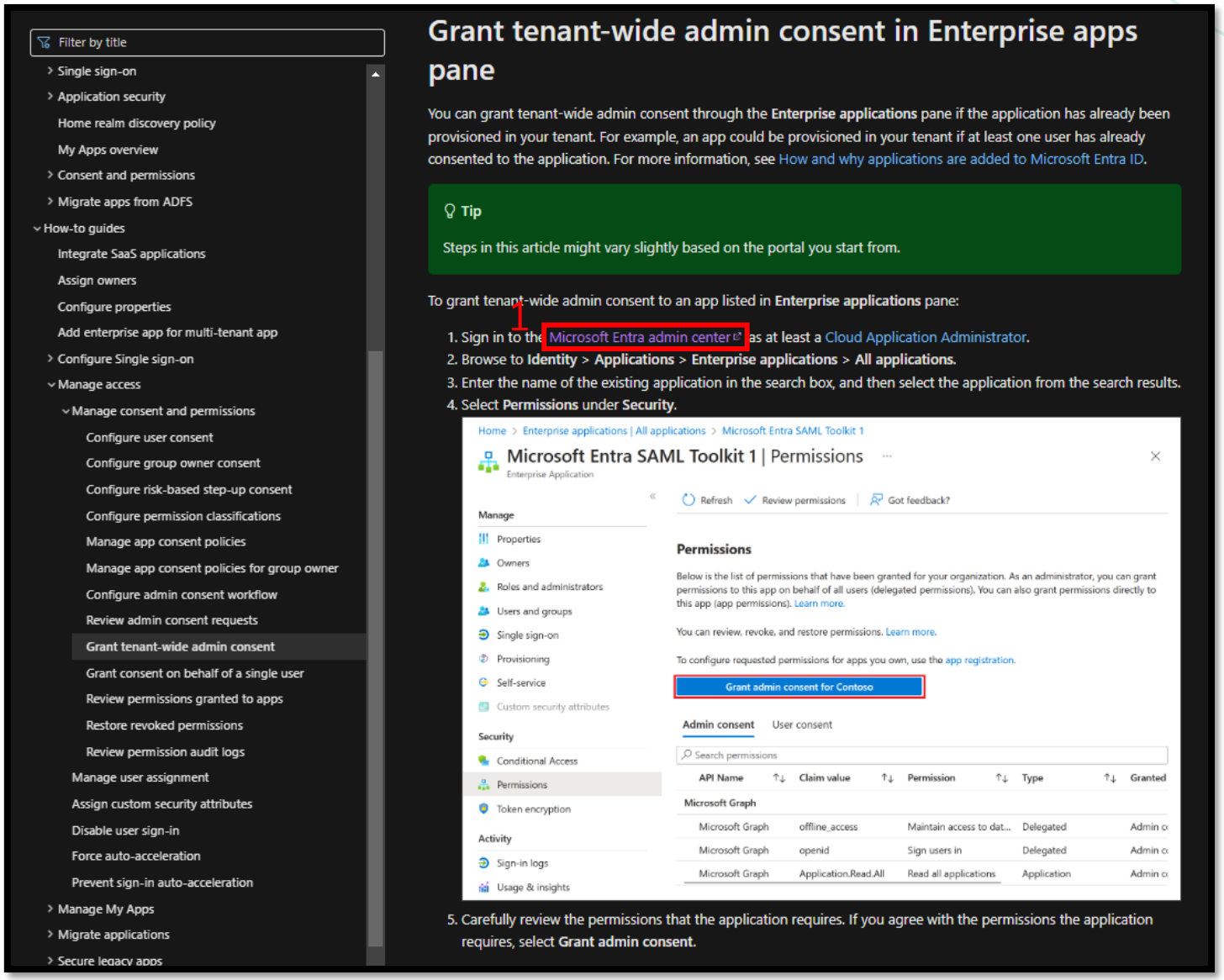
Troubleshooting

- Manually grant app access.
- Room resources account sign-in issues.
- Disable per-user MFA in MS365 Admin Center.
- Disable conditional access policy for IAdea Booking (for Outlook) in Microsoft Entra Admin Center.
- Disable password expiration for resource account.
- Disable Password Expiration on MS365 Admin Center (Alternative)
- List of IPs and domains to whitelist

1. Manually Grant App Access (1/2)

- **Issue**: Consistency and reliability problems; some data is either not updating correctly or disappearing.
- **Fix**:

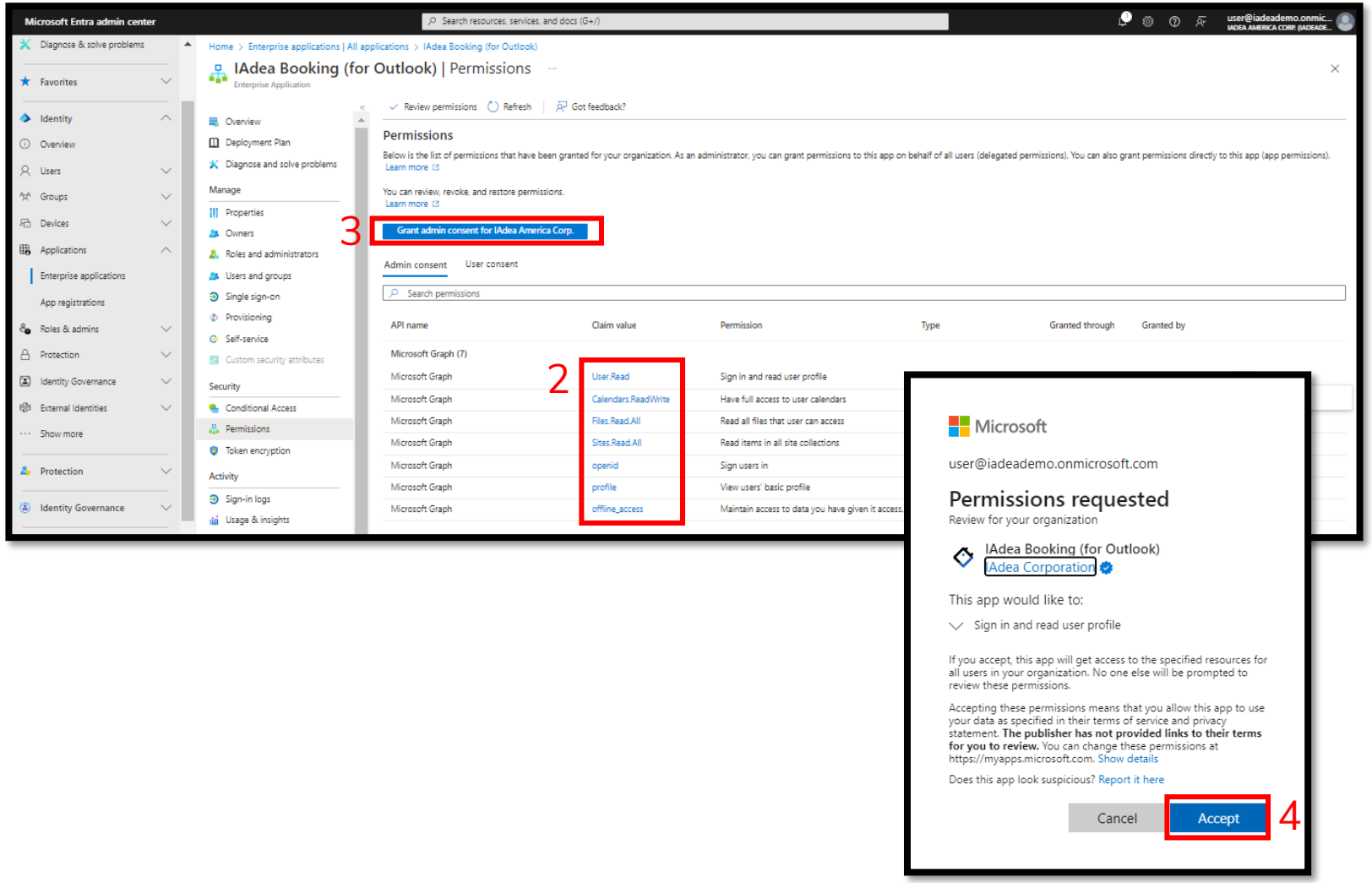
1. Follow this link for detailed instructions: https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/grant-admin-consent?pivots=portal



1. Manually Grant App Access (2/2)

- Issue: Consistency and reliability problems; some data is either not updating correctly or disappearing.
- Fix:

1. Follow this link for detailed instructions: https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/grant-admin-consent?pivots=portal
2. Verify that all claim values are listed under [Admin consent].
3. If not, click [Grant admin consent]
4. Log in and click [Accept]



2. Room Resources Account Sign-In Issues

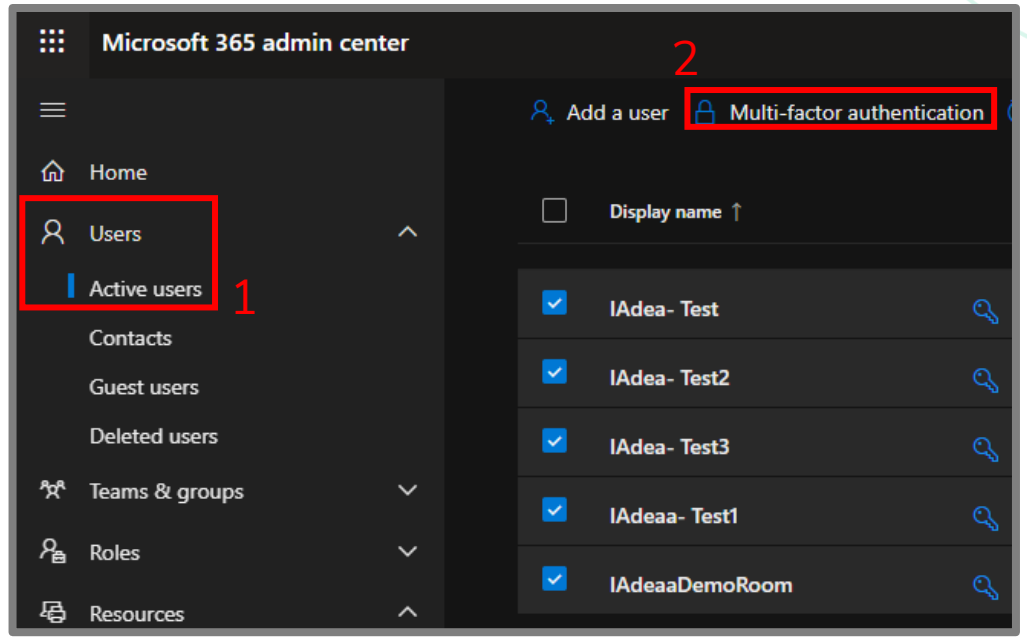
- **Issue:** Booking for Outlook device prompts for login after a set period.

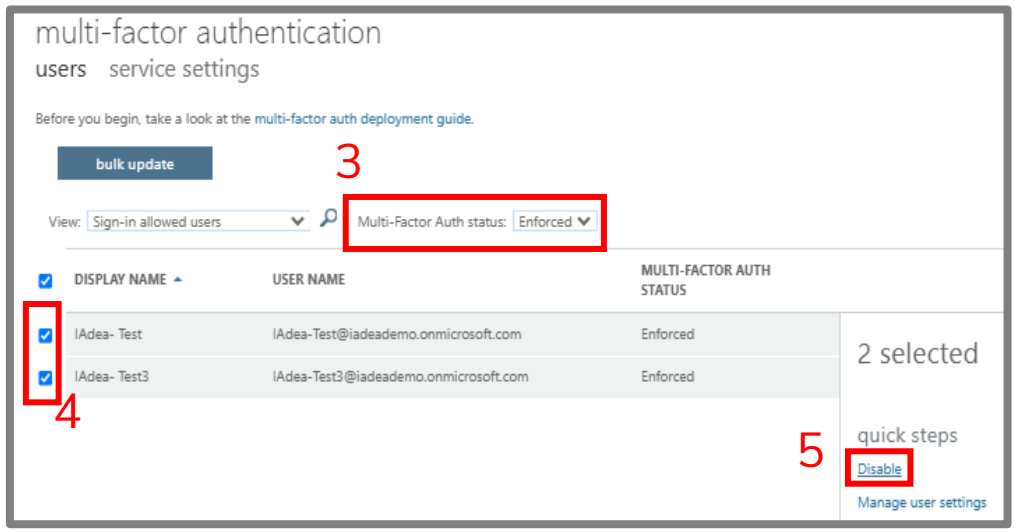
- **Reference on MS Teams Rooms:** Fix Teams Rooms resource account sign-in issues
  - ***Notes: Do not follow the instructions, as Booking for Outlook and MS Teams Rooms are separate apps (reference purpose only).***

- **Solutions for Frequent Sign-In Request Issues:**
  1. **MFA Not Disabled**
     - **Fix**: Disable per-user MFA on **Microsoft 365 Admin Center**
     - *Explanation*: Teams Rooms resource accounts shouldn't be configured to use MFA
  2. **Conditional Access Policies Blocking Sign-In**
     - **Fix**: Exclude the application from Conditional Access policies in **Microsoft Entra Admin Center**.
     - *Example of policy*: Conditional Access: Session
  3. **Password Expiration Enabled**
     a) **Fix 1**: Set password expiration to “never expire” for room resources accounts using **Microsoft Graph PowerShell** or **Active Directory (on-premises).**
     b) **Fix 2**: Disable password expiration in **Microsoft 365 Admin Center** and **Microsoft Entra Admin Center** (applies organization-wide).
     c) **Fix 3**: Set a longer password expiration period.

2a. Disable Per-User MFA in MS365 Admin Center

- **Issue**: Booking for Outlook device prompts for login after a set period.
- **Fix**:
  1. Log in to **Microsoft 365 admin center** with a global admin account and navigate to **[Users]** > **[Active Users].**
  2. Select **[Multi-factor authentication]** settings.
  3. Use the **Multi-Factor Auth status filter** (Enforced/ enabled).
  4. Select the **room resources account**.
  5. Click **[Disable]**.
- Detailed Instructions: [Turn off per-user MFA]





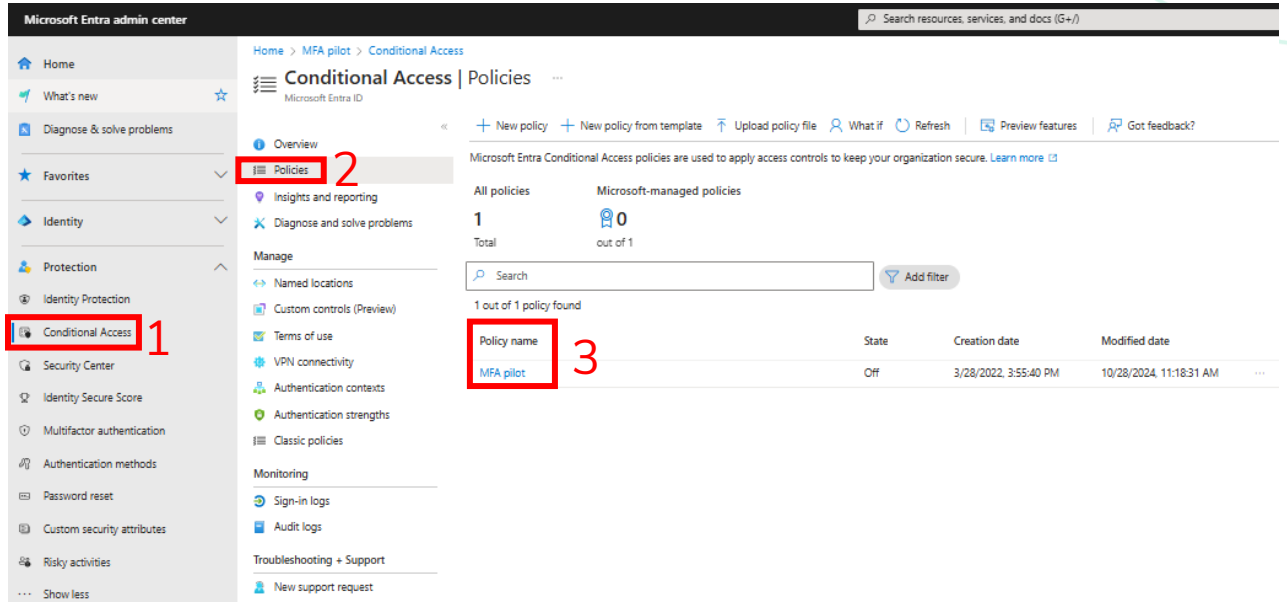
Turn off per-user MFA

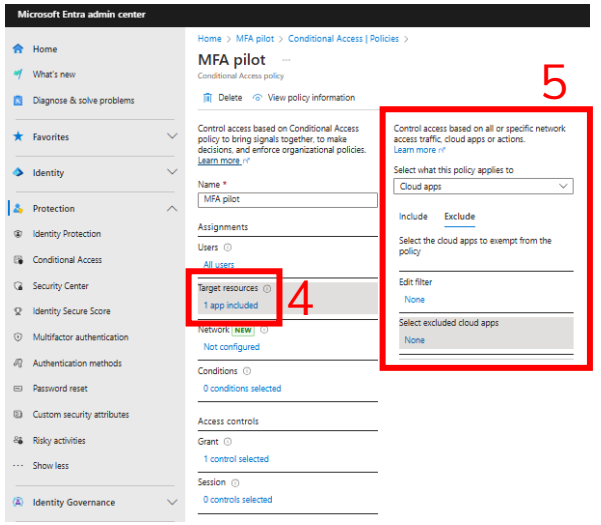
If you've previously turned on per-user MFA, you must turn it off before enabling Security defaults. You should also turn off per-user MFA after you've configure your policies and settings in Conditional Access.

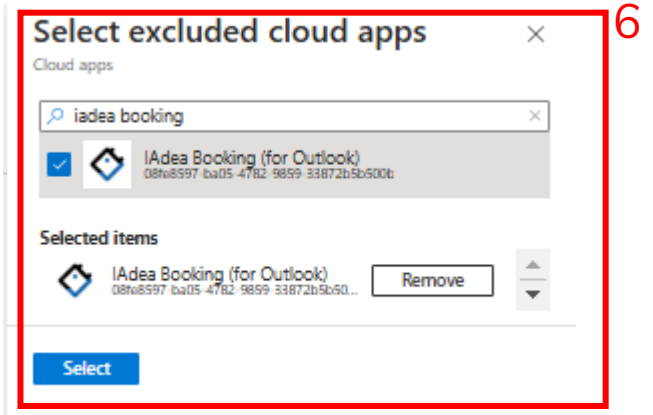
1. In the Microsoft 365 admin center, in the left nav choose **Users** > **Active users**.
2. On the **Active users** page, choose **multifactor authentication**.
3. On the multifactor authentication page, select each user and set their multifactor authentication status to **Disabled**.

2b. Disable Conditional Access Policy for IAdea Booking (for Outlook) in Microsoft Entra Admin Center.

- **Issue**: Booking for Outlook device prompts for login after a set period.
- **Fix**:
  1. Log in to **Microsoft Entra Admin Center** with a global admin account and go to **[Protection]** > **[Conditional Access]**.
  2. Select **[Policies]** and review each policy that might sign-in process.
  3. Open the policy.
  4. Go to **[Target resources].**
  5. Click **[Exclude]** > **[Select excluded cloud apps]**.
  6. Choose **[IAdea Booking (for Outlook)]** and click **[Select]**.
- Reference:
  - [How to exclude and include Cloud apps in Conditional Access Policies in Microsoft Entra | Microsoft]
  - [Configuring Azure Active Directory Conditional Access - Visual Studio App Center | Microsoft Learn]

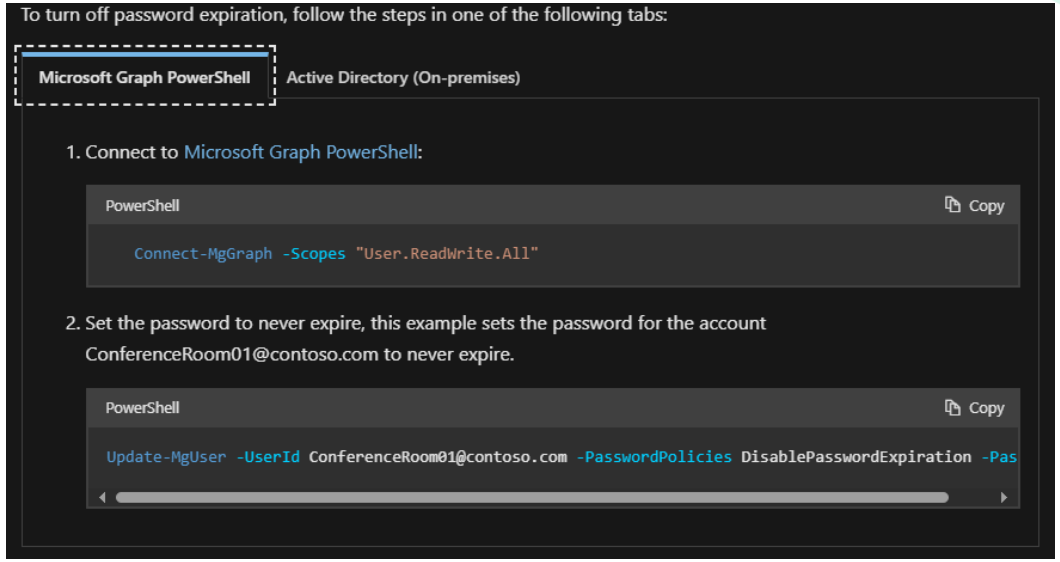


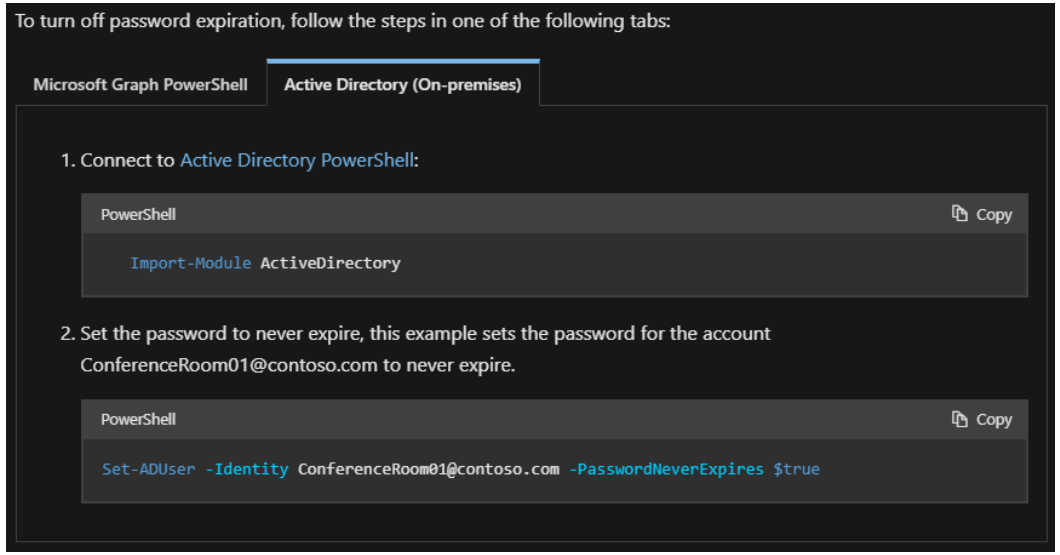




2c. Disable Password Expiration for Resource Account

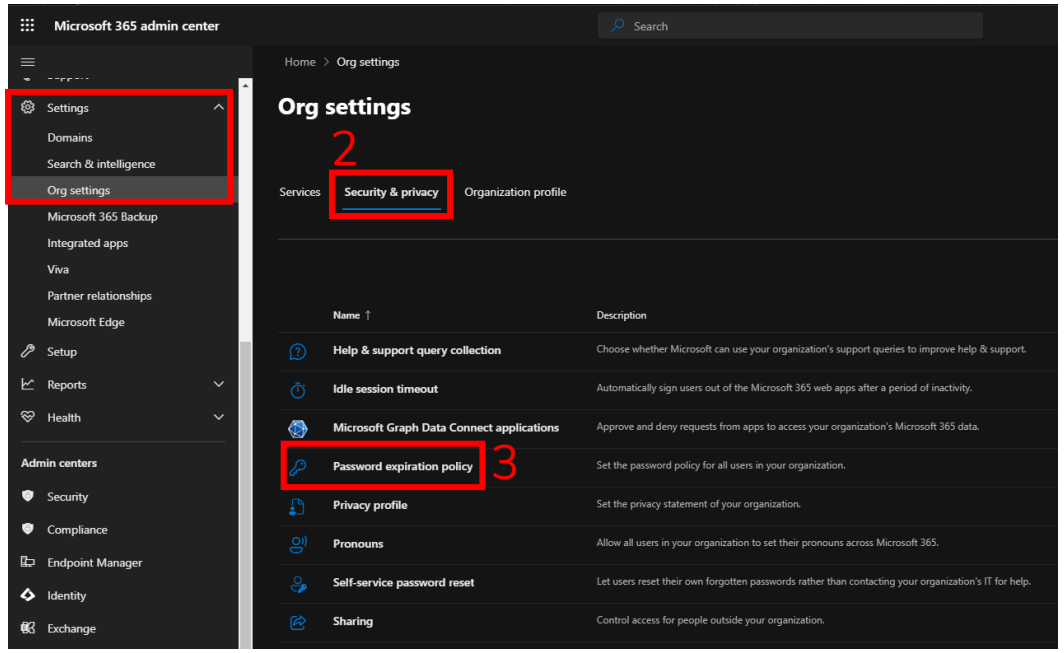
- **Issue**: Booking for Outlook device prompts for login after a set period.
- **Fix**:
  - **Microsoft Graph PowerShell or AD (On-premises)** is required to disable password expiration for specific accounts.
  - **Alternative Options:**
    - Disable tenant-wide password expiration (affects all users).
- Detailed instructions:
  - [Create resource accounts for Teams Rooms and shared devices - Microsoft Teams | Microsoft Learn]

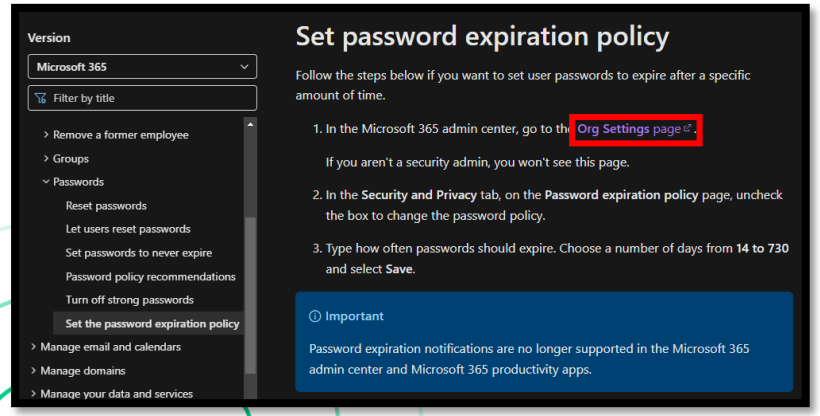


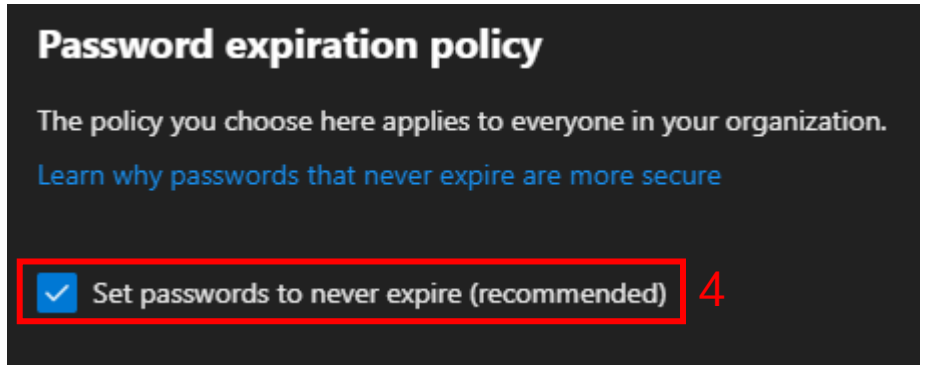


2c. Disable Password Expiration on MS365 Admin Center (Alternative)

- **Issue**: Booking for Outlook device prompts for login after a set period.
- **Fix**: *(Warning: Applies to entire organization)*
    1. Log in to **Microsoft 365 Admin Center** as a global admin account and navigate to **[Settings]** > **[Org settings]**.
    2. Open **[Security & privacy]** tab.
    3. Select **[Password expiration policy]**.
    4. Enable the **[Set passwords to never expire (recommended)]** option
- Detailed instructions:
    - Set the password expiration policy for your organization







3. List of IPs and Domains to Whitelist

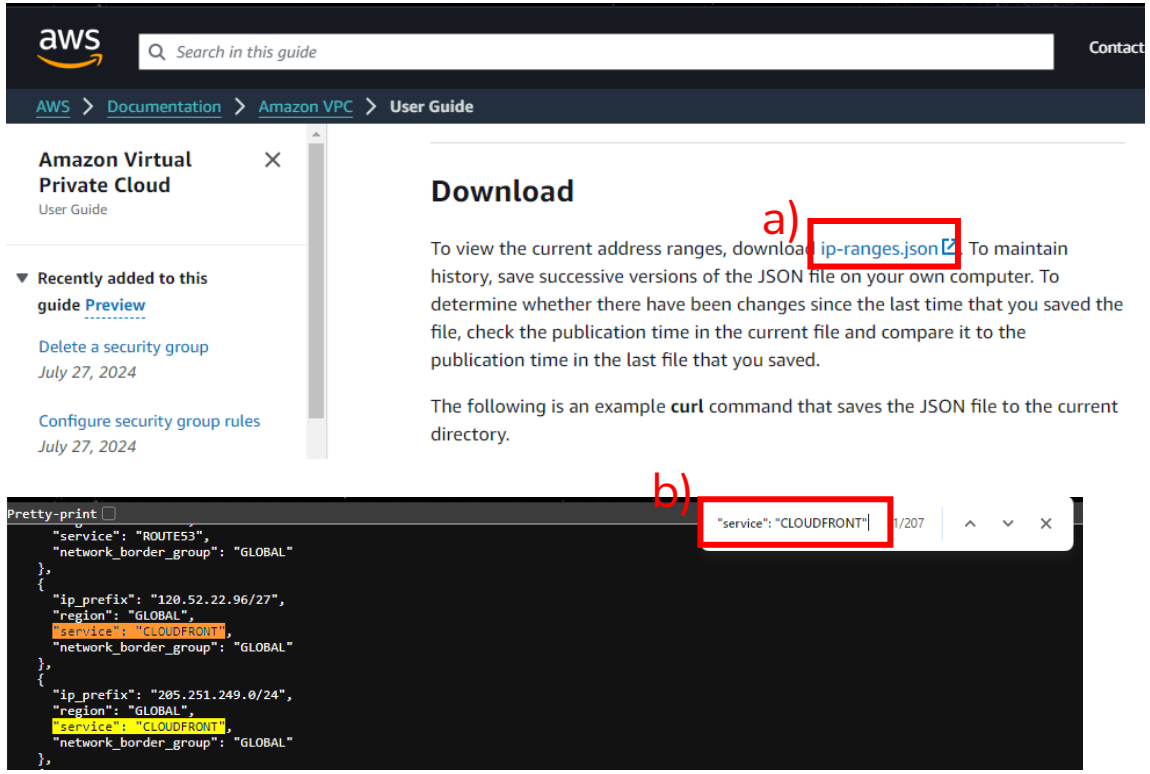
- Please allow both the domain and IP to minimize any network issues:

1. Responsible for license and API: https://support.iadea.com/hc/en-us/articles/360001155223-IAdeaCare-Why-is-my-device-not-receiving-a-pairing-code-or-always-showing-offline-on-the-IAdeaCare-website

2. Responsible for UI (AWS and CloudFront): https://docs.aws.amazon.com/vpc/latest/userguide/aws-ip-ranges.html
    a) Step 1: Download ip-ranges.json file on the website
    b) Step 2: Find [“service": "CLOUDFRONT”] and it will display several IP ranges
    c) Step 3: Determine which IP ranges are being used in your region.

3. Responsible for UI (AWS and CloudFront): office365/Azure/AD

4. Domain: booking.for-workplace.com



Thank you

America

20 Fairbanks, Suite 170
Irvine, CA 92618
USA

Taiwan

114, 3F, No. 21
Ln. 168, Xingshan Rd.
Neihu Dist., Taipei, Taiwan

Contact Us

Product questions

Sales@IAdea.com

Technical Assistance

Support@IAdea.com